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:	*Georgetown CyberCorps Fellows*
Name of Submitter/POC:	David Lipscomb
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	2.1	10	655	We propose an additional definition for "Subscriber-Controlled Wallet" inserted after Relying Party (RP). Subscriber-controlled wallet is referenced many times and is key to understanding the federated digital identity model in Figure 5.	Subscriber-controlled wallet: A digital identity certificate maintained by the subscriber to ensure security and privacy protections. The subscriber controls all access to the wallet and can individually allow outside entities access to authenticate the subscriber's certificate.
2	63-Base	2.1	10	640	We propose a revised definition to "Subscriber" that emphasizes it is a role that a "Subject" becomes after they are an "Applicant."	Subscriber: An applicant who has successfully completed the identity proofing and enrollment process or authentication.
3	63-Base	2.5	19-21	888-920	We propose modifications to the steps outlined in a federated digital identity model.	subscriber-controlled digital wallet acts as the IdP. In this model, the RP often establishes a trust agreement with the CSP, eliminating the need for a direct trust relationship between the RP and IdP. The following steps describe how an applicant becomes a subscriber in a federated digital identity model: Step 1: An applicant applies to an identity proofing and enrollment process with a CSP. Step 2: Upon successful identity proofing, the applicant becomes a subscriber. Step 3: The subscriber-controlled wallet is onboarded by the CSP. - The subscriber authenticates to the CSP's onboarding function. - The subscriber activates the subscriber-controlled wallet using an activation factor. - The wallet sends a request to the CSP, including proof of a key held by the wallet. - The CSP creates an attribute bundle that contains a reference for the key of the wallet and any additional attributes. The following steps describe how a subscriber-controlled wallet provides an assertion to the RP to establish an authenticated session: Step 4: The RP requests that the claimant authenticate. This triggers a request for federated authentication to the wallet. Step 5: The subscriber proves possession and control of the subscriber-controlled wallet. - The subscriber activates the wallet using an activation factor. - The wallet prepares an assertion including the attribute bundle provided by the CSP for the subscriber account. Step 6: The RP and the wallet communicate through a federation protocol. - The wallet provides an assertion and optionally additional attributes to the RP. - The RP verifies the assertion to establish confidence in the identity of a subscriber for an online service. - Note: RPs may use a subscriber's federated identity (pseudonymous or non-pseudonymous), IAL, AAL, FAL, and other factors to make authorization decisions. Step 7: An authenticated session is established between the subscriber and the RP. - Note: Other protocols and specifications often refer to attribute bundles as credentials. These guidelines use the term credentials for a different concept. To avoid a conflict, the term attribute bundle is used within these guidelines. Normative
4	63-Base	Fig. 5	20		We suggest splitting this diagram into two separate diagrams. One for the 'Subscriber becoming an Applicant' (1), and one for the 'Relying Party Application Process' (2). Additionally, since the digital wallet/attribute bundle is controlled by the subscriber, the wallet should be within the Subscriber Box. See example of Diagram 1.