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:	*Yubico*
Name of Submitter/POC:	*Joe Scalone*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63C	5.1	77	2731	"...the issuer MAY make available an online mechanism to determine the validity of a given attribute bundle, such as a status list queryable by the RP"	Given the validity of the attribute is critical to the overall process, we suggest the issuer SHOULD make an online mechanism to determine the validity of the attribute
2	63C	5.5	73	2604	Fixing a spelling mistake - "...bundle singing public key of the CSP"	Singing should be signing
3	63B	3.2.4	32	1337-1339	Attestation can provide a hihger level of confidence in the origin of the source of the authenticator and limit a potential attack vector. "Verifiers in federal enterprise systems SHOULD use attestation features to verify the capabilities and source of authenticators. In other applications, attestation information MAY be used as part of a verifier's risk-based authentication decisions."	Verifiers in federal enterprise systems SHALL use attestation features to verify the capabilities and source of authenticators. In other applications, attestation information MUST be used as part of a verifier's risk-based authentication decisions.
4	63C	5.6	74	2631	In order to preserve the privacy of the user, they should have the choice to see and choose the attributes that are provided to the CSP . "The subscriber-controlled wallet SHOULD provide a means to selectively disclose a subset of the attributes in the attribute bundle from the CSP."	The subscriber-controlled wallet SHALL provide a means to selectively disclose a subset of the attributes in the attribute bundle from the CSP.