Comment Template for: NIST SP 800-63-4 Suite (Draft 2)

Please submit responses to dig-comments@nist.gov by October 7, 2024

Organization:	*DirectTrust Community*
Name of Submitter/POC:	*Scott Stuewe*
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, 2.1, 2.3, 9.1			[GM] In regards to identity resolution there still remains some possible conflict with regards to context of scope. In Section 1.1, Pg. 1, Ln. 392, the scope is "unique individual within the context of the population of users served by the CSP or online service". In Section 2.1, pg.5, ln. 509, the scope is "unique identity in the population served by the CSP and is a real-life person". In 2.3, Pg. 9, ln. 640 the scope is "accurately distinguish an individual within a given population or context". Finally within 9.1, pg. 70 ln. 2483 the scope is "unique individual within the population served by the identity service". It is our belief that the scope should be consistent and encompass both the CSP and RPs that operate with that CSP, likely under a Federation Authority.	Suggest a consistent statement of scope for Identity Resolution [JM] that 1) has a living person as a minimum bar when identity verification is performed, 2) uniquely resolves against all living persons as its scope unless a narrower scope can be applied based on a risk assessment and 3) does not create duplicate identities within the CSP's scope.
2	63A	2.1.2			[JM] Best practice guidance for Trusted Referees and Applicant References seems necessary in order to prevent misuse.	Historically, professionals such as healthcare providers and attorneys have had an implicit role as Trusted Referees. To level set, including policies about Trusted Referees and Applicant References in practice statements would be a good first step, as would be best practice guidance materials relating to implementation of these roles.
3	63A	2.1.3	8	597-598	[GM] Remote Attended Proofing seems to describe a process outside of the control of the CSP given that the line states "location and devices .... are not in control of the CSP."	Suggest a change to allow the CSP to offer Remote Attended as a possible option with language such as "location and devices .... may or may not be controlled by the CSP" or clarify the definition of devices here as a CSP may use a back-end device for validation of a credential presented.
4	63A	2.1.3	8	593-594	[GM] Remote Unattended Proofing seems to describe a process outside of the control of the CSP given that the line states "location and devices .... are not in control of the CSP."	Suggest a change to allow the CSP to offer Remote Unattended as a possible option with language such as "location and devices .... may or may not be controlled by the CSP" or clarify the definition of devices here as a CSP may use a back-end device for validation of a credential presented.
5	63A	2.2	9	627	[GM] Various Statutes put restrictions around use of the SSN or at least requirements when being used, such as need to indicate if mandatory or voluntary, authority to collect, intended user etc. SSN may not be the best example to use without a note to indicate its inclusion does have additional requirements.	Possibly remove SSN as an example or place a footnote that would indicate the need for the collecting party to be aware of the requirements for use of SSN, especially if the CSP is a Federal Agency or is under contract of one or a direct reference to 3.1.3.2. [JM] Additionally, differentiating between cases for the number itself as opposed to the card, as well as whether the related practice of using SSN and KBV to invoke use of an antecedent event, that may not require notification of proofing, is still permitted or not.
6	63A	2.2		627	[JM] TIN is listed as an example of a government identifier in 2.2, but is not listed in the example evidence Appendix and it is not clear how TIN can be validated and verified throughout the federal realm (certainly not beyond it).	Suggest removing TIN from the example in 2.2.
7	63A	3.1.13.3	33	1423	[GM] The Applicant reference description implies that the applicant reference may be an existing CSP user that has been proofed at some level.	Indicate that the Applicant Reference may be an existing CSP user that has been proofed to at least the same level as the Applicant.
8	63A	4.3.2	45	1799	[GM] The type of Strong/Fair evidence required matches 4.2.2 but the verbiage is different while adding no additional value.	If 4.2.2 and 4.3.2 are in fact the same evidenciary requirements then have the verbiage the same
9	63A				[JM] Introduction of digital address as a core attribute in lieu of physical address introduces potential fraud opportunity, especially when notification of proofing can also be sent to an email address or phone number.	Would be helpful to include examples of when a digital address may be used instead of a physical address--e.g. when there is no verifiable physical address for an individual and a digital address may be used instead. However, last known physical address is likely practiceable even for those with housing insecurity. Similarly, clarify when notification of proofing to an address other than a verified physical address is sufficient (mobile number billed to an individual's name). Demonstration of control of a mobile number or email address should not constitute a verified address to which notification of proofing can be sent--without mailing to a verified address, consumers are unable to become aware of identity theft. Recommend emphasizing when address is not a current one and that notifications of proofing preferentially sent to a current address, if newer address found.
10	63A				[JM] Practice statement requirements do not include contact information for CSP and if embedded in a trust agreement practice statement information may not be available to consumers.	Consider requiring that CSP's practice statements are readily available to users and include a contact point for consumers and RPs to report potential fraud to the CSP. Or to request biometric deletion as in line 1232.
11	63A			895	[JM] Data washing requirements are a nice addition for privacy protection.	Consider whether an informative example would help ensure these requirements are met.
12	63A			910	[JM] SIM swap detection requirement is somewhat ambiguous.	Consider specifying required when phone number is used as one piece of evidence or in notification of proofing
13	63B	2.1.2	5	524	[GM] The term "approved algorithm" is ambiguous and is not a specifically defined term in the document or appendix.	Define the term as a defined term directly in the Appendix or provide a brief definition here with a reference to Approved Cryptography as defined in Appendix D
14	63B	2.2.2	7	577	[GM] The requirement that FIPS 140 is a mandatory requirement ONLY for Federal agency authenticators creates a two tier AAL2 authenticator.	We applaud NIST's recognition that there may be multiple ways to meet AAL2 without FIPS certification, we want to confirm that this was the intention. For example, is the intention that a CSP may utilize authenticators that have been certified under alternative programs to FIPS as long as they are transparent in publishing support for the same.
15	63B	Appendix A.3	84	2826	[GM] This is not a well structured sentence.	Since user's password choices are often predictable, attackers are likely to guess passwords that have previously proven
16	63B	Appendix B.2	87	2896	[GM] The storage of private keys that are cloned or exported are required to be encrypted but no restrictions or requirements are placed around this.	Recommend an indication that the encryption strength be at least that of the strength of the protected key.
17	63C	3.10.3		1356	[DJ] "The IdP and RP SHALL delete personal identity information in the subscriber account and RP subscriber account (respectively) upon account termination, unless required otherwise by legal action or policy." Ambiguous with respect to what entity can establish policy that would override the SHALL requirement. Is it IdP policy or RP policy or some other entity's policy?	Consider a more specific statement of which entity types can establish the overriding policy.