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:	*Dept. for Science, Innovation & Technology*
Name of Submitter/POC:	*Michael Animashaun*
Email Address of Submi:	[redacted]

Comment #	(Base, 63A,	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	General			General - Overall a very comprehensive document that is set out clearly but it is a hard read. Recommend that the text could benefit from being reviewed by content editors to make it less complex and more straightforward for readers. Many readers may not have the technical background or the understanding of the authors, so simplifying the language would make it easier to understand topics that are by nature complex and help improve take up of the guidelines. Providing use cases to illustrate topics would also help. The Identiy Proofing (A) and Authentication (B) Guides are laid out clearly and comprehensively cover the risk management and fraud management considerations. Although the Federation and Assertion (C) guidelines outline Wallets and Attribute Bundles the content of those sections is extremely dense and very difficult to follow and undertstand and the meaning tends to get lost in techncial jargon. It might be helpful to think about what outcomes are neeeded in using Wallets and Attribute Bundles and then structure the text to demonstrate how to achieve those outcomes. I also think the documents would benefit from example use cases that demonstrate how the concepts you outline will occur in the real world. For example; show how the concepts you outline in the guidelines apply to storing a driver's licence in a wallet.	
2	63-Base	General			Risk Methodology - The Guidelines set out the importance of understanding and assessing the riisks and outline an appropriate risk methgodology. However, one observation is that a risk assessment, is by definition a judgement based on a range of factors e.g. usability; security, fraud threat, operational etc and in some instances the right thing to do is contrary to the guidelines or may not fully implement the guidelines to the letter. By specifying that users "shall" meet the requirement, could in some instances be contradictory to a judgement based on a risk assessment. Suggest the guidelines should provide flexibility for risk assessors to make appropriate judgements rather than force them to meet a requirement that might not be achievable. This is covered in part at 2.4 Tailored requirements but doesnt	
3	63-Base	General			A Identity Proofing and Fraud - in the main, the differing requirements for IAL and fraud management are laid out. However, I think different interpretations could be applied to some of the current labels, for example digital	
4	63-Base	General			C Federation and Assertions - I think the concepts of wallets and assertionss section is outlined but it contains a lot of detailed, complex techncial explanations that are very difficult to relate to their application in everday terms. Suggest it might be useful to provide a summary or overview of wallets and assertions in non techncial language before getting into techncial detail or alternatively provide the details as separate links to the	
5	63-Base	General			**Syncable Authenticators - understand the need but not sure the risks of sharing authenticators across devices outweigh the benefits or how organisations can apply syncable authenticators and still meet the requirements for AAL2 Strong**	
6	63-Base	Introduction	2	375	Although these are Digital, standards, it would be useful to call out if they are are suitable for adopting for identity proofing in non digital channels: ie Face to Face and	
7	63-Base	2.1	10	639	Consider re-naming the Applicant to "user" NIST differentiates between the Applicant - not yet identity proofed and the "subscriber" who has completed identity proofing - does the distinction add any value?	
8	63-Base	2.3.1	13	735	Disagree that KBV are not an acceptable secret, it depends on the type of KBV. For example asking the user to input an automated random time bound OTP is a form of KBV. It is also secret as only the recipient knows	
9	63-Base	2.5	16	822	Figure 3 - it may be helpful to provide a real world example of the different stages in the models - to help explain which organisations might perform which role and an understanding of who does what, as readers unfamiliar with the concepts and terms used may struggle	
10	63-Base	3.3.2.1	35	1358	GAP _Specify what type of checks are required for each level of assurance	

11	**63-Base**	3.4	40	1492	This section is really helpful for organisations to identify how they can tailor requirements based on a risk assessment. However, the guidelines advise that organisations "Shall . . ." and that indicates the requirements must be followed strictly. What htakes	
12	**63A**	2.1	5	515	Its not clear if these guidelines support creation of an account with authenticators, without the need to require	
13	**63A**	2.1.2	7	555	Its not clear whether you see the Proofing Agent role as being required for all identity proofing transactions or whether its primarily for IAL3?	
14	**63A**	2.2	9	624	Suggest middle name is an optional requirement - not all users use their middle name, some may have multiples and depending on the auth source the middle name may not be captured	
15	**63A**	2.2	9	626	This assumes users always have to have gov issued evidence but some may not have any e.g. vulnerable users but they may have access to other non gov evidence e.g. bank accounts, so suggest you change it to a “Unique Identifier” rather ythan government identitfier	
16	**63A**	2.2	9	628	In this context the purpose of the address seems to be to facilitate adminsitarion of the ID proofing process rather than treating the address as a core attribute of the users identity? What happens if the user doesn’t have an address e.g. homeless person - they would not be able to meet this core attribute so fail the ID check	
17	**63A**	2.2	9	623	Is there a specific reason why you have not listed date of birth as a core attribute - as this is key attribute in differentiating between individuals who may have the same name and/or same address? Have you considered other potential attributes that could be considered core e.g. photograph, biometrics	
18	**63A**	2.4.1.1	10	664	The evidence section is still predicated on physical evidence and the evidence being issued to a postal address but this seems a step back given that these are digital guidelines. Physical evidence has a role but suggest more considerationi is needed for identifying and validating strong digital evidence that is not rerliant on physical docuimentationoir a physical address. For example, Passport records that cointain a digital image. In addition the reliance omn physical evidence will disadvantage people who are vulnerable and may not have the physical evidence or be able to obtain it, so coiuld never meet the identity checking requirements.	
19	**63A**	2.4.1.3	12	717	Suggest you de-couple crypto and F2F checks for the following reasons: It is possible for identity evidence with crypto features to meet STRONG, on line via without requiring a physical F2F challenge As these are digital identity guidelines, why emphasise the need for a F2F check, you should be exploring digitial aternatives rather than seeking reliance on physical F2F interactions	
20	**63A**	2.4.1.3	12	729	Disagree that a physical security check is as strong as a cryptographic check - for example a fraudster could manipulate a document image or details but not be able to replicate a chip embedded in the document.	
21	**63A**	2.4.2.2	13	748	Some digital evidence can meet STRONG requirements without needing cryptographic features. For example a Passport record is evidence of identity and contains identity attributes that are validated including the digital image a The evidence may not have cryptographic features but require techniques like PKI and symmetric hash or use of verifiable credentials to access the evidence	
22	**63A**		13	760	Suggest this should be strengthened to include a requirement that the issuing source has to protect the integrity of the evidence and attributes and ensure they are current.	
23	**63A**		14	792	Micro Transaction = Micro deposit	
24	**63A**		14	795	F2F	
25	**63A**		14	799	Remote- attended	
26	**63A**	2.5.1	15	817	They have removed KBV!!	
27	**63A**			817	This section relies on users having evidence of their identity or being able to use digital technology. It doesn’t identify methods for users who have no evidence and are digitally illeterate, very often the vulnerable and marginalised members of society. However, they may have a government or social security record and whilst KBV is a weak verification solution it does provide an opportunity for those disadvantaged users to prove their identity to at least IAL1.	
28	**63A**	3.1.3.2	22	1036	Supports my stance on use of NINO as an identifier (identity attribute) but not evidence of the identity	

29	**63A**	3.1.10	28	1246	IThese rate may be achievable in lab test settings but in reality there are many variables that contribute to a false non match rate e.g. users digital knowledge, lightinng, original photo image (rather than an embedded digital image) that make achieving this rate in reality alsmot impossible - suggest you apply an acceptable range e.g. 10%	
30	**63A**	3.1.12	29	1281	What about evidence validation where the evidence is a digital record e.g. a record with a financial institution and you validate the identity attributes provided by the claimed identity with the bank as an authoritative or credible source as outlined 2.4.1.1. - Line 666?	
31	**63A**	3.1.13.2.	32	1398	The list of requirements for trusted referee users advises that can validate identity attributes but makes no reference to verification the user in this scenario. I assume the trusted referee can't verify the identity of the applicant but might be useful to make that point explicitly?	
32	**63A**	3.1.13.4	34	1446	One of the key issues for the vouch process in meeting the IAL requirements is that a vouch can confirm or validate an applicant's identity attributes but cannot meet the verification requirements, as verifications is reliant on checking the applicants image against evidence issued by a trusted 3rd party that contains an image or biomtyeric, that the applicant doesn't have, which is why they have a applicant referee. Suggest you include a section of verification when a trusted referee or applicant referee is used	
33	**63A**		34	1466	We have questioned the value of asserting who is an acceptable relationship because the operational impact in checking the relationships status and/or the willingness of the trusted person to provide validation the identity is not guaranteed and they may charge. In addition due to the increase in digital many applicants have no direct contact with individuals e.g. bank managers and/or these type of roles in their daily lives.social	
34	**63A**	4.1.3	36	1528	Its not clear how you define and manage evidence where that evidence is a digital record. For example if a user has a bank account they could provide their bank account details and we could check those against the bank as an authoritative or credible source but there is no "evidence' as such that the user has to provide, they can self assert the attributes but they are validated if the bank confirms they are correc.	
35	**63A**	4.1.8	38	1594	Ity might be helpful to include a requirement that CPS has to implement procedures to minimise collusion between the applicant and the proofing agent. For example they could collude to create fake or synthetic identities.	
36	**63A**	4.1.10	39	1621	Is it possible for an applicant to create an account with an AAL without proving their identity?	
37	**63A**	4.2.6.1.	42	1707	Equivalent to GPG45 Score 2 - physical security check	
38	**63A**			1725	For IAL2 - NIST require 2 pieces of evidence and a physical address	
39	**63A**			1727	What happens if the user doesn't have a physical address e.g. they couch surf or the address is their normal residence but are currently at university?	
40	**63A**	8.2	64	2303	Pre=poultraionis a fraud risk as it implies the data is pulled from an existing source and so presenting to someone who is not the genuine user discloses PII and is contrary to Privacy Guidelines	
41	**63A**	8.3.		2304	Be mindful of disclosure of process or evidence requirements - can be used by fraudsters to determine what is needed	
42	**63B**	1	1	382	Can you please clarify if the authenticator identifier is separate from the identity identifier and can be issued separately. For example, is it necessary for the CSP to issue the authenticator identifier to the RP when the user authenticates? THat seems to have minimal value for the RP but I can understand issuing the identity identifier	
43	**63B**	3	11	686	I understand the need for inclusion but suggesting that multiple users can authenticate with a single device seems very risky and I dont understand how you can bind the auth and identity if multiple people have access?	
44	**63B**	3.1.1	12	702	Not clear on when a password is centrally verified and used as an auth factor and when it is considered an activation secret - examples would be helpful	
45	**63B**		13	715	This is an example of the tension between security and usability. A Longer password is more secure but usability studies consitently demonstrate that requiring users to set passwords with 8 - 15 characters is seen as complex and difficult to memorise.	

46	**63B**			732	KBA can be compromised and where everyone has a photo ID doc e.g. National ID Crad they are not needed. However, I believe KBA still have a place as part of the identity check, especially for vulnerable or disadvantged users who dont have photo identity docs like Passports or driver's licences. Biometrics are also not ideal - they can be stored on a native device as an authenticator but there is no link between the user and the biomteric - anyine could have stored the fingerprint or face on the device	
47	**63B**	3.1.7.4	28	1192	I can see the attraction for syncabale authenticators but doesnt syncing them by definition defeat the purpose of having a strong authentication credential bound to a single identity?	
	63B	3.2.3	30	1275	The text refers to IAPAR (Impostor Attack) but the document does not include the attack presentation classification error rate (APCER) or bona fide presentation attack classification error rate (BPCER) for biometric systems, which are recvognised as the industry standard for measuring biomeric performance?	
48	**63B**	3.2.8	34	1429	What is the value in having a physical mechanism as well as capturing a face biometric - how does the physical authentication demonstrate its the genuine person more than the face biometric? If the face biometric is corrupt then a fraudster would also just complete the physical mechanism	
49	**63B**	3.2.9	35	1431	Please provide examples	
50	**63B**	3.2.10	35	1461	We set requirements for autentication and account re-set	
51	**63C**	2.1	4	500	Suggest you also include Verifiable Credentials as an example of an assertion to a RP as its is becoming more widely adopted as a mechanism for managing PKI.	
52	**63C**	2.3	6	540	Unsure if this is an achievable requirement - agree that ideally it should be projected from injection attack but the threat is constantly evolving so its possible to have defences in place but they may not be 100% successful	
53	**63C**			542	Missing a "be",	
54	**63C**			630	This implies the roles are separate and autonomous but roles could be jointly performed by a single organsiation that creates and manages the account so performs the role of a CSP, at the same time as performing the role of an IdP.	
55	**63C**			679	It is possible for a subscribers attributes to be stored in the CSP record and then shared to the wallet, either as a credential e.g. Driver's Licence or the attributes linked to that cedential	
56	**63C**	3.2.3		Fig 1& 728	This is a very complex section that is diffult to read and understand. Would benefit from a diagram showing a use case and how the diiferent roles interact in that use case.	
57	**63C**	3.2	14	793	This sentence would add more value if it was highlighted earlier in the paragraph	
	63 C	4.6.7	58	2199	This section touches on accounts that have been termnimnated and are no longer accessible overall the document provide detail on re-authentication and revocation. However, there isn't any reference to inactive users - ie those users who may have created an identity and/or an authentication credential but haven't used it or logged in for some time. There is a risk that if these are not managed it will result in significant number of outdated and unused identities and credential. Suggest it will be helpful to state how long an identity/credential	