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:	*VISA, Inc.*
Name of Submitter/POC:	*Tran-Trong, Ky*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
		General			Visa has made the following comments to draw attention on the risk of deploying passkeys today, in particular where the relying parties carry the risk of impersonation. (Financial Services, Health care, Governement). Visa does not believe AAL2 conditions for passkeys are met without additional controls.	
1	63B	2.2.2 Authenticator and Verifier Requirements			Authentication methods such as Passkeys that claim AAL2 can expose vulnerabilities that can be exploited with simple unmitigated impersonation attacks that cannot be prevented or detected. In the case of Passkeys, i.e. unbound authentication keys, there is no possible check that the authentication keys registered are under control of the genuine user authenticator. i.e "something you have" factor , and "something you know or are" may be bound to a threat actor instead of the genuine user. Additional controls such as device identification or fingerprinting must be added to ensure that spoofed passkeys are not used from an unknown context or device. These requirements are needed to achieve AAL2 with unbound authentication keys. Visa's own testing validates that Passkey registration is vulnerable from simple, global, Man-In-The-Middle passkey spoofing ('swapping') attacks from any browsers (Refer to document : 'Visa Supporting Document for Comments to NIST SP 800-63-4') . Another source has confirmed the attack. (see **https://www.ndss-symposium.org/wp-content/uploads/2024-327-paper.pdf**). A requirement is missing that calls for an additional set of controls or compensating controls for AAL2 authenticators that cannot prevent impersonation.	Add text under 2.2.2 For AAL2, Authenticators and Verifiers SHALL protect against man-in-the middle (MITM) attacks, and detect attempts to register or use a authentication key in a context or device that the user does not have exclusive control on. For example in the consumer domain with payment services, for AAL2, Verifiers SHALL verify passkey binding with trusted platform product ID using attestation cerficates. Moreover, genuine attested authentication keys may be spoofed on browsers with otherwise attested attacker keys, so device identification controls must also be in place. For example in the Enterprise domain, registering the authentication keys using controlled MDM processes on malware-free devices. Verifiers SHALL verify the certificates and return a cryptographic proof to the authenticator indicating the authentication keys used in the backend correspond to keys inside the authenticator.
2	63B	3.1.6.1 3.1.6.2 3.1.7.1			A requirement is missing to bind the authentication keys to real world identities (e.g. passkey public key binding to the authenticators product IDs), so the verifiers can verify such binding, and gain trust that the passkeys are not under attacker control. Unbounded authenticaton keys correspond to no verifiable security or trust, because there are no prevention or detection mechanisms that the RP can use to differentiate attacker keys. MITM attacks spoofing unbounded keys outside a security enclave are easy, global, once a user has installed a browser extension.(Refer to document : 'Visa Supporting Document for Comments to NIST SP 800-63-4'), Refer to https://www.ndss-symposium.org/wp-content/uploads/2024-327-paper.pdf).	Add text Require that Authenticators claiming AAL2 profide a binding verification method (e.g. Certificate-based FIDO attestation) that verifiers can use to check that authentication keys used for authentication are protected by the device.
3	63B	3.1.7.2. Multi-Factor Cryptographic Verifiers			The following is not true for unbound authentication keys, such a unattested passkeys, or self-attested passkeys: "Verification of the output from a multi-factor cryptographic authenticator proves that the activation factor was used.". MITM attacks can be executed that bypasses the activation factor proves that the statement is incorrect. (Refer to document : 'Visa Supporting Document for Comments to NIST SP 800-63-4' , Refer to https://www.ndss-symposium.org/wp-content/uploads/2024-327-paper.pdf).	Indicate that Verifiers can only prove that activations methods are in place if the authent ication keys(i.e. passkey) are truly bound to the authenticator. (in the case of unbound passkeys, Certificate-based FIDO attestation is the minimum standard verification method).
4	63B	3.2.4. Attestation			Certificate-based Attestation must be required to establish any security for the CSP when no other method exists to bind the authentication keys to the authenticator. In particular for the consumer world, the SHALL statement is missing. A requirement is missing for verifiers to assess that the authentication keys (e.g. passkey public key) are bound to a trusted authenticator or device enclave. For AAL2, Verifiers must verify that users, and not attackers are in control of their authentication keys. Basic MITM attacks from web browsers demonstrate the easy substitution of genuine authentication keys with authentication keys known to the attacker. Attestation is necessary but not sufficient against authentication key spoofing, as the threat actor can also use untreaceable attested authentication keys. Device Identification or fingerprinting is a complementary control to ensure that the threat actor cannot use the spoofed passkeys from another device.	For AAL2 and above, Verifiers SHALL Require Attestation (not self-attestation) when there is no other method to bind the authentication keys (e.g. passkey) to its authenticator.

5	63B	5.1. Session Bindings			None of these necessary requirements prevent a MITM passkey spoofing attack.	Indicate that Verifiers cannot rely on browser or client sessions to verify that users are controlling the unbound authentication keys with their authenticators (eg. unattested passkeys).
6	63B	6.1. Authenticator Threats			Threat actors may replace the user authentication keys with their own, or add their own as an example of basic MITM threat, where the user loses control of their accounts. In Table.2, "End-point compromise" indicate that the attacker can substitue the user keys with keys known to the attacker without exporting them.	In "something you have", Indicate that the attacker in the consumer domain can exploit the vulnerability on any account that there is no method to prevent or detect the registration of additional passkeys generated outside the user authenticators.
7	63B	B.2 Cloning of Authentication Keys			Threat actors may conduct a hidden authentication key registration, bypassing user verification or leveraging stolen user credentials. A synchronous authentication step with existing credentials must occur when new authenticatiion keys are being registered.	For AAL2 and higher scenarios, Add the requirement for the user to perform MFA (e.g. AAL2) whenever the user adds a new authenticator or creates authentication keys.
8	63B	B.3 Implementation Requirements			Use cases in highly regulated industries e.g. payments, health care also require attestations. The text should be changed to include the need for attestations in these use cases, as well as those for the enterprise	Change from: "For enterprise use cases, agencies" to "For enterprise use cases and those in highly regulated industries e.g. payments, healthcare, agencies". Change from: "For enterprise use cases, agencies SHOULD implement attestation capabilities" to "For enterprise use cases and those in highly regulated industries, agencies SHOULD implement attestation capabilities Change from: "Attestations SHOULD NOT block the use of syncable authenticators for broad public-facing applications" to "Attestations SHOULD NOT block the use of syncable authenticators for broad public-facing applications BUT RPs providing public-facing applications in highly regulated industries COULD prevent the use of syncable authenticators that do not provide attestations". Change from: "RPs MAY use attestation to determine the level of confidence they have in a syncable authenticator." to "RPs MAY use attestation, or lack of an attestation, to determine the level of confidence they have in a syncable authenticator."
9	63B	B.5 Example			The examples given are necessary but not sufficient for a syncable authenticator to be classified as AAL2. Suggest that the text be make this clear.	Change from: "The following items summarize how WebAuthn syncable authenticators satisfy various aspects of AAL2 requirements:" to "The following items describe how WebAuthn syncable authenticators may satisfy particular AAL2 requirements. However implementation choices made by the WebAuthn syncable authenticator provider also determine whether the authenticator meets AAL2 or not. These implementation choices should be identified and validated against the best practice described in this document and the implementation requirements listed in B.3, to confirm that the WebAuthn syncable authenticator is compliant with AAL2"
10	63B	B.6 Security Considerations			The mitigations given should have a corresponding implementation requirement in section B.3	Ensure that each mitigation provided has an implementation requirement listed in B.3
11	63A	2 through 4			Remote Unattended seems to not have been covered in sufficient detail. There are places in the document, such as Sections 4.1.7, 4.1.8, and 4.1.9, that cover the other 3 scenarios (Remote Attended, Onsite Attended, Onsite Unattended (kiosks)) but not Remote Unattended.	Ensure that the structure of the requirements around all defined types of proofing is sufficiently clear.
12	63A	4.1.7			The threat of deep fakes for remote verification (attended or unattended) is not sufficiently covered. It is only mentioned under 4.1.7, under point #6, that the CSP should introduce challenges and response features. Given detecting deep fakes seems to be a moving target, we believe there should be a fallback option to use SUPERIOR evidence. Additionally, for at least IAL 3, SUPERIOR evidence should be a requirement instead of being only optional.	Ensure that mitigation efforts for the threats posed by deep fakes are adequately covered.
13	63C	3.13	36	1552	Typo: own instead of on	Similarly, a bearer assertion reference can be presented on its own to the RP and used by the RP to fetch an assertion.
14	63C	4.6.1.1	51	1950	Having an allowlist of RPs could mitigate phishing attacks. Hence the suggestion is for the wording to change to 'SHALL (instead of MAY) establish allowlist is required or optional. '	In an a prior trust agreement, IdPs SHALL establish allowlists of RPs authorized to receive authentication and attributes from the IdP without a runtime decision from the subscriber.
15	63C	10.1	103	3501	Typo: deleted "are" from "All of these scenarios are involve the same subscriber account"	All of these scenarios involve the same subscriber account.