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:	*NRI SecureTechnologies, Ltd.*
Name of Submitter/POC:	*Hideaki Furukawa*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
1					The new concepts of "enterprise" and "public" are appearing in 63B and 63C, without definition and explanation, and even having inconcistency of how their wordings. For example, "public-facing" and "enteprise-facing" in 63B, and "enterprise application" in 63C. Such inconsistency and the lack of explanation may cause confusions to readers to determine whether their online services are "public-facing" or "enterprise-facing".	Unify the wording of "enterprise-facing" (appearing as "enteprise systems" in the line 1337 of 63B, "federal enterprise" in the lines 2909, 2910, and 3024 of 63B, "enterprise applications" in the line 2966 of 63B and lines 1944, 3374, 3375, and 3378 in 63C, "enterprise use cases" in the lines 2972 and 2999 of 63B, "enterprise scenarios" in the page 93 of 63B). Besides, add definitions and explanations of "public-facing" and "enterpirse-facing" online services in the introduction and/or the glossary. One idea is to copy and modify the explanations from 2. Purpose of NIST SP 800-63Bsup1 as: "public-facing applications (i.e., federal information systems that interact with public identities, as described in OMB Memorandum M-19-17) and enterprise-facing applications (i.e., federal information systems that primarily interact with federal enterprise identities, as described in OMB Memorandum M-19-17)".
2	63-Base	1.3.1	5	494	"ISO 27001" should be "ISO/IEC 27001"	Replace "ISO 27001" with "ISO/IEC 27001". Also, it might be better to add ISO/IEC 27001 in the references.
3	63-Base	2.3.1	13	717	The definition and explanation of the activation secret is not aligned with them in 63B.	Change the first two sentences of the paragraph as follows. (Copied from 63B) "Password used locally as an activation factor for a multi-factor authenticator is referred to as an activation secret. An activation secret is used to obtain access to a stored
4	63-Base	3.4.2	43	1624	"IDPs" (Identity Providers) should be written as "IdPs", as according to the list of abbreviations.	Replace "IDPs" with "IdPs".
5	63-Base	3.7	50	1800	"Could" should be uncapitalized.	Uncapitalize "Could".
6	63A	2.1.2	7	567	The note regarding the trusted referees may be better to be in a separate paragraph and also be indented (same as other notes).	Separate the paragraph and indent the note regarding the trusted referees.
7	63A	2.5.1	14	789	Since 63C is now using the term "attribute bundles" for (verifiable) credentials, it may be better to align the wording with it.	Either add "attribute bundles" next to "verifiable credentials" or replace "verifiable credentials" with "attribute bundles"
8	63A	3.1.2.1	18	897	The note regarding the data washing may be better to be in a separate paragraph and also be indented (same as other notes).	Separate the paragraph and indent the note regarding the data washing.
9	63A	3.1.13.4	34	1443	The note here may be better to be in a separate paragraph and also be indented (same as other notes).	Separate the paragraph and indent the note.
10	63A	4.3	44	1791	Attendance of CSP proofing agent for identity proofing at IAL3 is described as "must", which may be better to use "SHALL" to clarify that it is a requirement. Also, it might be better to clarify to whom this requirement is mandated to by paraphrasing the sentence.	Replace "must" with "SHALL". Also, paraphrase the sentence as "In addition, a CSP proofing agent, described in Sec. 2.1.2., SHALL attend at IAL."
11	63A	4.4	49		For the evidence collection of IAL3, it might be better to rephrase "1 STRONG + 1 FAIR" with "1 FAIR and 1 STRONG" to align with the IAL2's.	Replace "1 STRONG + 1 FAIR" with "1 FAIR and 1 STRONG"
12	63A	4.4	49		"digital" might be missing in fron of the "signature verification" for the Attribute Validation of IAL2.	Add "digital" in front of the "signature verification" for the Attribute Validation of IAL2, unless it is intentionally written without "digital".
13	63A	4.4	49		For the requirements same as the lower level's, describe as "Same as IALx"	For the Evidence Collection of IAL3, describe as "Same as IAL2". For the Attribute Collection of IAL2, decribe as "Same as IAL1". For the Evidence Validation of IAL3, describe as "Same as IAL2". For the Attribute Validation of IAL3, describe as "Same as IAL2" (unless IAL2 is not mandating a sigital signature verification, but a signature verification, as pointed out in the comment
14	63A	8.3	65	2320	"enrollment codes" might be a mistake of "confirmation codes".	Replace "enrollment codes" with "confirmation codes".
15	63A	8.3	66	2366	"enrollment codes" might be a mistake of "confirmation codes".	Replace "enrollment codes" with "confirmation codes".
16	63A	A.2	80		Veteran Health ID Card (VHC) is listed as an example of a fair evidence, and listed again as a strong evidence example.	Remove the VHIC from either fair or strong evicence examples.

17	63B				Besides the cryptographic authenticators', authentication secrets of other types of authenticators can be synced (e.g., password and TOTP in a password manager). To avoid confusion, it may be better to rephrase "syncable authenticators" with "syncable cryptographic authenticators" in the guidelines.	Replace all "syncable authenticators" with "syncable cryptographic authenticators" in the guidelines.
18	63B	2.5	10		Since syncable (cryptographic) authenticators are not allowed at AAL3, due to its exportability, it may be better to add "Syncable cryptographic" in the AAL2's permitted authenticator types of the table for to make easily understandable.	Add "Syncable cryptographic" in the AAL2's permitted authenticator types.
19	63B	3.1.1.2	14	771	"the secret" should be stated as "the password", since "memorized secret" has been rephrased to "password".	Rephrase "the secret" as "the password".
20	63B	3.1.6	25	1140	"Single-factor" may be missing before "cryptographic authentication".	Add "Single-factor" in the beginning of the sentence.
21	63B	3.1.7	26	1140	"Multi-factor" may be missing before "cryptographic authentication".	Add "Multi-factor" in the beginning of the sentence.
22	63B	3.1.7.1	27	1153	Users are able to use private keys for WebAuthn synced to another device without user verification under certain conditions (e.g., if a WebAuthn RP is setting UV as discouraged and the authenticator is not conducting user verification), which means that syncable (cryptographic) authenticators can be also applied to single-factor cryptographic authentication.	Copy the paragraph regarding syncable (cryptographic) authenticators (line 1153-1155) to section 3.1.6.1 Single-Factor Cryptographic Authenticators.
23	63B	3.1.7.3	27	1171	When subscriber-controlled wallets are used for authentication with protocols such as WebAuthn, as referenced in the annex of the EUDI Wallet's draft implementation act for integrity and core functionalities, then the wallet itself can be considered as a cryptographic authenticator (whether multi-factor or single-factor depends on if the wallet asks for activation factor upon the authentication or not). This subclause should add it, as besides using federation protocol, such as SIOP, for authentication.	Add sentences as follows: "When a subscriber-controlled wallet is used for cryptographic authentication with protocols such as WebAuthn, the wallet itself is to be considered as a cryptographic authenticator. Whether the wallet is a multi-factor or single-factor cryptographic authenticator depends on if the wallet asks for activation factor upon the authentication or not."
24	63B	3.1.7.4	28	1192	What's currently written in this section is already mentioned in the line 1153-1155.	Remove this section, or add a new section which also explains about other "syncable" authenticators.
25	63B	3.2.7	34	1411	"the secret" should be stated as "the password", since "memorized secret" has been rephrased to "password".	Rephrase "the secret" as "the password".
26	63B	4.1.3	41	1665	The example of a subscriber having a multi-factor authenticator from a social network provider, considered AAL2 without identity proofing" is difficult to understand. Also, in the latter part of the sentence, the statement of "would like to use that authenticator at an RP that requires IAL2" is confusing, as it sounds like referring to federation.	Change the sentence to as follows: "For example, the subscriber may have an own multi-factor authenticator, and would like to use that authenticator at an RP or IdP, that requires AAL2."
27	63B	4.2	42	1686	"Recovery codes" are used as a method of "account recovery" at various web services. However, "saved recovery codes" can be considered as a look-up secret (as even described in the line 815-817 of 63B) and so for "issued recovery codes" as OOB authenticators, and the CSPs (web services) are conducting authentication (a claimant is proving possession and control of the code issued and bound to a subscriber account). Therefore, recovery codes should not be listed as methods of account recovery, or at least be stated that they are alternative authentication methods without phishing resitance.	Remove the saved/issued recovery codes from the sections under 4.2, and only leave "recovery contacts" and "repeated identity proofing" as methods of account recovery. Or, state that saved/issued recovery codes are alternative authentication methods, and also address that they do not have phishing resitance.
28	63B	4.2	42	1686	Regarding the account recovery, it is better to recommend subscribers to bind multiple authenticators and use password managers/syncable (cryptographic) authenticators, which consequently reduce the possibility of the subscribers to conduct account recovery.	Add sentence(s) in the section which recommends (as SHOULD) CSPs to encourage subscribers to bind multiple authentication methods that fulfils desirable AAL and also to use password managers/syncable (cryptographic) authenticators (for AAL2 and below), which reduce possibility of a subscriber conducting account recovery.
29	63B	4.2.2.1	45	1766	There is no requirement of issuing (or binding) multi-factor authenticator upon identity proofing in 63A, and therefore what is written in this sentence is incorrect.	Remove the sentence. Then, insert "To recover an account that can authenticate at a maximum of AAL1" in the beginning and "repeated identity proofing" in the end of the next sentence.
30	63B	4.2.2.1	45	1768	"subscriber accounts at AAL1" is confusing.	Rephrase as "an account that can authenticate at only AAL1", which aligns with the descriptions of recoveries at AAL2 and AAL3.
31	63B	8.2.1	67	2304	Eventhough this part is now explaining usability considerations for typical usage without a password manager, the consideration of user experience by supporting copy and paste functionality is assuming that a user is using password manager.	Add a new line before "user experience during entry of the password" (line no. 2302) as "Usability considerations for usage with a password manager include:".
32	63B	Appendix A.	83	2764	"passwords" is included in "password" (formally "memorized secret").	Rephrase "passphrases, PINs, and passwords" as "passphrases and PINs".
33	63B	B.2	87	2893	It is unclear to whom the key management requirements for syncable (cryptographic) authenticators are applied to. Also, it is difficult for RPs/verifiers to investigate whether each users' secret keys are managed in such manner if the keys are stored in sync fabrics.	Clarify that the requirements of the key management is for sync fabric providers, and/or modify the listed requirements as something to be announced to the users from the RPs/verifiers.

34	63B	B.5	91	3034	WebAuthn's multi-factor syncable authenticators can conduct local authentication with not only activation secret but also with biometric characteristic.	Modify "require users to input an activation secret" with "conduct local authentication with activation factor (e.g., activation secret and biometric characteristic), if used as multi-factor cryptographic authenticator"
35	63B	B.6	92		For the sixth column of the "Mitigations", "syncing fabric" may be a mistake of "sync fabric".	Replace "syncing fabric" with "sync fabric".
36	63C	10.4	99	3333	"Credential" might be a mistake of "Attribute Bundle".	Replace "Issuance of a Credential to a Digital Wallet" with "Issuance of an Attribute Bundle".
37	63C	10.4	99	3335	"credentials" might be a mistake of "attribute bundles".	Replace "credentials" with "attribute bundles".
38	63C	10.4	99	3357	The use case described here is identity proofing, not authentication.	Replace "When the subscriber needs to authenticate to an RP" with "When an RP wants to conduct identity prrofing of the subscriber".
39	63C	10.4	99	3358	"credential" might be a mistake of "attribute bundle".	Replace "credential" with "attribute bundle".