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

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*RSA*
Name of Submitter/POC:	*Jean-Christophe Laurent, Senior Principal Product Manager*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	Authentication and	iii	169	This section asks reviewers to comments if emerging techniques such as FIDO passkey are sufficiently adressed in the guidelines.. But this is the only mention of FIDO or passkey, ie these terms are not used in any other part of the document, so the answer to this question about FIDO is 'NO'.. Also, the 'sense' of the term 'passkey' associated with FIDO is changing.. it used to be only about the new Multi Device Credential mechanism used FIDO 'passkey', but 'passkey' has now been adopted as a generic name by the FIDO alliance for all types of keys, so basically cover both the 'classic' Device bound keys, such as Hardware Authenticators like RSA DS100 or Yubikey devices, and the 'Multi Device Passkeys'.. The current implementation of Multi-Device passkey, with its lack of defined attestation, and its lack of possibiilty of controlling/restricting the 'Multi Device' features raise some serious questions re: Enterprise Security, and should be covered in this document.. Note that the FIDO alliance has tasked one of its working group to evaluate how to address these security questions, but there is no currently published timeline for this work.	Explicitely cover and distinguish in the document the 'classic' FIDO credentials (Hardware based Authenticator) and the FIDO Multie-Device credentials (software based Authenticator), and explain the current concerns about the security model for FIDO Multi-Device credentials,
2	63B	Authentication and	iii	169	The delineation of Authenticators by Authentication Type is no longer fine grained enough for the class of cryptographic authenticators (Single factor cryptographic software, Single factor cryptographic device, multifactor cryptographic software, etc.). In the past you would have symmetric key based cryptographic authenticators and asymmetric key based cryptographic authenticators. The majority of the asymmetric authentication schemes used digitally signed X509 public key certificates to protect the integrity of the public key along with a robust public key infrastructure. With the introduction of FIDO we now have an authentication scheme that does not rely on X509 certificates, or a classic PKI, to protect the public key. That protection is now provided by the various relevant FIDO protocols and the back-end FIDO service. In addition, with the introduction of passkey (I'm using the original definition of passkey here not the newer overloaded term), private keys that would normally never leave a FIDO token can be shared in order to address various user scenarios. In order to provide relevant guidance on how to securely use FIDO authenticators to meet the various controls in 800-63 it is necessary to lay the groundwork by actually discussing FIDO in 800-63. Defining a new class of Cryptographic authenticators is a prerequisite to doing this.	Developed two new categories of cryptographic authenticators/verifiers, one for the classic PKI based approach (such as those used in smartcard-based authentication like the PIV card) and one for FIDO. Then, based on these new categories provide more focused guidance around FIDO specific issues like passkey.