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:	*NIST*
Name of Submitter/POC:	*Elaine Barker*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	1.2		434	It would be useful to indicate that there are multiple assurance levels for each function	
		2.1		646	Change "relyin" to "relying"	
		2.2.1		683	Use "Provision the subscriber account with"	
		2.3.1		700	Probably should say that a PIN is a password	
		2.3.1		715	Insert a comma after "keys"	
		2.3.1		717	Are there other kinds of activation secrrets besides passwords?	
		2.3.1		728	Do you want to add that a password cannot be used as the second factor with a biometric characteristic? Though it could be used as a third factor.	
		2.5		887	Define digital wallet	
		3		930	It would be useful to mention that the DIRM process is explained below.	
				1021	Where is the guidance on assigning Low Moderate and High?	
				1033	Where are discussions on tailoring?	
				1120	All impacted what?	
				1190	Insert a semicolon after "harm", "income", and "housing"	
				1266	Insert "damage" after "further"	
				1268-69	Change "results" to "result". Insert "damage" after "further"	
				1294-99	There is something not quite right about this sentence when the parenthetical statements are removed.	
				1307	Insert "the" before "Combined"	
				1367	A sentence referring to Table 1 and summarizing its purpose is needed.	
				1387	A sentence referring to Table 2 and summarizing its purpose is needed.	
				1398	A sentence referring to Table 3 and summarizing its purpose is needed.	
				1411	s "xAL" defined?	
				1462	Insert a comma after "benefits"	
				1464	Are both of these models explained anywhere?	
				1495	Change"process and seeks" to "process that seeks" (otherwise, the sentence says the the "risks...seeks"	
				1505	Remove the last "of"	
				1511	I think the comma before "but" isn't needed	
				1522	Change :consistent" to either "to be consistent" or "consistently"	
				1545	Insert a comma after "usability"	
				1569	Insert "the" between "to" and "internet"	
				1575	Insert "the" after "whether"	
				1601	Insert a comma after "resistance"	
				1606	Remove the second occurrence of "is intended to address"	
				1612	Remove the comma before "but"	
				1639	Remove the comma after "evidence"	
				1693	Insert a comma before "as appropriate"	
				1697	Change "as" to "that are"	
		Table 4, 1st row			Change "successfully proof" to "successfully provide proof of their identity"	
		Table 4, 2nd row			Change "proof" to "provide proof of identity"	
		Table 4, row 4			Change "Percentage" to "percentage of failures"	
		Table 4, row 5			Change "proofing" to "the identity proofing process"	
		Table 4, Fraud per proofing type			Change "by" to "for" and insert "identiy" before "proofing"	
		Table 4, Health desk calls (per type)			Insert "identity" before "proofing"	
				1731	Insert "an" before "informad"	
				1747	Change to either "have disproportionally damaging impacts" (remove "a") OR "have a disproportionally damaging impact" (make "impact" singular")	

				1800	Decapitalize "Could"	
				1836	Insert "the" before "NIST"	
				2066	I don't think a comma is needed after "account"	
				2119	insert "the" after "has"	
				2173	This definition is written as if ithe authentication secret allows the attacker to impersonate the subscriber rather than deterring the attacker from doing so. Reword. Maybe something like "A generic term for any secret value in an authentication protocol that deters an attacker from impersonating the subscriber." The second paragaph also needs some work along the same lines.	
				2188	Reword to something like "...to authenticate the subscriber asociated with the account,..."	
				2212	Insert "a" before "federation"	
				2224	Insert a comma after "card"	
				2240	The use of a KEM (e.g, Kyber) should be considered. This could require revising of the definition Would need to be coordinated with the team developing 800-227	
				2439	Since when is an organization or company considered as a person. Consider using the term "legal entity"	
				2455	Use "via" instead of "through"?	
				2546	This definition needs rewording! Consider the definitions for private key and secret key in the various key-management documents. Also, should "encapsulation" be mentioned here to accommodate a KEM?	
				2551	Insert "The" at the beginning of the definition (e.g., The operation of set of operations...)	
				2596	Do we want to add "encapsulate" here to accommodate a KEM?	
				2702	Insert "to" before "create" . The "to" before "verify" could be removed	
				2724	The comma after "population" should be a semicolon as well as the remaining commas in the definition	
				2735	Should this definiton be update? The latest update of TLS is 1.3.	

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:	*NIST*
Name of Submitter/POC:	*Elaine Barker*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	1	1	380	Make it very clear at the beginning of the document that this document considers a subject to be a real person, natural person (the glossary that provides this information is at the end of the document. You might include a list of words that are human beings: natural person, real-life person, individual, applicant, claimant, etc.	
2	63A	1	1	386	However, this use of subject may not be a human being.	
3	63A	1.1	1	402	Is a subscriber always a person (i.e., human being)?	
4	63A	2.1.1	6	532	Provide an example of an attribute. Refer to 2.2?	
5	63A	2.1.1	7	540	Provide a link to where the pathway is discussed.	
6	63A	2.1.3	8	611	Why REQUIRE a remote unattended process. I would think that "may" would be more appropriate.	
7	63A	2.4.1.1	10	665	Insert "a rating of" before "FAIR"	
8	63A	2.4.1.2	11	686	Change to "...considered as STRONG evidence"	
9	63A	2.4.1.3	12	708	Change "SUPERIOR" to "as SUPERIOR evidence"	
10	63A	2.4.1.3	12	719	Add "at an appropriate security strength using an approved algorithm/method"?	
11	63A	2.4.2	12	734	Insert "that" after "confirm"	
12	63A	2.4.2.1	13	742	Insert "that" after "confirming"	
13	63A	2.4.2.2	13	753	Remove the comma; The verification needs to be made at an appropriate security strength using an approved algorithm/method	
14	63A	2.5.1	14	791	Remove the comma before "but"	
15	63A	2.5.1	14	793	What is a micro transaction?	
16	63A	2.5.1	14	806	Insert "that" after "ensure"	
17	63A	3.1.1	16	837	The commas after "available", "IAL", and ") should be semicolons. The last phras has a problem; maybe insert "the" before "use" and remove the comma after "use"?	
18	63A	3.1.1	16	842	"The" could precede "types"	
19	63A	3.1.1	16	845	Insert :the' before "training". Insert "that" after "technologies"	
20	63A	3.1.1	16	Footnote 1	I don't think the comma after "referee" is needed.	
21	63A	3.1.1	17	851	Remove the comma before "and"	
22	63A	3.1.2.1	18	910	It should be recognized that an applicant may have recently changed phones/devices	
23	63A	3.1.2.1	18	919	What is a transaction velocity?	
24	63A	3.1.3.1	21	1003	Reference where this is discussed	
25	63A	3.1.9	26	1177	Entering 64 bits manually is ridiculous! How about entering as hex characters (0..9A..F)? Alternatively reword as "Continuation codes shall be determined using at least..."	
26	63A	3.1.9	26	1181	Define throttling here (limiting the number of retries)	
27	63A	3.1.9	26	1182	Define hashed form; is it covered more thoroughly in 63B? Do you mean just hash function or could it also be a MAC or XOF?	
28	63A	3.1.10	26	1188	Insert "that" after "repudiate"	
29	63A	3.1.10	27	1204	Insert "that" after "event"	
30	63A	3.1.11	27	1228	Insert "a" before "subscriber's"	
31	63A	3.1.11	28	1244	What is a non-real-world user?	
32	63A	3.1.11	28	1251	Explain 1:N matching (e.g., in a footnote)	
33	63A	3.1.11	28	1252	1 out of 1000? Explain the terminology.	
34	63A	3.1.11	28	1259	Insert "that" after "confirm"	
35	63A	3.1.12	29	1283	"of" needs to be changed to "by" (even if already used in tthe sentence). This is not about inspecting the agent or trustee	
36	63A	3.1.12	29	1290	Is the reader expected to know what .10 is intended to be?	
37	63A	3.1.12	29	1295	Insert "a" after "implement"	
38	63A	3.1.13.1	31	1356	The issue is not meeting the requirements (exactly), it's not being able to prove their identity using the same procedures as most others. Reword?	
39	63A	3.1.13.3	33	1428	Consider removing "for identity-proofing applicants" in the last line (for simplicity).	
40	63A	3.1.13.4	34	1444	Insert "The" in front ot "use"	

41	63A	4.1.7	38	1580	Insert "the" after "records"	
42	63A	4.1.7	38	1583	Remove the first "to" in "to prior to"	
43	63A	4.1.7	38	1590	Change "orders" to "order"	
44	63A	4.1.8	38	1597	Insert "that" after "ensure"	
45	63A	4.1.8	39	1604	Insert "the" after "records"	
46	63A	4.2.1	40	1658	Why use SHALL for unattended remote? SHOULD would be more appropriate	
47	63A	4.2.4	41	1673	Insert "that is" before "evidence"	
48	63A	4.2.4	41	1675	Insert "an" before "interrogation"	
49	63A	4.2.4	41	1678	Insert "that is" before "able"	
50	63A	4.2.4	41	1679	Insert "the" before "physical" and "presented"; insert "a" before "visual"	
51	63A	4.2.4	41	1682	Inset "the" before "physical" (twice)	
52	63A	4.2.5	41	1699	Insert "the" before "presented"	
53	63A	4.2.6.1	42	1708	Insert "an" before "automated"	
54	63A	4.2.6.1	42	1709	Change "being" to "that is"	
55	63A	4.2.6.1	42	1721	Insert "the" before "evidence"; remove the comma before "or" and after "evidence"	
56	63A	4.2.6.1	42	1730	See the comments for 2 (b) (line 1721)	
57	63A	4.2.6.2	43	1741	Change to "identity evidence that is presented"	
58	63A	4.2.6.3	43	1765	Change to identity evidence that is presented"?	
59	63A	4.2.6.3	43	1768	Insert "the" before "evidence"	
60	63A	4.2.6.3	44	1772	Insert "the" before "evidence"	
61	63A	4.2.6.3	44	1774	How about "..biometric evidence other than a stored facial image on the identity evidence or in records..."	
62	63A	4.3.1	44	1795	Change "collocated" to either "co-located" (with a hyphen) or "colocated" (with no hyphen)	
63	63A	4.3.2	45	1798	Insert a comma after "3"	
64	63A	4.3.2	45	1799	Insert "evidence" after "better)" and "SUPERIOR"	
65	63A	4.3.3	45	1804	Change "it" to "the CSP"	
66	63A	4.3.4	45	1816	Change to "an interrogation of the digital..."	
67	63A	4.3.4	45	1818	Insert "the" before "physical" and "that is" before "able"	
68	63A	4.3.4	45	1820	Insert "the" before "physical" and "presented" and "a" after "through"	
69	63A	4.3.4	45	1823	Insert "the" before "physical" (twice)	
70	63A	4.3.4	45	1826	Insert "a" before "cryptographic"	
71	63A	4.3.5	46	1838	Insert a comma before "if available"	
72	63A	4.3.6	46	1840	Insert an apostrophe in "applicatants" to show ownership (i.e., applicant's)	
73	63A	4.3.6	46	1845	Insert "the" before "evidence"	
74	63A	4.3.6	46	1848	Insert "the" before "evidence"	
75	63A	4.3.6	46	1850	Insert "the" before "identity" and "authoritative"	
76	63A	4.3.7	46	1858	What is meant by non-natural materials. Maybe provide some examples.	
77	63A	4.3.7	47	1862	Insert "that" after "ensure"	
78	63A	4.3.7	47	1870	Insert "the" before "session"	
79	63A	4.3.7	47	1873	Remove the first occurrence of "to"	
80	63A	4.3.7	47	1878	Change "for" to "of"	
81	63A	4.3.10	48	1913	Reword to "...protected session with the user, the CSP SHALL compare a biometric sample collected from the applicant to the one collected at the time of proofing, prior to issuance of the authenticator.	
82	63A	4.3.10	48	1914	Insert "during this process" after applicant" and change "issuance of the authenticator" to "issuing or enrollng the authenticator"	
83	63A	4.3.10	48	1917	Insert "or enrolling" after "issuance"	
84	63A	4.4	49	Table 1	Evidence collection: Put "or" on a separate line from "1 FAIR + 1 STRONG"; consider changing "+: to "and"	
85	63A	4.4	49	Table 1	Evidence validation: For IAL1, place a period after "doc". Define "doc." and "auth." somewhere	
86	63A	5.1	50	1930	You are recommending a randomly generated identifier ? This is looking like a password. This is crazy!	
87	63A	6	54	Table 2	Social engineering: Insert "who is" after "attacker in the 3rd column:	
88	63A	6	54	Table 2	Video or Image Injection Attack: The second column needs rewording	
89	63A	6.1	55	Table 3	Social Engineering: Insert "a" before "validated"	
90	63A	6.1	55	Table 3	Video or...: Running matching what?	
91	63A	6.2	56	2029	External to what? The organization?	
92	63A	7.1	57	2042	Insert "that" after "attributes"	
93	63A	7.1	57	2045	Change "Further" to "Furthermore"	
94	63A	7.1	57	2047	Remove the comma after "use"	
95	63A	7.1.1	57	2059	Insert a hyphen between "third" and "party" Also applies to line 2062	
96	63A	7.1.1	57	2066	Insert a comma before "and"	

97	63A	7.2	58	2070	Change "The" to "These"	
98	63A	7.2	58	2073	Remove the comma after "transactions"	
99	63A	7.3	58	2091	Change the comma after "proofing","assertion," and "migrations" to semicolons	
100	63A	7.4	59	2121	Insert "that" after "event"	
101	63A	7.5	59	2131	Change "should a problem occur" to "if a problem occurs"	
102	63A	8	61	2173	Insert "the" before "context"	
103	63A	8	61	2174	Change "considering" to "that considers"	
104	63A	8	61	2192	Do you mean "increasing" or "improving"?	
105	63A	8	61	2197	Maybe use "a significant time lapse"?	
106	63A	8.1	62	2226	Insert "an" after "Use"	
107	63A	8.1	62	2228	Also, limit acronyms and abbreviations	
108	63A	8.2	63	2253	Add something like "so that acceptable forms of evidence can be determined and advertised."	
109	63A	8.2	63	2254	Insert "that' after "ensure"	
110	63A	8.2	63	2255	Insert "with" after "users"	
111	63A	8.2	63	2259	Insert "An" before "explanation"	
112	63A	8.2	64	2269	Insert "where identity proofing can be provided" after "location(s)"	
113	63A	8.2	64	2276	Insert hyphens bafore and after "over"	
114	63A	8.2	64	2281	Insert "obtaining" before "reminders"	
115	63A	8.2	64	2296	And what type of trusted referee service can be provided?	
116	63A	8.3	65	2323	Insert "use" before "applicant"	
117	63A	8.3	65	2334	Also include an approximate time frame when verification would be expected	
118	63A	8.3	65	2340	Also whether they can provide an authenticator and guidance about what would be acceptable	
119	63A	8.3	67	2409	How? Give an example?	
120	63A	9	69	2443	Change to "guidance below"	
121	63A	9	69	2469	Change "digital divide" to "something like "technology challenges"?	
122	63A	9.2	71	2514	Insert "a" before "comparison"	
123	63A	9.2	71	2516	Insert "a" before "successful"	
124	63A	9.2	71	2528	"who' seems to be referring to "child". How about "...such as a parent who can vouch for the identity of a minor child "	
125	63A	9.2	71	2531	Insert "that have been" before "identity"	
126	63A	9.3	72	2554	Insert "to be" before "established"	
127	63A	9.3	72	2563	Remove the comma after "technologies" and "algorithms", and change "which" to "that"	
128	63A	9.3	72	2573	Change " , which" to "that"	
129	63A	9.3	73	2585	Insert "identity" before "proofing"	
130	63A	9.4	74	2612	Insert a comma after "e.g."; remove the other two commas.	
131	63A	9.4	74	2630	"for" is not necessary here	
132	63A	A.1, A.2, A.3	78, 80,	Tables 4, 5, and 6	Fill in the missing words	
133	63A	A.1	78	Table 4	What is a micro deposit? What is an MNO? Should "intended origin" be "claimed origin"?	
134	63A	Appendix C	85	2796	Assertions seem to also be made about an applicant.	
135	63A	Appendix C	85	2799	Provide examples	
136	63A	Appendix C	85	2808	Insert "that are" before "bound"	
137	63A	Appendix C	86	2839	Insert "the" before "angle"	
138	63A	Appendix C	86	2843	I think the claimant is a person in this document, isn't it?	
139	63A	Appendix C	87	2845	Change "reached" to "contacted"?	
140	63A	Appendix C	88	2884	You forgot sex, e.g., women	
141	63A	Appendix C	90	2950	Since when is an organization or company a person. How about "legal entity"	
142	63A	Appendix C	91	2997	I wouldn't use "messages" or "files". You might use all or part of the definition in SP 800-57 Part 1.	
143	63A	Appendix C	92	3019	Insert "the" before "identity"	
144	63A	Appendix C	92	3031	Change "subscriber" to "subscriber's real-life identity"	
145	63A	Appendix C	93	3064	Insert "and" before "reputation"	
146	63A	Appendix C	94	3085	Is a subscriber always a person?	
147	63A	Appendix C	94	3087	Change "and authenticators" to "and information about the authenticators"	