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:	*FIDO Alliance*
Name of Submitter/POC:	*Jeremy Grant and Andrew Shikiar*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	4.2	42	1686	Regarding account recovery, it is better to recommend subscribers to bind multiple authenticators and/or use password managers/syncable authenticators, which consequently reduce the risk 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 and/or use password managers/syncable authenticators (for AAL2 and below), which reduce risk of a subscriber conducting account recovery.
2	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 authenticators can be also applied to single-factor cryptographic authentication.	Copy the paragraph regarding syncable authenticators (line 1153-1155) to section 3.1.6.1 Single-Factor Cryptographic Authenticators.
3	63B	2.5	10	678	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 for to make easily understandable.	Add a new row to the table on this page for "Synced authenticators " in the AAL1 and AAL2 permitted authenticator types that notes they are Permitted for these AALs and Not Permitted for AAL3
4	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"
5	63B	B.2	87	2893	We believe the key management requirements here are intended to apply to sync fabric providers, but some have suggested they might be interepreted as applying to the RP. Since an RP does not have a way to know how a sync fabric is implementing these requirements, it would make sense to clarify that they apply to sync fabric providers.	Clairfy that this section is intended to apply to sync fabric providers.
6	63B	Appendix B	87	General	Besides the cryptographic authenticators, authentication secrets of other types of authenticators can also be synced (e.g., password and TOTP in a password manager). To avoid confusion (such as people thinking this covers syncing of OTPs), it may be better to rephrase "syncable authenticators" with "synced cryptographic authenticators" in the guidelines.	Replace all "syncable authenticators" with "synced cryptographic authenticators" in the guidelines.
7	63B	General (And Appendix B)			Industry has settled on the term "synced" passkeys rather than "syncable" - we would suggest a global change in the document to the use of the term "synced"	Change all "syncable" references to "synced"