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

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

Organization:	Notarize, Inc.
Name of Submitter/POC:	Yehoshua Silberstein
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	4.1.1	8	466	In Section 4.1.1, the diagram illustrates a sample IAL2 flow. This flow: a. Includes an enrollment code, though enrollment codes are no longer required per Sec. 5.1.6; and b. Does not include the proofing notification now required by Sec. 5.4.5.	For the purpose of the diagram's clarity: a. Remove the enrollment code as it is no longer required by Sec. 5.1.6; and b. Incorporate the proofing notification that is required by Sec. 5.4.5.
2	63A	4.3.4.4	13-14	630-632	Sec. 4.3.4.4 states that core attributes that are on a piece of evidence that has already been validated per Sec. 4.3.4.1 do not require further validation. However, Sections 5.3.3 (IAL1) and 5.4.3 (IAL2) require that all core attributes obtained from the eivdence must be validated against authoritative or credible sources. Can you please confirm that these sections are not contradictory because by Sec. 4.3.4.4 requiring the validation of the evidence against an authoritative or credible source, this would also be considered a validation of its attributes against an authoritative or credible source? Meaning that for both IAL1 and IAL2, confirmation that the credential is genuine in accordance with Sec. 4.3.4.1 would qualify as both validation of the evidence and its attributes?	
3	63A	5.4.2.1	27	1068	a. For IAL1, Sec. 5.3.3 requires fair pieces of evidence to be visually insepcted by trained personnel. The IAL2 standards require the presentation of a fair piece of eivdence (Sec. 5.4.2.1), but do not discuss how to validate the fair evidence. Does the fact that strong eivdence is being electronically validated obviate the need to validate the fair evidence beyond confirming that it is consistent with the strong evidence? b. Additionally, the validation process in IAL1 for fair evidence seems to be limited to manual validation of phsyical pieces of fair evidence. Is there a concept of digital fair evidence and/or electronic validation similar to the validation of strong or superior evidence?	
4	63A	5.1.6 & 5.1.7	21-22	863-904	The requirements for validating and verifying an address are unclear, especially as they relate to digital addresses. Addresses that are documented in the presented identity evidence are validated and verified through validation and verification of the evidence. Digital addresses (phone number or email) however, would generally not be present in a credential and would require a separate step for validation and verification and the standards are unclear as to how to perform the validation and verification. First, attribute validation is defined in line 2205 of 800-63-4 as “the process or act of confirming the a set of attributes are accurate and associated with a real-life identity.“ Arguably, confirming the existence of a possessive attribute such as an address does not validate it as belonging to a real-life identity. But an applicant who demonstrates possession of a digital address has both validated that the address is associated with an identity and verified it as associated with their identity. This argument can be applied to enrollment codes to allow them to function as both validation and verification of a digital address. However, the enrollment code standards in Sec. 5.1.6(1) seem to require an enrollment code be sent to an already validated address. Additionally, the requirements for proofing notifications in Sec. 5.1.7(1) say that a proofing notification must be sent to an address of record that is preferably not the one that received the enrollment code. In line 1607 of 800-63-4, an address of record is defined as “The validated and verified location (physical or digital) where a subscriber can receive communications using approved mechanisms.” Taken together, this implies the possiblity of having a digital address that was validated and verified without relying on an enrollment code. This possibility is also supported by the fact that the new standards only require proofing notifications for IAL2 identity proofing but do not require enrollment codes. However, the standards do not provide another method for validating and verifying these addresses other than via an enrollment code.	
5	63A	5.3.3	27	1064	For validation at IAL1, Sec. 5.3.3 allows for visual inspection by trained personnel. Can you please confirm whether these trained personnel have to meet the requirements of Sec. 5.1.9 for trusted referees? Or is there a different set of requirements for trained personnel acting under Sec. 5.3.3?	