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

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

Organization:	*DocuSign*
Name of Submitter/POC:	*Pete Seeger*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1a	63A	5.3.3		1068	"The CSP SHALL validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel." Our comments relate to this requirement as it applies to IAL1. We interpret this language to require that human personnel shall visually verify the piece of evidence systematically. As such, we believe that this requirement brings complexity, cost, and delay in the validation process without taking into account progress made in automated verification technologies to date. For example, in most cases, when the image is of good quality, automated verification technologies will have better accuracy than a human verification.	For IAL1, we believe NIST should amend the guidance to require human validation only for cases where the automated verification has not delivered a sufficient level of confidence in the outcome – e.g., the probability associated with the proposed outcome by the automated verification system is below a certain threshold. That being said, we believe, automated verification should only be trusted in cases where the system ensures that the capture of the image (or the video stream) is performed at the moment of the verification. If we have misinterpreted the language, we request clarification of the intent.
1b	63A	5.3.3		1068	"The CSP SHALL validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel." In addition to the comments provided above, we request clarification of this language as it applies to IAL2. Based on our interpretation, we believe the intent is to make it a mandatory requirement for IAL1, and therefore it would also apply to IAL2, as IAL2 is always stricter than IAL1.	Today, in IAL2 a CSP can use either one SUPERIOR evidence, or both STRONG and FAIR evidence. In the proposal, it appears that If the CSP leverages the second alternative for evidence, then the CSP would be restricted from having an automated evidence procedure. Therefore, the CSP would have only one option for evidence in the case of an automated procedure – i.e., the use of SUPERIOR evidence, which must involve a medium with digital content (SmartCard). As this section is NORMATIVE, DocuSign requests clarification of the text to ensure that a CSP is not limited to a single approach to evidence should they choose to use an automated procedure over an agent„ which would be more restrictive than the current requirement.
2	63A	5.3.3		1067	"If present, confirming the integrity of digital security features" (This comment applies to the language in line 1067 and all other locations in the document that are similar. There are many cases where the ID means includes digital information, but it is not used. For example, the Identity card includes a smartcard, which is not used as part of the identity validation process. This language implies that in this case, the smartcard must be used as part of the validation.	We request clarification of the language to allow that in the case that there is a smartcard within the physical document that is not used, that the evidence may still be considered STRONG, but not SUPERIOR.
3	63A	general			In the existing revision, the use of KBV/KBA is allowed for some use cases, but is not mentioned at all in the version 4. Considering the current predominance of the use of KBA/KBV techniques for ID Proofing in the US landscape today, we believe it is important the standard explicitly mention this technique as allowed or not.Further, we encourage the Agency to provide guidance on how to interpret a compliant use of these techniques.	
4	63C	6		1247-12	This section requires (SHALL) to have the relevant IAL and relevant AAL that were performed by the IDP. However, in line 1263, the written sentence is "Assertions SHOULD specify the AAL when an authentication event is being asserted and IAL when identity proofed attributes (or values derived from those attributes) are being asserted."	We request clarification regarding the use of SHALL and SHOULD in these scenarios. Is the intent to treat these scenarios similarly, whereby it is a requirement in lines 1247-50 and in 1263, or is the intent to provide the option for use in 1263?
5	63A	5.1.9			Trusted Referees and Applicant References: This section provides examples of hypothetical circumstances regarding a given applicant that would require the use of a trusted referee, but then leaves the decision of what situations ultimately require a trusted referee to the CSP. We believe this could lead to varied definitions of those situations across industries and potentially affect NIST's intent of enhancing equity. We encourage NIST to define specific instances where the trusted referees are required to better serve a larger group of applicants. In addition, the guidance is not clear if employees designated as trusted referees can perform other functions at the CSP or if this should be their sole responsibility.	