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

Please submit responses to dig-comments@nist.gov by April 14, 2023

Organization:	*FIDO Alliance*
Name of Submitter/POC:	*Andrew Shikiar and Jeremy Grant*
Email Address of Submitter/	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	Base	Note to Reviewers	iv	210	NIST asks "Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks? We believe support for multi-device FIDO passkeys are appropriately addressed in 63B. We do think it would be helpful for NIST to include additional language to discuss how to secure the "sync fabric" associated with passkeys - perhaps with language that ensures that authenticators facilitating the synchronization of private keys among different devices do so in an end-to-end-encrypted fashion protected by an appropriate key strength, and the authentication to the sync fabric meets appropriate requirements. There are a number of ideas from members on this point and we would welcome the opportunity to discuss pros and cons of different ideas.	
2	Base	Note to Reviewers	iv	214	NIST asks "Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?" We believe the new definition of phishing resistance is excellent, and clearly reflects the way that FIDO authenticators address this requirement. For clarity's sake - and to make it easier for implementers who do not share NIST's expertise in understanding how the FIDO approach to phishing resistance aligns wtih NIST guidance - it would be VERY helpful to note in 5.2.5.2 that WebAuthN/FIDO2 is one example of an approach to Verifier Name Binding (as NIST did in slide 35 of its January 12th webinar slides) In 5.2.5.1, NIST notes that client-authenticate TLS is an example of a phishing-resistant protocol that uses channel binding; it would make sense to provide a similar example for 5.2.5.2	At the end of 5.2.5.2, note: An example of a phishing resistant authentication protocol that uses Verifier Name Binding is FIDO2/Web Authentication, because the authenticator output is cryptographically bound to the domain name identifier.
3	63B	5.2.11	38-39	1481-1485, 1502-1507	In the first paragraph, an activation secret is defined as a secret used to decrypt a stored secret key or to provide access to an authentication key. However, in the last paragraph, the secret is defined as to be used to release an authentication secret or to decrypt an authentication secret. We beleive "release" is the more appropriate term - as "decrypt" may be read as meaning that it would be available in plaintext.	Align the description of usage of the activation secret in the two paragraphs.
4	63B	5.2.11	39	1506	The term "memorized secret" should be "activation secret" to align with the entire section.	Replace the term "memorized secret" with "activation secret"
5	63B	5.1.3.1	21	863	Clarify requiremenmts for key storage regarding key exportability: It sounds like an underlying Single-Factor/MF Cryptographic *Device* is assumed here - as opposed to SF/MF Crypto SW which allows the exportability of keys.	Clarify whether key exportability is allowed here or not
6	63B	5.1.9.1	30	1186	"Removed" may be a confusing term: It is not relevant in this context whether the key still is available on "this device", but whether it is available outside as well. "Removed" suggests the key may no longer exist on the device, which is unlikely in most MDC use cases.	Replace "(i.e., cannot be removed)" with "(i.e., cannot be extracted)"
7	63B	5.1.9.1	30	1202	"an authenticator be either a separate piece of HW or an embedded processor…" - the user verification should be seen as part of the authenticator as well: Background: Need to clarify that even (single-device keys in) platform authenticators can be a MF Cryptographic Device - not only Security Keys.	Clarify that the authenticator often includes the user verification component as well - not only the crypto chip/engine. Additionally, clarify that FIDO authenticators supporting single-device credentials (either "legacy" FIDO credentials or device public keys (DPK) typically could meet that requirement).
8	63B	5.2.4	34	1340	Attestation is a good way to support requirement in line 1573 in Authenticator Binding.	Explicitly mention that attestation is a strong way for the RP to verify the "type of user-provided" authenticator. Suggest to add a clarifying statement about the consequences of NOT being able to verify the "type of user-provided" authenticator.
9	63B	6.1	41	1573	Attestation is a good way to support requirement in line 1573 in Authenticator Binding: This especially applies to authenticators that allow the key export so the RP could verify that exported keys are handled appropriately - see also comment #4 regarding line 1157 above.	Mention that attestation as defined earlier provides a strong way for the RP to verify the "type of user-provided" authenticator.
10	63B	8.2	55	1944	Mitigation strategies for Authenticator duplication	Mention sync-fabrics/"passkey providers" implementing stringent AAL2/IAL2/FAL2 for restoring multi-device keys that have been backed up as one potential strategy.
11	63B	5.2.12	39	1508	"Direct connection" could be more clearly defined. The FIDO CTAP 2.2 hybrid transport protocol uses a mix of protocols to support Cross-Device Authentication in a phishing-resistant manner, without what has been traditionally defined as a direct connection (physical cable, Bluetooth pairing, and/or Wi-Fi direct assocation).	Please clarify the meaning of "direct connection" and whether equivalent solutions like CTAP 2.2 hybrid transport could be considered "direct" (or potentially add a statement about "direct equivalence")
12	63B	5.2.12	39	1523	"Use an authenticated encrypted connection". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement to provide data from the client to the authenticator to then allow both parties to establish a secure websocket connection	Clarify the meaning of "connection" in this context so that solutions like CTAP 2.2 with hybrid transport qualify

13	63B	5.2.12	39	1524	"A pairing process". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement. There is no Bluetooth layer pairing / relationship, by design.	Please consider cases where a traditional bluetooth "pairing" relationship is not used (such as hybrid which essentially uses an application level relationship)
14	63B	6.1.2.1	43	1627	"at least two valid authenticators of each factor that they will be using". With a MDC passkey, the same credential could exist in two authenticators. Would a single passkey stored in multiple authenticators meet this requirement?	May need clarity for credential vs authenticator in this context
15	63B	5.2.11	38	1487	Many users' PINs on mobile phones are still set at 4-digits. For public-facing use cases: if 6 digits is a hard requirement, it will have the effect of excluding millions of AAL2 capable FIDO authenticators in the hands of the public. We believe it would make sense to continue to allow 4-digit PINs for consumer use cases but require 6 digits for GFE authenticators. Note that studies have been done that shows that PIN lengths at 6 digits are not markedly more secure than PIN lengths of 4 digits (https://www.usenix.org/system/files/sec22fall_munyendo.pdf and https://maximiliangolla.com/files/2020/papers/sp20-670-this-pin-can-be-easily-guessed_v9.pdf).	Authenticators making use of activation secrets SHOULD require the secrets to be at least 6 characters in length and SHALL require the secrets to be at least 4 characters in length. Authenticators procured by federal government agencies making use of activation secrets SHALL require the secrets to be at least 6 characters in length. To meet AAL3, an activation secret SHALL be at minimum 6 characters in length.
16	NIST SP 80063A	5.1.8	23	925	The language is somewhat vague and confusing - biometric consent could mean things like the use of biometrics to have a nonrepudiated consent form. Stored with is problematic perhaps from an implementation point of view. Change to "CSPs SHALL store a record of subscriber's consent for biometric use and associate it with subscriber's account"	
17	NIST SP 80063A	5.1.8	23	928	Individual is vague. Request is insufficient. Change to "CSP SHALL support the ability for subscribers to delete all of their biometric information upon request at any time, except where otherwise restricted...	
18	NIST SP 80063A	5.1.8	23	936	Utilize system-level metrics, not technology level. FMR-->FAR	
19	NIST SP 80063A	5.1.8	23	937	Utilize system-level metrics, not technology level. FNMR-->FRR (also note FRR should include rejection related to PAD subsystem, i.e. BPCER)	
20	NIST SP 80063A	5.1.8	23	937	FRR of 1% would be too low for identity proofing that includes PAD; Recommend 5%	
21	NIST SP 80063A	5.1.8	23	953	Add performance metrics for liveness/PAD, specifically IAPAR; Suggest IAPAR<15%; Suggest testing methodology like FIDO	
22	NIST SP 80063B	4.2.1	8	514	Note is a bit confusing - first biometrics cannot be a solo factor, but then, it's unnecessary to use 2 authenticators... Change to Note: A biometric characteristic is not recognized as an authenticator by itself. When biometric authentication meets the requirements in Sec. 5.2.3, the associated device must be authenticated along with the biometric. The associated device then serves as "something you have," while the biometric match serves as "something you are."	
23	NIST SP 80063B	5.2.3	32	1257-1277	Delete; Not needed, counterproductive as recommendations incorporated this in the framework. 800-63 4.3.1 describes biometrics as a cornerstone of authentication - no need for these disclaimers	
24	NIST SP 80063B	5.2.3	33	1280	Utilize system-level metrics, not technology level. FMR-->FAR	
25	NIST SP 80063B	5.2.3	33	1283	Change "SHOULD" to "SHALL"	
26	NIST SP 80063B	5.2.3	33	1283	Add performance metrics for liveness/PAD, specifically IAPAR; Suggest IAPAR<15%; Suggest testing methodology like FIDO	
27	NIST SP 80063B	5.2.3	33	1283	Missing FRR; Suggest 5%	
28	NIST SP 80063B	5.2.3	33	1288	Remove reference to Clause 12; The document shall reference the whole of 30107-3 as there are many relevant requriements related to PAD testing that shall be followed.	
29	NIST SP 800-63A	4.3.3.1	11	553	We would prefer to see more definition or guidance on "reasonably assumed". This requirement can be difficult to document during assurance certification process.	
30	NIST SP 800-63A	4.3.3.1	11	551	The fair requirements are vague on the nature of confirmation from the "Issuing Source". In practice, Issuing Source is not equipped nor under any obligation to provide such confirmation services.	
31	NIST SP 800-63A	5.1.8	23	943	10. CSPs SHALL make all performance and operational test results publicly available. >>> Unless specified or granted permission otherwise by the agencies or end user organization, Operational Test results are confidential information. CSPs may not have the necessary legal authority to disclose the operational test results. The responsibility of disclosing Operational test results should be the responsibility of the federal agency and not CSPs.	Federal agencies must make the best effort to disclose all performance and operational test results publicly available.
32	NIST SP 80063A	5.5.8	31	1209	Supervised Remote ID Proofing is last section: mDL, eID and VCs are upcoming technologies that in general could be suitable for unsupervised remote ID Proofing. It would be great to show where they fit and what the minimum requirements (on a high level) are to achieve IAL3.	Add section 5.5.9 "Requirements for IAL3 Unsupervised Remote Identity Proofing" where mobile Drivers License (mDL), electronic ID cards, Verifiable Credentials etc. are handled