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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*Nonoe*
Name of Submitter/POC:	*Ryan Palmer*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	5.4.2	28	1111	Break out Evidence Validation and Core Attribute Validation	These are 2 different steps, breaking them out brings clarity. This is how they are broken out in IAL 3 section of document
1	63A	5.4.3	28	1067	The current guide for document validation does not mandate validation of evidence details to confirm the authenticity of documents. Using inadequately validated or fictitious documents for the verification (comparison) process jeopardizes the entire proofing process. Attack Concern: Attackers with moderate sophistication can produce fake documents, including those with security features. Document validation should extend beyond visual inspection or examination of security features, as these methods can be easily bypassed or replicated by moderately skilled actors. Additionally, training for document inspection and technical detection may not be consistently implemented, and often has vague requirements. Document validation should not rely on non-issuer records. For example, using phone account records (name, address, DOB) to validate a driver's license based on matching information (name, address, DOB) is not recommended. Instead, validation should be conducted through records provided by the Department of State, Tribal authority, DMV, or a third party holder of issuing records (AAMVA). Where validation of key attributes is not possible, CSPs should document deviations and appropriate mitigations based on the issuing body's limitations. NIST should be informed of these challenges, and should provide implementation guidance on appropriate validation where this data is not accessible E.G. if some states do not provide such information. NIST should work to ensure sources of issuing records for key evidence types (passports, drivers licenses, state IDs, tribal IDs, military IDs) are available to CSPs to validate evidence in a secure manner without compromising user privacy. Note: Core attributes do not have to precisely match a single piece of evidence. However, evidence should be validated based on the information obtained from it. For instance, if an individual's address has changed, the evidence should be validated against issuing records using the old address (as printed on the evidence). Other records (e.g., phone records) can be used to validate the current address attribute, which would then become a core attribute.	Clearly outline minimum requirements to validate Strong/Superior evidence details against issuing records. Potential language could be: The CSP shall validate the key attributes on the presented document against the issuing authority or against issuing records held by a trusted source to validate the document matches the document officially issued. (1) Document Details collected from evidence: Issuer (state, entity, et cetera), document ID, Expiration Date or as captured in the implementation guide for the particular evidence. (2) Personal Details collected from evidence: Given Name, Surname + at least one other personal field such as Date of Birth, Full Address, Place of Birth or as captured in the implementation guide for the particular evidence
2	63A	5.5.3.1	30	1168	The current guide for document validation does not mandate validation of evidence details to confirm the authenticity of documents. Using inadequately validated or fictitious documents for the verification (comparison) process jeopardizes the entire proofing process. Attack Concern: Attackers with moderate sophistication can produce fake documents, including those with security features. Document validation should extend beyond visual inspection or examination of security features, as these methods can be easily bypassed or replicated by moderately skilled actors. Additionally, training for document inspection and technical detection may not be consistently implemented, and often has vague requirements. Document validation should not rely on non-issuer records. For example, using phone account records (name, address, DOB) to validate a driver's license based on matching information (name, address, DOB) is not recommended. Instead, validation should be conducted through records provided by the Department of State, Tribal authority, DMV, or a third party holder of issuing records (AAMVA). Where validation of key attributes is not possible, CSPs should document deviations and appropriate mitigations based on the issuing body's limitations. NIST should be informed of these challenges, and should provide implementation guidance on appropriate validation where this data is not accessible E.G. if some states do not provide such information. NIST should work to ensure sources of issuing records for key evidence types (passports, drivers licenses, state IDs, tribal IDs, military IDs) are available to CSPs to validate evidence in a secure manner without compromising user privacy. Note: Core attributes do not have to precisely match a single piece of evidence. However, evidence should be validated based on the information obtained from it. For instance, if an individual's address has changed, the evidence should be validated against issuing records using the old address (as printed on the evidence). Other records (e.g., phone records) can be used to validate the current address attribute, which would then become a core attribute.	Clearly outline minimum requirements to validate Strong/Superior evidence details against issuing records. Potential language could be: The CSP shall validate the key attributes on the presented document against the issuing authority or against issuing records held by a trusted source to validate the document matches the document officially issued. (1) Document Details collected from evidence: Issuer (state, entity, et cetera), document ID, Expiration Date or as captured in the implementation guide. (2) Personal Details collected from evidence: Given Name, Surname + at least one other personal field such as Date of Birth, Full Address, Place of Birth or as captured in the implementation guide.