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: Beyond Identity

Name of Submitter/POC: Dean H. Saxe

Email Address of Submitter/POC [redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	3.1.7.1	40	1153	The language used in this section has led many readers to the incorrect assumption that all syncable authenticators, particularly passkeys, meet the requirements for AAL2. Without a careful reading of appendix B, readers may be lead to incorrect conclusions. NIST should more clearly document that syncable multifactor cryptographic authenticators are always AAL1 and MAY be compatible at AAL2, if, and only if, the requirements in Appendix B are achieved.	Some cryptographic authenticators, referred to as “syncable authenticators,” can manage their private keys using a sync fabric (cloud provider). These syncable authenticators SHALL BE compatible at AAL1, if the requirements for AAL1 and this section are met. AAL2 compatible syncable authenticators MUST meet the additional requirements for using syncable authenticators located in Appendix B.
2	63B	3.1.7.1	40	1158	Syncable authenticators will often cache the activation secret presentation, thus allowing an activation secret to be entered at a time before the authentication event. The text should clarify that caching the activation event is sufficient at AAL1, but incompatible with AAL2. Updated language in 3.2.10 would also suffice to capture this nuance.	Each authentication operation that uses the authenticator SHALL require the activation factor to be input. For authenticators that are usable at AAL2 and AAL3, caching of the activation secret, such as unlocking the syncable authenticator with a password or biometrics prior to the authentication event, SHALL NOT be permitted. Verification of the activation secret for authenticators usable at AAL2/3 MUST be required in response to the authentication event.
3	63B	B.1	87	2888	The guidance in this section is designed to enable syncable authenticators to be usable at AAL2. The introduction should clearly state this in order to reduce the confusion about when a syncable authenticator is usable at AAL2.	This appendix provides additional guidelines on the use of syncable authenticators in order to be usable at AAL2. Syncable authenticators that do not meet these guideliness SHALL NOT be usable at AAL2.
4	63B	B.3	88	2935	In the absence of an attestation, these flags may be modified and may not accurately represent the state of the authentication event. As with any client provided data, the data should not be trusted unless it is demonstrated to be trustable. In the WebAuthn ecosystem, this trust is established through attestation. This additionally impacts the statements on p91 in lines 3037 to 3041. As of today, popular, commercially available synced authenticators send the UV flag, even when the activation secret was cached at a time in the past.	This section describes certain flags in the WebAuthn specification that federal agencies acting as RPs should understand and interrogate when building their syncable authenticator implementations to align with NIST AAL2 guidelines. In the absence of attestation, or other to be defined trust signals, these flags should be treated as untrusted in the same manner as any other client-supplied data. Services MAY use these flags as part of their assessment of the authentication event, but MUST NOT trust this data in the absence of attestation.
5	63B	B.3	90	2982	Modify the language to state that attestations may not be required, but should be requested, collected, and assessed if made available by the authenticator.	RPs SHOULD attempt to collect attestations, where they are made available by authenticators. RPs SHOULD use attestation to determine the level of confidence they have in a syncable authenticator where such data is made available.