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:	*TraitWare, Inc.*
Name of Submitter/POC:	*Chris Canfield - Director of Technology*
Email Address of Submitter/POC:	*c* [redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63B	3.2.5			We see a use case where channel binding is established between the client and the verifier by an initial pairing which also associates the client to an external authenticator (physically separate from the client). All communications between the client and verifier satisfy the channel binding requirements. In this scenario, an authenticator MAY be physically separate from the channel bound client as the authenticator has been previously cryptographically associated with the verifier during a registration process. The external authenticator may also be used in the process to establish the channel binding between the client and verifier. During this establishment process the external authenticator may associated with the client at the verifier. For authentication, the client may request a verifier signed and then client verfied identifier. This identifier may be presented to the external authenticator (via QR/bluetooth/NFC). The authenticator must cryptographically sign this identifier and present it to the verifier. The client may make a request to the verifier to establish if the identifier has been successfully submitted by the authenticator. If the verifier determines that the authenticator output (signed identifier) was submitted by the client-paired authenticator and it is valid, the authenticaion event is valid.	An external authenticator MAY be used provided the authenticator and client are both cryptographically bound to the verifier and associated with each other by the verifier. The external authenticator MAY be used to establish the channel binding between the client and the verifier, during which the verifier may accociate the client with the external authenticator.