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:	*NSA*
Name of Submitter/POC:	*Mike Boyle*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63B		9	552	From the wording, it appears direct authentication using biometrics is now supported. It's not clear that the robustness of biometric verification justifies this. Recommend direct biometric authentication with central validation be restricted.	Remove allowance for direct biometric authentication until methods to support it are proven.
	63B		11	614	Reference to log-out can lead to confusion; implied termination of already initiated/background processes is beyond the scope of this publication.	Omit "e.g. logout" and refer to such processes consistently as terminate the RP session.
	63B		14	688	Normalization and matching standards should be referenced. Vague language can lead to confusion and mis-calculated strength metrics. Poor normalization practices can lead to impersonation or denial of access to authorized resources.	Reference standards (RFCs) or provide specific requirements for string matching.
	63B		16	758	While noting NIST has “not published guidelines on specific password hashing schemes”, recommends the use of a memory hard function (MHF) with Argon2 and scrypt provided as examples. This seems problematic especially as the two schemes mentioned are not built on NIST approved primitives.	The special pub should instead recommend use of PBKDF2 and switch to the use of a MHF if/when one is approved by NIST. Note there are MHFs that can be used with NIST primitives such as hash functions, or modified to do so. This would help streamline lab validations of such solutions, as well as reduce the number of primitives that need to be supported by devices.
	63B		17	772	The recommended minimal iteration count of 10,000 for PBKDF2 seems low.	Increase the minimum, e.g., the Open Worldwide Application Security Project (OWASP) recommends counts of 600,000 and 210,000 for PBKDF2-HMAC-SHA256 and PBKDF2-HMAC-SHA512 respectively. Further, the recommended count should increase over time to account for Moore’s law. This can easily be done using a table that project out 10 years or so.
	63B		17	780	Example of separate storage mechanisms using hardware-backed protections should be singled out (SHOULD) as opposed to a parenthetical remark that may be ignored.	Restate as SHOULD use…
	63B		18	813	Rate limiting of strings (memorized secret, as well as OTP, Lookup and out-of-band) is good generally, not just when the intended entropy is greater than 64.	Add "and SHOULD be used when entropy is greater than 64"
	63B		21	863	Requirement is confusing. Discussion of device-specific authentication for OOB direct addressing would hint that this be mutually authenticated channel, not just verifier authenticated. Clarify.	Clearly specify device authentication SHALL be provided…
	63B		21	864	Be specific which key is being discussed. Device-specific private key is implied, but OOB secrets, session key etc. might also be referred to as keys.	Clearly speficy "device authentication key"
	63B		21	869	Clarify SF versus MF OOB mechanisms wrt separate activation/unlocking of the app. Reference 5.1.3.4 or label this section SF OOB for clarity.	Relabel section as SF OOB, and add "… not meeting the requirements of 5.1.3.4…"
	63B		21	874	Previous discussion is that OOB approval-based mechanisms are not allowed. Omit reference to these mechanisms. Automated transfer of secrets from the primary device should be addressed using language that distinguishes it from disallowed methods.	Remove all references to approval based OOB, "push notification" and "confirmation of transaction" after explaining the method is no longer allowed.
	63B		22	883	Push notification (here and subsequently) is commonly used to describe the disapproved approval-based OOB method. Avoid confusion by specifying 'verifier-initiated' rather than 'push notification'	See above, and replace with 'verifier-initiated'
	63B		22	888	Discussion seems to only require the authenticator device be verified for one of the two OOB methods, and only when verifier initiated. Clarify that verification requirements apply in all cases.	Expand to systematically cover primary-to-secondary and secondary-to-primary as well as authenticator-initiated and verifier-initiated (4 cases).
	63B		23	927	What are these indicators of compromise and how may a verifier observe them? As these are not readily available and the threats are prevalent, recommend SMS/PSTN delivery be prohibited altogether. Instead, secure messaging apps might be used to mitigate PSTN delivery.	Specify mitigations to OOB over PSTN that can be met.
	63B		23	935	Use consistent language from 5.1.3.1, where activation data is recommended, not required.	Repeat "activation data… "SHOULD" and clarify the additional requirements/options (prior to establishing the secondary channel, prior to displaying OOB secret, to establish an automated controlled interface between channels…)
	63B		23	937	Remove reference 'confirming the transaction…' to approval-based mechanisms that are no longer allowed.	See above
	63B		24	982	Clarify that access to the OTP seed key is only required during enrollment of the authenticator and should not be available post-enrollment.	Add "… during enrollment…"
	63B		24	985	Consider adding key establishment as a valid method for sharing seed keys.	
	63B		25	997	OTP entropy is not well defined, and might be confused with the underlying seed key and hash/crypto engine producing the OTP values. Since OTP values are truncated to as few as 6 characters, recommend always using rate limiting.	Replace with "rate limiting SHALL be performed."
	63B		26	1046	Clarify that access to the OTP seed key is only required during enrollment of the authenticator and should not be available post-enrollment.	Add "… during enrollment…"
	63B		27	1063	OTP entropy is not well defined, and might be confused with the underlying seed key and hash/crypto engine producing the OTP values. Since OTP values are truncated to as few as 6 characters, recommend always using rate limiting.	Replace with "rate limiting SHALL be performed."
	63B		27	1069	Colloquial use of "soft" media is not appropriate for a normative section. Specify that software must be instantiated on a device under exclusive control of the user. Clarify that this may be achieved during registration of a personally controlled device, or using additional authentication factor(s) to access the instance for shared devices.	Replace with "… is software installed on a device which manages access to a crypographic key stored on the device…. The key is established during enrollment of the device…. User activation data (biometric or PIN/passphrase) is required prior to allowing use of the key…. The software SHOULD prevent export of the key or other exposure of the key in plaintext."
	63B		27	1081	Allowing export does not distinguish software versus hardware, and should not be recommended even for software devices. Consider requiring non-export in all cases, or at a minimum require controlled export under certain circumstances. Note that FIDO's desire to address lifecycle support gaps is not justification for requiring export of private keys; rather a controlled mechanism can be used to re-register new credentials as part of the device replacement process.	Remove parenthetical remark.
	63B		28	1103	Vague "suitably secure" needs to be described this if considered normative	Specify "… an isolated execution environment protected by hardware or a separate processor with controlled interface to the main processing unit of user endpoint."
	63B		28	1106	"length" should be "strength" to be consistent especially for crypto methods (alternatively, remove reference to 112 bits).	Replace "length" with "strength"

	63B		28	1109	Equivalent statement for FIPS validation should also apply for software as well as in OTP methods that use cryptography directly, and OOB methods that leverage cryptography to establish device authentication.	Replicate "The authenticator is subject to applicable [FIPS140] requirements of the AAL at which the authenticator is being used." for each OTP section, and within the OOB sections discussing device authentication "...in support of establishing the channel."
	63B		28	1133	Clarify that access to the secret key is only required during enrollment of the authenticator and should not be available post-enrollment.	Add "... during enrollment..."
	63B		31	1218	Refer to session and process limits that make this restriction practical.	Refer to session management section.
	63B		32	1264	Speculative statements about unproven, untested mechanisms should not be referenced as normative.	Remove allowance for direct biometric authentication until methods to support it are proven.
	63B		33	1306	What breakthrough in biometric validation allows confidence in central/remove validation	Remove allowance for direct biometric authentication until methods to support it are proven.
	63B		34	1321	Retraining the template, together with remote validation, will allow interpolation that reduce risk of exploitation.	Remove allowance for direct biometric authentication until methods to support it are proven.
	63B		34	1337	All attestations should be signed.	Replace with "Attestations SHALL be signed using..."
	63B		34	1340	Attestation is a strong mechanism being recommended as part of ZT guidance.	Replace MAY with SHOULD
	63B		35	1361	AiTM applies to any authenticator that is not phishing resistant	Omit OTP (or add "and OOB").
	63B		35	1364	Statement about combinations of authenticators is only true if each is presented independently	Consider recommending that combinations of authenticators protected under a mutually authenticated channel using a phishing resistent authenticator can be considered phishing resistant as well.
	63B		35	1385	Description doesn't match title.	Refer to authenticators (or authentication protocols) that 'support verifier name binding', provide examples for clarity and generalize recommendation for all RFC 6125 name types (at a minimum).
	63B		36	1413	Clearly describe applicability and protections for each authenticator methods.	Specify which authenticators (look-up, memorized secret, OOB?) require hash-based protection for matching and specify the mechanism used (salt, method, number of iterations etc.) for each. For OTP methods, recommend specifying use of HSM for protecting the verifier's copy of seed values.
	63B		37	1448	Consider how this might be supported (device attestation?) for non-PKI authenticators.	
	63B		38	1496	Exactly 10?	Consider flexibility "no more than 10"
	63B		39	1507	Direct use of a memorized secret as a key is not recommended.	Specify that the memorized secret be used as input to derive a key...
	63B		39	1524	Options are specified using SHALL (option 1) and MAY (option 2) appear contradictory.	Revise to say "SHALL use either a secure pairing process or a wired connection", and continue to specify requirements for each option.
	63B		42	1610	Process hints at using look-up secrets, but details are not correct.	Reference look-up secret and ensure details are aligned (select a value based on input from verifier).
	63B		43	1638	Validtity times should be flexible	Replace "20 minutes" with "up to 20 minutes"
	63B		43	1648	Methods for increasing binding strengh should be as rigorous as obtaining the desired AAL in the first place.	Require that the AAL 1 authenticator be revoked and replaced after upgrading, since section 6.1.1 requires that the initial authenticator be considered temporary. Also clarify that such bootstrapping does not allow one to upgrading to an AAL 3 account (e.g., by adding a third AAL 1 authenticator).
	63B		46	1737	Two-factor authentication is not defined.	Use "multifactor" throughout.
	63B		49	1836	Requirements do not allow session binding to TLS or IPSEC using DH-methods.	Replace 1,2, and 4: 1: Secrets are established during or immediately after authentication 2: Secrets are established using input from an approved random bit generator containing at least 64 bits of entropy 4: Secrets are either transferred from the session host to the RP or CSP via an authenticated protected channel, or derived from keys established as part of establishing a valid, mutually authenticated protected channel
	63B	8.1, 8.2	52		It seems more logical to split "Assertion Manufacture or Modification" into two cells when considering the adjacent cells in the table.	In Table 3, change the second row of the first column to "Assertion Manufacture" and the third row of the first column to "
	63C	General			Federation is already complicated and abstract; using inprecise language, collequial terminology, and using informally defined terms inconsistently makes this much more difficult to understand.	~~Provide formal definitions of federation protocol, federation model, and federation transaction, and use the terms~~ consistently. Avoid alternative descriptions such as identity protocol, authentication protocol, authentication process etc. in reference to a defined term. Avoid login, logon, log on, log into when authenticate is meant. Logon implies a specific context and additional requirements that are outside the scope of this document. Differentiate or use common terminology for provisioning API, identity API and assertion API. Provide forward references to sections defining terms, or concepts used in summary sections or when used to support other requirements. Provide concrete examples, including mutual-authenticated TLS to ground abstract concepts. Use a consistent definition of dynamic registration - established using applicant-provided information versus established using minimal (no) administrator intervention. Registration information and configuration information are completely different - configuration information and software assertions used to establish RP credentials requires further explanation. Requirements to use 'appropriately secure methods' are vague, and have no value. Be explicit and/or reference allowed mechanisms.
	63C	General			Focus on clearly defining security and privacy requirements, and avoid making allowances for unproven methods.	Reconsider parenthetical comments that reference unproven or speculative techniques. Requirements for dynamic registration create a chicken-and-egg scenario. Consider a minimal condition on IdP to have a valid public key certificate issued by a CA trusted by the RP. This significantly simplifies the concept and is very likely to be adopted. The abstraction here makes this unintelligible, and misinterpretation will lead to insecure implementations. Don't recommend continued use of unauthenticated cookies.
	63C				Assertions that do not include (implied) AAL claim should not be allowed. Instead a 'denied' assertion should be provided. It seems more reasonable to use the empty AAL claim to indicate that the AAL assigned in the trust agreement is met.	
	63C				Be consistent regarding allow- and block- lists.	Avoid implementation-specific ("add an RP to," e.g.) to such lists and use generic language ("constrain an RP by use of") that does not imply a specific implementation.
	63C				Address wildcard identifiers in the registration phase, not just by reference in other sections	Require best practices use of wildcards (or restrict altogether) for RP and IdP identifiers.
	63C	5.3.3			Specify reference to "other party" in relationship to receiving a response	Omit - the IdP is required to send and receive notifications of attribute sharing.
	63C				Require that sensitive attribute values not be shared, rather than imposing requirements on subscribers.	Clarify that only the attributes (not values) are provided.
	63C	5.3.4			Not sure of the intent here. RPs shouldn't ask for attributes they don't want to accept.	Consider revising to address the use of allow- and block- lists at the RP to indicate alternate sources of attributes, or omit.
	63C	5.6			The concept of a federation network is not introduced.	Restrict discussion to IdP and Proxies (as an IdP) signaling; RP-to-RP signaling is not recommended.
	63C	5.6			Reverse recommendation for RP to not terminate a session	RPs SHALL be able to terminate a session if the assertion or external attributes available to the RP do not meet its requirements, but MAY allow restricted access...
	63C	6			Consider more generic language that also applies to DIAMETER-like authentication servers using modern (EAP-TTLS e.g.) methods. This is similar to backchannel use case (and it would convenient to have common guidance for this case as well).	

	63C	6.1.2			Consider generalizing the requirement so symmetric keys derived from mutually authenticated (certificate based) channel establishment can be used as (phishing resistant) bound authenticators	
	63C	6.1.2			Consider TLS resumption as a bound authenticator (used independently of the IdP) - this falls in between session validity and assertion validity and this seems to prohibit it if the session key is the bound authenticator.	
	63C	6.1.2.1			Presenting a certificate is not an authenticator	Require proof-of-possession of the private key.
	63C	6.1.2.1			Holder of key is no longer defined.	Omit
	63C	5.6		1180	Reference to 'other API' is not clear. Other attributes can be obtained by an RP through local sources not affiliated to the IdP/federation protocol, or can be obtained via specific channels (attribute API?) of the backend connection.	Clarify using precise language. Indicate that the RP may have locally managed attributes supporting granular access controls, but this is out of scope, and specify if the term attribute API potentially refers to multiple API for various authoritative sources associated with the federation, potentially independent of the IdP.
	63C	7	48	1600	The order of the bullets in the section 7 introduction seems unnecessarily different from the order bullets in the subsections. Furthermore, the use of hyphens (e.g., "front-channel" vs "front channel") is inconsistent.	Switch the order of the two bullets and normalize the hyphenation.
	63C	7.2	51	1658	It is unclear what is meant by "awkward" in this statement. Some potential interpretations are: (1) queries would introduce additional latency (2) queries would require non-standard software, (3) queries would break the definition of the model entirely, as it would seem to imply creation of a back-channel.	Increase the technical precision of this statement.
	63C	8.1, 8.2	54		It seems more logical to split "Assertion Manufacture or Modification" into two cells when considering the adjacent cells in the table.	In Table 2 and Table 3, change the second row of the first column to "Assertion Manufacture" and the third row of the firs
	63C		62	1919	The speculations in this sentence seem more accurately applicable to "social media" providers. Any organization that is capable of serving as an IdP is arguably a "social network" using the colloquial definition.	Replace all instances of "social network" in this sentence with "social media".
	63C	12.3	71	2235	If desired, this appears to be the most appropriate section to introduce technical content on Verifiable Credentials.	Add an informative example section describing a Verifiable Credentials workflow.
	63C				Interoperability, a key consideration for many forward-looking, web-centric credentials schemes, does not appear to have sufficient consideration in this document.	Add an informative "Interoperability Considerations" section. This section can either be standalone or, to better conform to the stated themes of the revision, be placed under usability (interoperability creates better user experiences) or equity (interoperability improves accessibility).
	Base	5.1.4	29	1152	The other bullets on this page describe concrete failure modes while this bullet describes an abstract risk. To improve consistency, this bullet should explicitly describe the analogous failure mode (or modes) associated with the excessive information collection.	Change bullet to "The impact of falling victim to a breach of information that was excessively collected and retained to su
	63-Base	5.2.2.3			Discussion of FAL does not include implications of low FAL on the confidence the RP has in the authentication asserted. For example, an RP should treat an FAL1 assertion susceptible to insertion, but claiming AAL3 authentication of a user as weaker than direct AAL3 authentication of the user to the RP. This high level discussion, including possible constraints on the assertion of high AAL by low FAL should be provided in the base, and reflected in part C.	Add constraints for AAL values asserted by low FAL IdPs.
	63-Base	A.1			Use consistent and precise language to distinguish components of a federation protocol.	Add definitions for federation protocol, trust agreement, federation registration, and assertion transactions (see comment for 63-C above).
	63-Base	A.1			Use consistent and precise language to describe backend interfaces.	Add definitions for identity API, provisioning API and attribute API (or consolidate all as identity API - see comment for 63-C above).
	63-Base	A.1			Avoid loaded terms to avoid unintended requirements or restricted use of this standard.	Conditional on adjudication for comments to 63-C: if 'configuration,' 'logon,' etc. are intended to have different meaning here than in other related standards, provide precise definitions. Otherwise, use generic terms ('registration information,' 'authentication,' etc.) respectively.