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:	*L3Harris Technologies*
Name of Submitter/POC:	*Allen Westley*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
1	63B	Syncable Authenticators	11	5 thru 12	Syncable authenticators allow for key sharing across devices, but risks like unauthorized key use or sync fabric compromise are not sufficiently addressed. More specific controls are necessary to mitigate these risks for public-facing services.	Strengthen controls by requiring detailed logging and monitoring of key sync actions in public-facing services. Add a specific requirement for secure backup processes and the use of AAL2-equivalent MFA for accessing synced private keys.
2	63B	Wallet-Based Authentication	12	8 thru 20	Wallet-based authentication is described, but attribute bundles are not fully explained. The explanation should better clarify how the bundling process integrates with overall authentication mechanisms to provide strong phishing-resistant claims.	Expand the section to include more detailed examples of how "attribute bundles" work in practice and outline additional security controls for bundling sensitive attributes in wallet-based authenticators. Suggest requiring MFA to activate wallets for attribute retrieval.
3	63C	Federation Protocol	14	18 thru 24	The federation protocol involving wallet-based authentication mechanisms lacks specific controls on signing and verification processes. It needs more precise guidelines to ensure phishing resistance and prevent unauthorized assertions.	Add more specific guidelines on the signature verification processes in wallet-based authentication and require cryptographic proofs of audience-restricted assertions. Recommend that agencies ensure proper implementation of phishing-resistant cryptographic signatures for wallet-based systems.