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

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

Organization:	*American Express*
Name of Submitter/POC:	*Sue Koomen*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	2	12		When creating a subscriber account, are you suggesting a Wallet model, a Cloud model, or both?	
2	63-Base	2.1	10		Can an issuer take the CSP role and RP take a verifier role in terms of doing the authentication by itself? The CSP should only gather information and verify for it.	
3	63-Base	2.2	11		After enrollment and ID proofing are done, where are the authenticator attributes that the CSP created, stored?	Maybe this is covered in A but we didn't see it.
4	63-Base	2.3.2	13		When the RP gets the subscriber attributes from the CSP or verifier, how does the RP verify that the attributes are from the legitimate CSP/Verifer? Are there guidelines NIST has on how this information is Proofed? Certified? Trust Store, Etc.?	Maybe this is covered in A, B but we didn't see it.
5	63-Base	general comment			Can an RP verify the attributes it gets from a verifier/CSP using a Decentralized entity-like ledger? Why are decentralized ledger not included as a general guideline in the base volume?	
6	63-Base	2.5	17-20		In W3C standards Verifiable Credentials there are 3 entities: Issuer, Holder and Verifier. Can the three models in Fig. 3, 4, and 5 fit the W3C model with a decentralized Ledger?	Can the flows show how this lines up to W3C Verifiable Credential Models?
7	63-Base	2.5	20		In Figure 5, what is the role of the CSP/verifier, when the assertion goes from the Issuer Device to the RP?	
8	63-Base	2.5	20		In Figure 5, the CSP and verifier are trhe same identity; when the RP asks for attributes from the user, the RP can talk directly to the subscriber. Does the CSP have a role?	
9	63-Base	2.5	20		Figure 5, can authenticators be registered to the subscriber controlled wallet? You talk about authenticators on the cloud. Is there a model that authenticators can just be on the wallet? Hybrid model where some are on the wallet and some are on the cloud?	
10	63-Base	general comment			Can the base volume explain Digital Identity models with some real examples of the entities - RP, Verifier, CSP, Subscriber and IdP?	
11	63A	2.1.2	7		Can there be risk levels defined as a general guideline when a Trusted Referee has to make a risk based decision for an applicant with insufficient identity evidence?	
12	63A	2.1.2	7		Are there any guidelines you can provide on who can be an Applicant Reference?	
13	63A	2.1.2	7		The identity roles defined on page 7 are all human elements but there are no roles for digitally signed documents; does the role have to be a human?	
14	63A	2.1.3	8		For Remote Unattended Identity Proofing, what guideance is NIST providing for what can be provided digitally to the CSP? For example, for digitally signed credentials, should they be a hyper ledger based credential? DUI based? MDL based? Etc.	
15	63A	2.1.3	8		Can there be general guidelines on the core attributes required for eachof the Identity Proofing types? Could the attributes for remote unattended be different than onsite attended?	
16	63A	2.4.1.3	12		Superior evidence requirements should mention the need for a trust anchor as a requirement to confirm identity cryptographically.	
17	63A	2.5.1	14		Identity verification methods - what protocols are recommended as a general guideline for digital assertion? When getting identity information, what protocol should be used to send information to a CSP? (open ID, EUDI wallet, etc.)	
18	63A	3	16		CSP needs to inform users which 3rd parties it might share the users information with for identity proofing, prior to sharing it	
19	63A	5	50		Users should be allowed to designate what RPs can have access to what parts of their stored identity data. CSP should let the user know if they support selective disclosure or predicates. Can CSP provide all to anyone, once they have it?	
20	63A	3.1.9	26		Can continuation codes be digitally signed so that if a user has to come back to finish a session, it can be verified that the same party is returning to complete.	
21	63A	3.1.5	23		In the general secuirty requirements guidelines, can industry standard protocols like DIDComm and OpenID4VC be mentioned a a good practice to adopt for enhanced security?	
22	63A	3.1.10	26		Notifications of proofing - user should know how they can unenroll if they would like to in the future	
23	63A	5	50		Need general guidelines on where subscriber account details can be hosted - Cloud, Wallet, Hybrid, etc.?	
24	63A	Appendix A			on the Superior examples, can you include an example of a Hyperledger based SSI wallet implemented as a decentralized identity holder wallet protected with keys on the device and with the trust anchor on a ledger?	
25	63B	2.1.1	5		You havent mentioned "out of band issuer based authentication" in the 7 authenticator types. Where does it belong?	
26	63B	3.1.1.2	13	732	The document states that Knowledge-based authenticators are not recommended but wouldn't you recommend them for AAL1?	
27	63B	3.1.7.1	26		If I tap a card in an app to authenticate, would that be categorized as a muti-factor cryptographic authenticator, or not?	

28	63B	Annex B			User access to private keys in sync fabric/cloud pretected with AAL2 MFA should exclude the multi-factor cryptographic authenticator which may in turn use the private keys from the sync fabric.	
29	63B	Annex B			Can we give provision to the user to clone the private key from the sync fabric to the user's choice of device instead of all, or include an expiry?	
30	63B	Annex B			Can there be general guidelines.on the implementation to share authentiction keys between users? Ie., close proximity, BLE, etc.	
31	63B	Annex B			Are there guidelines on how a cloud provider can provide an interface for a user to see what passkeys they hae and what devices have the passkeys/who they've shared them with, and to be able to manage them as needed (if want to delete for example). Cloud interface should be protected with AAL2MFA.	
32	63B	Annex B			Can there be guidelines around implemenation of a one time use authentication key on a device to authenticate a user journey on a different device connected to an RP? (using QR, BLE, NFC, close proximity etc.). I'm uisng a device that doesn't have my PK - what does NIST recommend as an authentication device?	
33	63B	Annex B			In addition to mentioning the webauthn flags - UP, UV, Backup Eleiglbe and State, can NIST add a flag to know if user chose to register and authenticate Webauthn on the same device or another device and provide deviceId on the device on which authentication happens?	
34	63C	general comment			Throughout Volume C, federation between IdP and RP has been explained using OIDC and SAML standards. Based on the available industry standards, federation can also be achieved used OpenID4VC and DIDComm protocols with very similar guidelines that are mentioned in Volume C. Is NIST planning to include emerging Digital ID protocols in their guidelines going forward?	