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:	*N/A*
Name of Submitter/POC:	*Tom Clancy*
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63C	4.9	63	2347	Any metadata or values required to support the functionality of selected security extensions must be included.	Add: "10. Any claims or values required to achieve functional and security interoperability of core protocol or extensions required to achieve the tailored FAL."
2	63C	4.11.1, 10.12	67, 104	24,633,532	Reference is to FAPI 2.0 Security profile, which is intended to secure RESTful APIs and does not include the OIDC identity layer.	Replace reference on page 105 with a different FAPI profile that includes OIDC, iGov, MITRE's Enterprise Mission-Tailored Profiles, or a list of technical profile options.
3	63C	3.12	34	1561	Missing Assertion Protection mechanisms: sender-constraining assertions	Add section for sender-constraining tokens (assertions) to make it available as tailoring; add as "Recommended" to FAL2 column in Table 1. Federation Assurance Levels; add reference to new section in Table 3. Mitigating Federation Threats as another mitigation for assertion manufacture or modification.
4	63C	3, 3.4.2	9, 20	628, 970	"Profile", as in a "profile of a protocol" is used without introduction or glossary entry. "Profile" is also used to describe user data collected incrementally.	Recommend shifting the document's final paragraph on p104, lines 3531-3533, to the opening of Section 3 and include a description of technical profiles as an outcome of FAL tailoring to provide interoperability at known assurance levels, and semantic profiles for metadata value consistency.