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:	
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63A	2.1.2	8	583	Providing training "consistent with the requirements" be general enough that some of these identity task challenges would be pushed further down the line	For more specificity, referencing another NIST guidance or documentation might enforce a higher level of rigour
	63A	2.4.1.1	10	665	The capitalization of FAIR, STRONG, and SUPERIOR could be confusing as acronyms	Consider treating the adjective as part of a proper noun, or use a different marking (e.g., italicized) might be cleaner
	63A	2.4.1.1	11	674	Typo: List has two items labelled with 1	
	63A	3.1.2.1	18	897	"data washing" does not appear to be a common term for this activity	Use a more common term or drop the term altogether
	63A	3.1.8	25	1145	Confirmation (and Contiuation) Codes have no requirement for proving that the code came from the CSP, which could result in confusion or uncertainty for the applicant	Include a SHOULD statement providing a mechanism / information for applicants to verify that the code originated from the expected CSP
	63A	4.2.4	41	1688	It seems potentially insecure that failure in cryptographic validation still allows for the evidence to be considered valid	Potentially remove that clause, or provide some clarification around why this would be useful/secure.
	63A	4.4	49	1920	Evidence Collection row IAL3 has inconsistent formatting, and does not exactly reflect the requirements from the text	Correct for consistency in formatting and information
	63A	6	53	2007	Infrastructure threats are not considered in this document, which is fair but seems lacking in that some ramifications of infrastructure threats should be considered	
	63A	Appendix C	86	2815	"authenticator" and "multi-factor authenticator" do not appear in the Glossary	Either include the definition, or note that the terms appear in the Glossary in 63B
	63B	3.1.1.2	13	730	The requirement is not entirely clear, in which system it is referring too, or if it means that subscribers should just not write down the password	
	63B	5.2	51	1977	Typo: "special considerations apply to session management and reauthentication" appears to be duplicated in the sentence	Remove the second occurrence of the phrase
	63B	B.4	90	2994	Typo: There is no Table 5, and it not clear which table it is supposed to be mapping to	
	63-Base	2.1	10	646	Typo: "relyin party"	"relying"
	63-Base	3.7	50	1800	Typo: "Could" should not be capitalized	
	63C	2	3	464	Typo: "a a given FAL"	"a"
	63C	2.3	6	542	Typo: missing a word	Potentially should be "the assertion shall be audience restricted"
	63C	3.1.2	11	686	It is not entirely clear if "component controlled by a single subscriber" refers only to wallets or to something more general	
	63C	3.6	23	1099	Typo: "A subscribers attributes"	"subscriber's"
	63C	3.10.1	29	1300	Typo: "The attackers assertion"	"attacker's"
	63C	3.11.2	32	1408	This subsection has no normative statements despite discussing an important concept in a normative section.	Add or convert existing statements to add normative weight (even if it is just CAN or MAY)
	63C	3.13	32	1408	This subsection has no normative statements despite discussing an important concept in a normative section.	Add or convert existing statements to add normative weight (even if it is just CAN or MAY)
	63C	3.12.2	35	1504	"Issuer" appears to be used throughout the document as a direct synonym for IdP, which clutters the term space without adding apparent value. It is also misaligned with the usage of the word "issuer" in existing literature from the SSI space (which is actually described in 800-63-4 main)	Consider deprecating the "issuer" terminology through this document
	63C	3.13	36	1552	Typo: "be presented own its own"	"on its own"
	63C	3.15	37	1585	The term "bound authenticator" should be defined	Add definition either in the glossary (ideal) or in the prose (minimal)
	63C	4.1	43	1718	Only use of IdAM in the publication; was this the intended term and if so providing an entry in the glossary would help	
	63C	4.5	44	1731	It could be clearer for the steps in the figure (Fig 6) to be numbered and map directly to the written description of the process flow	
	63C	4.9	63	2330	The terms "subject [identifier]", "issuer [identifier]", and "audience [identifier]" are introduced as synonyms (per the accompanying parenthesis) of "subscriber, IdP, and "RP" but are not used afterward	Consider renaming to "subscriber identifier", "IdP identifier", and "RP identifier" to reduce term clutter
	63C	4.9	63	2346	Does the required inclusion of the key identifier mean that many assertions already satisfy the FAL3 requirement in 2356?	
	63C	4.11.1	65	2422	Typo: "varies form one protocol"	"from"
	63C	5.2	69	2522	It could be clearer for the steps in the figure (Fig 13) to be numbered and map directly to the written description of the process flow	
	63C	5.3	71	2540	This phrase indicates that the trust agreement is between the RP and the CSP for subscriber-controlled wallets, without indicating the permissible scope of that agreement. Under this wording, it is possible for the agreement to mandate specific wallets only, which could exclude competing or future wallet options.	Clarification should be provided to indicate that the trust agreement covers a class of services (wallets meeting certain capabilities or specifications) to be more broadly inclusive of new technologies or implementations in the future.
	63C	5.4.1	73	2596	This paragraph should be broken out to a new subsection and (ideally) expanded. In the current that, this paragraph is the closest piece of content in the document that addresses the important topic of "attribute bundle" revocations for user-controlled wallets (which relates to 4.6.4 for the general-IdP version). However, this topic has greater implications than account deprovisioning, as CSP might plausibly want to change some attributes without deleting the entire subscriber account	
	63C	5.5	73	2604	Typo: "attribute bundle singing public key"	"signing"

	63C	5.8	74	2648	The terms "subject [identifier]", "issuer [identifier]", and "audience [identifier]" are introduced as synonyms (per the accompanying parenthesis) of "subscriber", "subscriber-controlled wallet", and "RP" but are not used afterward	Consider renaming to "subscriber identifier", "IdP identifier", and "RP identifier" to reduce term clutter
	63C	5.11	77	2734	The SHALL statement indicates that subscriber-controlled RP accounts can not be pre-provisioned. There is no clear rationale for why the wallet accounts should be controlled differently.	Some rationale should be provided for clarification, or this paragraph should be altered/removed.
	63C	6	78	2742	This section should touch more on a security issue that becomes more pronounced with the addition of wallets and attribute bundles, namely: the use and proliferation of stale, revoked, superceded, or otherwise outdated credentialing information	
	63C	9	94	3213	Typo: "could learn that that the"	"that"
	63C	Appendix B			There is no entry in the glossary for wallet / subscriber-controlled wallet, which could be useful to define for more clarity	