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:	*Spruce ID*
Name of Submitter/POC:	*Oliver Terbu, Director of Identity Standards & Jonathan Rufrano, Public Sector and Institutional Lead*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	Note to Reviewers	iii	175-177	The use of emerging technologies such as W3C Verifiable Credentials and mdoc, as standardized by ISO 18013-5 and ISO 23220, respectively, can aid in the implementation of an unattended and fully remote IAL2 workflow. This approach can shorten the identity proofing process by reusing existing digital evidence from previous identity proofing processes with the same or higher IAL. Past pilots, such as the one conducted in the UK regulatory sandbox, have demonstrated that reusing digital evidence can effectively reduce onboarding time, increase privacy (in certain circumstances), and maintain security. Although this approach relies on existing identity proofing or verification technologies, the reusability of digital evidence represents a new aspect of the process that can reduce the costs of identity proofing for federal agencies and enhance the user experience by shortening the onboarding time. When combined with privacy enhancing technologies and cryptography, these methods can achieve high identity assurance, superior user autonomy over data, and lowered impact of data breaches through data minimization, compared to prevalent approaches such as sending scans of sensitive documents.	Were this comment to be taken into account, the following requirements apply: The issuer (e.g. CSP) of the digital credential is trusted and it is the issuer that is responsible for ensuring that the digital credentials are secured in a trustworthy digital wallet (e.g. mdoc app). Trust in the wallet can then be increased by leveraging device attestations (available on Android and iOS) and binding a key to the digital identity document for holder authentication. The legitimate, intended, or designated holder of the digital credential has to be authenticated at the time of transaction through a key endorsed by the issuer (e.g. CSP) which is bound to the digital identity document, so the verifier or RP can rely on the trustworthiness of the key and the statements made in the digital evidence.
1	63-Base	Note to Reviewers	iii	178	The ISO 18013-5 and W3C Verifiable Credentials standards have standardized the data model representation of digital credentials and identity documents for evidentiary purposes. However, there is currently a lack of standardization for exchange protocols and transport mechanisms for unattended online transactions where the RP and digital identity wallet communicate via the Internet. ISO 18013-7, ISO 23220-4, and OpenID for Verifiable Presentations are promising candidates for achieving secure and unattended exchanges, while the proposed W3C mdoc browser API can provide similar functionality.	NIST can assist in ensuring that these specifications can be implemented without any vendor restrictions.
1	63-Base	Note to Reviewers	iii	182-183	This question is essentially asking for secure methods to exchange digital evidence between a CSP and a subject, with standardized data model representations already established for Verifiable Credentials and mdocs. While unattended secure exchange protocols are being developed, the most promising options include the protocols defined in ISO 23220-4, ISO 18013-7, the OpenID Foundation's OpenID for Verifiable Presentations, and the proposed W3C mdoc browser API. Out of these, only OpenID for Verifiable Presentations is capable of accommodating different digital credentials or evidence formats, such as mdoc and Verifiable Credentials.	
1	63-Base	Note to Reviewers	iv	210-213	Although we acknowledge that NIST 800-63 has shifted towards a more user-focused language, certain aspects need to be addressed or further elaborated to fully accommodate the emerging digital identity technologies such as Verifiable Credentials and mdoc, as defined by W3C and ISO.	There is a lack of guidance on how Verifiable Credentials and mDocs can be mapped onto the non-federated identity model described in NIST 800-63-4. Some informative examples on this matter would be useful, considering that there may be multiple valid ways of implementing this approach according to the non-federated approach as per NIST 800-63. For instance, in the non-federated model, the CSP can be seen as the digital credential issuer, the Subject can be seen as the subject/holder of the digital credential and the verifier can be a standalone component that is trusted by the RP or could be an integrated component of the RP itself. The verifier would verify a response (deviceResponse as per ISO 18013-5 or Verifiable Presentation as per W3C Verifiable Credentials standard) created by the digital wallet which does not require a component operated by the CSP since the response from the digital wallet is verifiable without reaching out to the CSP directly. Furthermore, to allow such a mapping, the current text might have to be adapted so that the Subscriber does not necessarily have an account with the CSP. It should be sufficient that the Subject has a digital wallet that manages a key that is an authenticator for the digital credential to be used for holder authentication / holder binding etc. The digital credential would still be managed by the CSP throughout the entire lifecycle to support important functions such as deletion, revocation and re-provisioning such as in the case of updating certain attribute values.
1	63-Base	Note to Reviewers	iv	239-241	Providing concrete examples would be useful in both federated and non-federated approaches. In the case of the non-federated approach, collaborating with industry experts to develop a model for mapping the existing model to the three-party-model described in the W3C Verifiable Credential and ISO 18013-5 standards would be beneficial.	