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:	*Self*
Name of Submitter/POC:	*Lorrayne Auld*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	2.1	10	640	Remove extra dash at beginning of Subscriber definition	
2	63-Base	2.2	11	669	Volume A doesn't use a hyphen between identity and proofed nor is it used in other parts of this document (see line 827 as an example).	Recommend changing to 'identity proofed'
3	63-Base	3.4.4	44	1652	Suggest adding example locations (repository, organization's web site) of where the practice statements and DIAS should reside for RPs to review.	
4	63A	1.2	2	427	Spell out PII	
5	63A	2.1.1	6	530-531	Example states IAL2 so suggest collecting two pieces of evidence. The OR implies one piece of evidence is collected.	
6	63A	2.1.1	6	532	Suggest “core attributes” to make it more specific than just the term “attributes.”	
7	63A	2.1.1	6	538	Credible source is defined in lines 768-774 and recommend that a reference to section 2.4.2.4 be included in this sentence.	
8	63A	2.1.1	6	538	Credible validation sources isn’t defined. While this is an example, suggest listing a couple of authoritative (DMV) and/or credible sources (AAMVA). See comments for section 2.4.2.4 lines 765-767	
9	63A	2.1.1	7	546	Page 9 line 629 calls a phone number a digital address. Please use this term instead of an address for phone number and reference to section 2.2).	
10	63A	2.1.2	7	555	Is the Proofing Agent trained by the CSP? Who trains that individual and is there a requirement that that individual must be proofed at the level or higher if the applicant being identity proofed? Is a Proofing Agent only used for IAL1?	
11	63A	2.1.2	7	559	Same comment applies here regarding training for a Proofing Agent in line 555.	
12	63A	2.1.2	7	573	Are the attributes provided by the Applicant Reference only the core attributes? I would think core plus any others required.	
13	63A	2.1.2	8	582-584	CSP wouldn’t train the Applicant Reference yet the language implies it does	
14	63A	2.1.3	8	602	Kiosk for IAL3 SHALL be in a secured and monitored physical location to avoid tampering of the kiosk. If this is for IAL2, what mechanisms are in place to prevent altering and/or tampering of the CSP-provided device?	
15	63A	2.4	10	649	Government agencies won’t accept expired evidence for identity proofing even if it expired the day before (though I wish they did). Expired is okay for IAL1 and possibly IAL2 but NOT for IAL3. Suggest lifting the language from line 736.	
16	63A	2.4.2.2	13	752	Add fraud detection as part of the automated document validation process.	
17	63A	2.4.2.4	13	765-767	I view AAMVA either as a credible source or a trusted intermediary for physical driver's licenses. To my knowledge, not all states participate in the DLDV service. I don't know enough about the DLDV service but it makes me think it's an attribute service querying the authoritative sources for the state DMVs in an ICAM architecture. See https://www.aamva.org/it-systems-participation-map?id=594 for latest list of partitipating states. AAMVA's DLDV architecture is here: https://www.aamva.org/getmedia/cb603635-3454-4331-b2c6-288d894f7fc4/AAMVA-DLDV-Overview-for-Customers.pdf	Move AAMVA to line 774.
18	63A	2.4.2.4	13	765-767	AAMVA may eventually become an authoritative source for mDLs if and when the States look to them as the issuer of the Digital Trust Service (DTS). mDL implementation and DTS participation by state is here near the bottom of the page: https://www.aamva.org/jurisdiction-data-maps	
19	63A	2.5.1	14	804-805	Is captured video the same as liveness detection for remote unattended?	
20	63A	2.5.1	15	813-816	Mention fraud detection tools MAY be used o help perform the biometric comparison.	

21	63A	3.1.1	16	831	Is anyone updating the practice statement template from revision 3 to revision 4?	I suggest you reach out to MITRE and request a Word version of MITRE's templates. It could be helpful to update them to revision 4 once it's no longer draft.
22	63A	3.1.3.2	22	1046	Shouldn't one require the CSP to publish their privacy policy which MUST include the collection and/or storage of attributes, capture of biometrics, and what they are used for? Also, it should be published where it's easy to find. A good example is https://www.id.me/privacy	
23	63A	3.1.5	23	1092	Suggest adding risk based analytics tools to this list	
24	63A	3.1.7	25	1130	Suggest changing SHOULD to SHALL especially for IAL2 deployment	
25	63A	3.1.7	25	1140	Suggest having the privacy policy published and available on both the Agency's website and the external CSP.	
26	63A	3.1.8	26	1163	Invalidate the confirmation code upon its use or when it expired (whichever comes first)	
27	63A	3.1.11	29	1274	Suggest PAD with liveness detection capabilities.	
28	63A	3.1.13.1	31	1353	Change 'Referees' to 'Referee'	
29	63A	3.1.13.1	31	1379	Suggest annual refresher training and recertification for all Trusted Referees of the CSP.	
30	63A	3.1.13.1	31	1387	Add a bullet to indicate that the Trusted Referee SHALL be identity proofed at the level or higher of the applicant.	
31	63A	3.1.13.1	31	1387	Add a bullet regarding how one revokes the privileges of a TR when they are no longer employed by the CSP or no longer are in the role of a TR	
32	63A	at section 4	36	1505	Suggest changing viable to desirable.	
33	63A		36		Suggest TWO pieces of FAIR evidence OR ONE piece of STRONG or SUPERIOR that contains a facial portrait. Then the rest of the text in this section makes more sense to me (send a confirmation code if only FAIR evidence is presented).	
34	63A		36	1523	Suggest a new paragraph here. This sentence implies remote unattended identity proofing. If I'm in person, why would the CSP send a code to me?	
35	63A		37	1533	Items one and two suggest use of fraud detection tools.	Recommend using stronger language for items one and two
36	63A		37	1543	If I present FAIR evidence only, what government identifier is used? Especially if I present a utility bill and a bank statement as my FAIR evidence.	Government identifier I would think would be used for STRO
37	63A		37	1553	I can't think of a single bit of identity evidence presented that would be linked to a mobile device. So this confirmation code implies mailing the code via USPS.	I suggest re-writing this sentence to make it clearer regarding the confirmation code. I don't see how it can be associated with the evidence presented.
38	63A		38	1570	Protected channel = encrypted channel? If yes, recommend using encrypted.	
39	63A		38	1598	Add same language regarding FISMA Moderate as stated on lines 1617-1618 (Malware Protection, Admin Specific Access Controls, and Software Update processes)	
40	63A		39	1620	Add in here lines 1604-1610 for recording the session via kiosk.	
41	63A		40	1642	I suggest adding a sentence regarding the CSP will add a record that the applicant was successfully identity proofed at IAL1 at a specific date and location (remote, in-person) as part of their audit log.	
42	63A		40	1648	How does one have confidence that I'm in possession of said evidence without doing a biometric comparison? I fear a data breach following these revised guidelines. Traffic on the Dark Web illustrates how these fraudsters steer away from the biometric capture following IAL2 revision 3. I no longer have the proof to back this though as I had to give up all my deliverables when I retired from MITRE. I would be VERY CAREFUL and personally wouldn't want to have that risk for IAL2. I don't have an issue with using this language for IAL1.	Strike out without the use of biometrics.
43	63A		40	1648	I will go one step further. What about all the existing CSPs who already at great expense went through IAL2 conformance criteria for revision 3? I don't think these CPSs will be very happy with the striking of this requirement. Again, I strongly suggest you strike out the without the use of biometrics from IAL2. The risk outweighs the benefits from a fraud detection/prevention to NIST's reputation.	
44	63A		41	1675	Items (a) and (b) suggest use of fraud detection tools.	Recommend using stronger language for items one and two
45	63A		42	1711	Non-biometric pathway introduces risk for IAL2. For the remote attended session, what level of training does the proofing agent have to detect a video injection attack, deep fake, etc. if no tools are used to do the comparison of the biometric samples provided by the applicant?	
46	63A		42	1720	What FAIR evidence has a facial portrait? Are you thinking a school ID or a work badge (NOT a PIV or CAC)? I would include an example here.	

47	63A		42	1723	Suggest striking from asynchronous to the end of the sentence. If comparison isn't done in real-time, how do I know that the applicant at the time of proofing truly matches the biometric portrait on the evidence presented at the time of proofing? Also, if this comparison is done and the proofing agent deems that there is NOT a match, how is that subscriber then revoked access and who determines what fraud that fraudulent subscriber did?	
48	63A		42	1733	Suggest striking from asynchronous to the end of the sentence.	
49	63A		43	1740	I assume that this confirmation is performed in real-time.	Suggest using language stating that confirmation of a subscriber's ability to access the evidence digitally is performed in real-time
50	63A		44	1774	Can you please provide an example of STRONG and SUPERIOR evidence that doesn't have a facial portrait?	
51	63A		44	1795	the kiosk or device SHALL be in a controlled facility (not in the middle of a shopping mall)	
52	63A		44	1799	Suggest this collection be One piece of STRONG and two pieces of FAIR and remove (or better) at end of the line	
53	63A		44	1799	Suggest adding another line that states "Two pieces of STRONG, or"	
54	63A		46	1835	I think from a risk perspective the SHOULD becomes a SHALL to query an authoritative or credible source.	
55	63A		46	1838	Suggest adding fraud detection checks in this section	
56	63A		46	1840	Change applicants to applicant's	
57	63A		48	1906	I would add a (g) that states that the devices are owned by the CSP and resides within a controlled space where tampering of the equipment cannot be performed by an individual.	
58	63A		48	1916	From a risk perspective, I suggest changing this MAY to a SHALL	
59	63A		49	1920	Revise IAL3 evidence collection to be 1 STRONG and 2 FAIR or 2 STRONG, or 1 SUPERIOR	
60	63A		49	1920	Add fraud detection to Physical and Digital Evidence row for all IALs	
61	63A		50	1939	Suggest adding language regarding where the CSP records this information for the subscriber.	
62	63A		55	2017	Social Engineering row. Suggest user behavior (copy/paste info, pause at fields the true applicant will know such as SSN, DoB, etc) will also help detect a fraudster.	
63	63B	3.1.3.3	21	967	Comment: I don't foresee giving up landline phones (non-VOIP) in the foreseeable future. This method is preferred for our aging population as well as those who don't have a smart phone (but may have a flip phone as well as a landline).	
64	63B	4.2.1.3	44	1743	What happens if a subscriber goes through the entire set of saved recovery codes? I am thinking of those with failing memory (elderly) who may need to do an account recovery or password reset multiple times per month. I'm thinking this is where the CSP suggests to the subscriber to have a recovery contact in place (if that person hasn't already designated someone else as their recovery contact) as well as repeating a portion of the identity proofing process for AAL2 or higher (though this adds in a negative user experience	
65	63B	4.2.3	45	1789	Suggest adding the option to send an account recovery notification to the recovery contact.	