Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*FPKIMA*
Name of Submitter/POC:	*India Donald, Wendy Brown*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base		ii	149	typo identify instead of identity	
	63B	4.1.2	7	468	Is this a typo? Was it supposed to say Authenticators rather than Verifiers? Verifiers operated by or on behalf of federal government agencies at AAL1 SHALL be validated to meet the requirements of [FIPS140] Level 1	If not, please explain the relationship between verifiers and FIPS 140 Level 1
	63B	4.1.3	7	473	30 days seems excessive to allow a single user session to last	
	63B	4.2.2	9	534-535	What does it mean for a Verifier to be validated against FIPS140? (Is there a conflict in the term verifier as it is used in 63B vs Verifier as defined in the base document?)	
	63B	4.3.2	11	600	What does it mean for a Verifier to be validated against FIPS140?	
	63B	6.1.3	46	1736-1739	It is unclear if the example would meet the requirement for an RP that requires IAL2 as having an AAL2 authenticator doesn't make the IAL any stronger than what was initially used to meet IAL1.	Please clarify
	63B	6.2	47	1773-1776	Does the following intend to make the ability to suspend a mandatory requirement & does this include for PIV? The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	Please confirm
	63C	5.2.2	21	815	in the following statement - could the IdP really sign the RP's software statement or would the RP sign it? Does the IdP sign it about the RP for conveying the info to the subscriber or is this statement for use of the IdP? Software statements are lists of attributes describing the RP software, cryptographically signed by an authority (either the IdP itself, a federation authority as in Sec. 5.1.2, or another trusted party).	Please clarify - looks like from RFC7591 - the IdP signs it for the subscriber info
		5.4.2	27	1011	Typo - pick one or the other "from with"	
	63C	10.2.1	64	1977	the term "associated entity" needs clarification	