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: Beyond Identity

Name of Submitter/POC:
Monty Wiseman

Email Address of Submitter/POC:
[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
1	63B	2.1	4	502	While authentication protocol was defined in several places in 800-63, what constitutes a "secure" authentication protocol is not defined. Either define what is means to be "secure" or remove the modifier.	Successful authentication requires that the claimant prove possession and control of the authenticator through an authentication protocol.
2	63B	2.2	6	544	Same comment as above	Same suggested change as above
3	63B	3.1.1.2	13	807	In other sections the TPM is mentioned parenthetically as an example implementation. For consistency, this should also be included here.	such as a hardware security module or trusted execution environment (TEE) (e.g., TPM).
4	63B	3.1.7.1	26	1145	The text describing activation factors parenthetical uses i.e. i.e., is restrived which implies that only those types of activation secrets are permitted. Some devices such as the TPM provide additional activation methods. For example, proof of possession of an externally controlled key (e.g., a smartcard) is also supported. Recommend changing the parenthetical to e.g. See comment #7	Multi-factor cryptographic authenticators encapsulate one or more private or symmetric keys that SHALL only be accessible through the presentation and verification of an activation factor (e.g., a password or a biometric characteristic).
5	63B	3.2.4	32	1333	While the list is "not limited to" it would be beneficial to the industry to state that some devices (e.g., the TPM) can also provide an attestation of a key's properties (e.g., key type and size, authorization policies that can be used as activation secrets, etc.). Note that this is NOT the same as the 2nd bullet which is the properties of the Authenticator. This is the properties of the key within the Authenticator.	Add a bullet: properties of the key
6	63B	3.2.4	32	1334	The key attesting the above properties should be at least as strong as the attested properties themselves.	Attestations SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication) and is at least as strong as the property being attested to.
7	63B	3.2.10	36	1472	Some devices (e.g., the TPM) permit restrictions on use of a key based on a rich set of policies. Among those policies is the proof of possession of an asymmetric key (e.g., one contained in a PIV). The use of proof of possession of an external asymmetric key (or even a symmetric key using HMAC) should be permitted alongwith password or biometric. Recommend ammending Table 1 to include this option.	An activation secret may also be proof of possession of a key external to the authenticator. An example is proof of possession of an asymmetric key is a PIV (which itself may require a PIN/Password to activate). Similarly, proof of possession of a symmetric key using an HMAC will meet this requirement.