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:	*Yubico*
Name of Submitter/POC:	*Joe Scalone*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	5.2.4	34	1328-1341	As credentials shift away from solely hardware-based authentication models, the vulnerabilities shift to credential protection at rest.As such, attestation must be required as part of any authenticator security model. Additionally, attestation is crucial for remote provisioning because it provides a way to verify the identity and integrity of the device being provisioned. It also allows the remote provisioning system to verify that the device being provisioned is authentic and has not been tampered with. A trusted authenticator helps keep the chain of trust in place. From a zero trust perspective, blindly trusting any authenticator must be avoided. By using attestation, the remote provisioning system can use provided signals to verify that the device is running the correct configuration and meets FIPS guidelines. In the future, attestation will also provide information indicating if the credential has been derived from another credential. Attestation helps to ensure that the device is secure and compliant with federal policies, standards, and allowed to be used for particular systems. Attestation is equally important for citizen facing and non-government entities, because it can securely guarantee the origin of its use and prevent account takeover attacks, protecting personal information and securing finances. Attestation can also reduce the risk of supply chain attacks, as one can track signals from the authenticator at the time of registration and compare them at the time of authentication Attestation is the key control for non-hardware based authentication models. It provides critical information regarding the process by which a new credential is created, how it is managed, and what it can do. This, in turn, allows administrators to make informed authorization decisions and monitor potential threats. The attributes created through attestation can be used to secure transactional authentication from any authenticator.	Attestation is an important key to maintating the authentication chain of trust and provenance of the authenticator. Because of this, it should be explicitly stated and requires for AAL2 and AAL3. An authenticator that protects a secret, needs to provide assurances to the protection of those secrets. Add "Attestation" row to Table 1 on page 13. Not required for AAL1, Recommended for AAL2 and Required for AAL3.
2	63B	4.2, 4.3	8-12	495-656	Device Attestation is a very important key to maintaining the authenticators chain of trust. Because of this, it should be required for AAL2 and AAL3. This would ensure the provenance of the authenticator and assure the security of the transaction.	Device attestation SHOULD be required for AAL2 and AAL3.
3	63B	4.2.2	9	539-543	Line 539-543 "OMB Memorandum [M-22-09] requires federal government agencies to offer at least one phishing-resistant authenticator option to public users at AAL2. While phishing resistance as described in Sec. 5.2.5 is not generally required for authentication at AAL2, verifiers SHOULD encourage the use of phishing-resistant authenticators at AAL2 whenever practical since phishing is a significant threat vector" Since phishing resistant authenticators are now required by OMB for all government use, "While phishing resistance in Sec. 5.2.5 is not generally required for authentication at AAL2" should be removed. "SHOULD encourage the use of phishing resistant authenticators at AAL2" should be changed to "SHOULD require phishing resistant authenticators at AAL2" These changes would put NIST guidance in line with the guidance from OMB M-22-09. Phishing resistance should only be optional at AAL1. In today's environment, AAL1 should include some form of MFA, with phishable options should reside here.	"OMB Memorandum [M-22-09] requires federal government agencies to offer at least one phishing-resistant authenticator option to public users at AAL2. Verifiers SHOULD require the use of phishing-resistant authenticators at AAL2 whenever practical since phishing is a significant threat vector" Allow for phishable MFA options at AAL1 only.
4	63B	4.2.1, 5.1.3.1	8, 21	510, 847-879	Many different studies and several high profile incidents have brought attention to the disadvantages of using SMS as a method of multifactor authentication, in any form. While it may be easy and cell phones have become ubiquitous, it still provides a very poor level of security. Companies may implement SMS MFA to reach AAL2, because of the ease of implementation and use. While this would provide some level of friction during the authentication process, it does not provide an adversary any resistance and is a known security risk.	Depricate the use of SMS based authentication at AAL2 by removing Out-Of-Band authenticators from line 510.
5	63B	5.1, 5.2.11	14. 38-39	673-674,1482-1484,1504-1507	There are multiple definitions for activation secrets. On line 673-674 activation secrets are defined as "Memorized secrets that are used locally by a multi-factor authenticator" On line 1482-1484 "An activation secret is used to decrypt a stored secret key used for authentication or is compared against a locally held stored verifier to provide access to the authentication key" On line 1504-1507 "... a secure element that released the authentication secret only upon presentation of the correct activation secret."	There are multiple different definitions of activation secrets. Develop a single unified definition for activitaion secrets.
6	63C	4.2	8	520-521	*800-63-4C Line 520-521 - "The authenticator presented is known as a bound authenticator, described in Sec. 6.1.2" Attribution can provide a clear statement on signals, identities and security for every authenticator. This action, in addition to binding the authenticator to the IdP/RP SHALL establish a clear picture of the authenticator in question with every transaction.*	Add a requirement for attestation to the definition of a bound authenticator.
7	63B	4.2.2	9	522-530	Line 522 - Cryptographic authenticators used at AAL2 SHALL use approved cryptography. Authenticators procured by federal government agencies SHALL be validated to meet the requirements of [FIPS140] Level 1. Software-based authenticators that operate within the context of an operating system MAY , where applicable, attempt to detect compromise (e.g., by malware) of the platform in which they are running. They SHOULD NOT complete the operation when such a compromise is detected. At least one authenticator used at AAL2 SHALL be replay resistant as described in Sec. 5.2.8. Authentication at AAL2 SHOULD demonstrate authentication intent from at least one authenticator as discussed in Sec. 5.2.9. *800-63-4B Line 522-530 Any rules regarding the security capabilities of hardware and software authenticators should be in parity. Software based authenticators should be required to detect compromise of the platform they are running.*	Regulations regarding hardware and software authenicators need to be in parity. All software, BYOAD and cryptographic authenticators should have approved cryptography and use a minimum of FIPS 140 Level 1 approved cryptography. Line 522 remove the word "Cryptographic"

8	63B	4	6	434	Even though FIPS 140-3 certifications were introduced in 2019, you were still able to start the FIPS 140-2 certifications until mid 2021 and active modules will not be moved to the historical list until September 2026. Devices that were certified at FIPS 140-2 should still be able to be used up to 5 years post certification, due to the time and cost of the certification process. Suggest changing language to just refer to valid FIPS 140 certifications. Furthermore, as of this moment there are currently only 7 FIPS 140-3 certified modules total., with only 1 certification since the beginning of the year. In comparison there have been 39 total certifications at the FIPS 140-2 level to this point. (2/24 date of writing).	Add "FIPS 140-2 certificications should still be allowed to be used until they are moved to historical or revoked." after line 434.
9	63B	5.1.8.1	29	1146-1168	Credentials can be managed by various escrow systems to ensure operability and those escrow systems need to be protected with the same rigor as the overall AAL they are aligned with, in addition to the standards for cloud computing. This will ensure the chain of trust stays intact. Attention should also be given to the management layer of credential escrow systems to assure they are held to the same standard as the credentials.	Add language making cloud based identity escrow systems and the restoration of escrowed secrets held to the same AAL standard as the credentials. The cloud based system SHOULD be protected with phishing-resistant MFA.
10	63B	5.2.11	38	1487	Yubico supports the current draft language to have the activation secrets set to a minimum of 6 characters in length	n/a
11	63B	4.2	8	495-520	AAL2 provides a broad spectrum of MFA options to cover a number of scenarios from public and consumer access that cover a number of risk factors in each group. Given there isn't a differentiation between user groups, it is difficult to have clear guidance based on the different risk exposure of these two fundementally different groups. Additionally, regardless of user groups, risk factors need to be assess based on the data that is being protected and the risk profile of the different groups.	Organizations need to perform their due diligance for their subscribers to understand the appropriate AAL2 controls that should be implemented. At a minimum, PII data protection and work force subscribers should strongly be encourage to use phishing-resistant authentication mechanism.