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:	*Wiz, Inc.*
Name of Submitter/POC:	*Chris Carpenter*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	3.1.3			"A third method of out-of-band authentication compares secrets received from the primary and secondary channels and requests approval on the secondary channel.This method is no longer considered acceptable because it increased the likelihood that the subscriber would approve an authentication request without actually comparing the secrets as required. This has been observed with “authentication fatigue” attacks where an attacker (claimant) would generate many out-of-band authentication requests to the subscriber, who might approve one to eliminate the annoyance. For this reason, an authenticator that receives a push notification from the verifier and simply asks the claimant to approve the transaction (even if they provide some additional information about the authentication) does not meet the requirements of this section." The two bolded sections are not equivalent. Simply asking for approval does not require the comparison of secrets. Push notifications that simply ask for approval are the typical avenue for authentication fatigue attacks. However, comparing secrets (typically implemented as matching displayed numbers) should be acceptable at least at lower assurance levels for implementations that disallow additional notifications or implement additional verification measures if an incorrect match is received (such as a notification to an approved email address or secondary contact method). In that case, a subscriber will not receive more than one request and cannot be the victim of an authentication fatigue attack. Further, if the subscriber is presented with an authentication prompt from a malicious website, the numbers will not match because they are generated by a shared secret between the primary and secondary devices. While this is still not phishing resistant because it involves user interaction, it is arguably more resistant than inputting an out-of-band secret from a secondary device to the primary. -- Matching secrets as suggested above more effectively demonstrates user control of the secret and the authentication session than inputting a secret from the secondary device. In the latter circumstance, physical possession of the device is only required to retrieve the secret, not to authenticate with it, and provides zero to low assurance that the party authenticating physically	1. Allow comparison of secrets from primary and secondary channels WITHOUT device authentication as a “something you have” factor for AAL1
	63B	3.1.3			"A third method of out-of-band authentication compares secrets received from the primary and secondary channels and requests approval on the secondary channel.This method is no longer considered acceptable because it increased the likelihood that the subscriber would approve an authentication request without actually comparing the secrets as required. This has been observed with “authentication fatigue” attacks where an attacker (claimant) would generate many out-of-band authentication requests to the subscriber, who might approve one to eliminate the annoyance. For this reason, an authenticator that receives a push notification from the verifier and simply asks the claimant to approve the transaction (even if they provide some additional information about the authentication) does not meet the requirements of this section." The two bolded sections are not equivalent. Simply asking for approval does not require the comparison of secrets. Push notifications that simply ask for approval are the typical avenue for authentication fatigue attacks. However, comparing secrets (typically implemented as matching displayed numbers) should be acceptable at least at lower assurance levels for implementations that disallow additional notifications or implement additional verification measures if an incorrect match is received (such as a notification to an approved email address or secondary contact method). In that case, a subscriber will not receive more than one request and cannot be the victim of an authentication fatigue attack. Further, if the subscriber is presented with an authentication prompt from a malicious website, the numbers will not match because they are generated by a shared secret between the primary and secondary devices. While this is still not phishing resistant because it involves user interaction, it is arguably more resistant than inputting an out-of-band secret from a secondary device to the primary. -- Matching secrets as suggested above more effectively demonstrates user control of the secret and the authentication session than inputting a secret from the secondary device. In the latter circumstance, physical possession of the device is only required to retrieve the secret, not to authenticate with it, and provides zero to low assurance that the party authenticating physically	2. Allow comparison of secrets from primary and secondary channels WITH device authentication as a “something you have” factor for AAL2

	63B	3.1.3			"A third method of out-of-band authentication compares secrets received from the primary and secondary channels and requests approval on the secondary channel.This method is no longer considered acceptable because it increased the likelihood that the subscriber would approve an authentication request without actually comparing the secrets as required. This has been observed with “authentication fatigue” attacks where an attacker (claimant) would generate many out-of-band authentication requests to the subscriber, who might approve one to eliminate the annoyance. For this reason, an authenticator that receives a push notification from the verifier and simply asks the claimant to approve the transaction (even if they provide some additional information about the authentication) does not meet the requirements of this section." The two bolded sections are not equivalent. Simply asking for approval does not require the comparison of secrets. Push notifications that simply ask for approval are the typical avenue for authentication fatigue attacks. However, comparing secrets (typically implemented as matching displayed numbers) should be acceptable at least at lower assurance levels for implementations that disallow additional notifications or implement additional verification measures if an incorrect match is received (such as a notification to an approved email address or secondary contact method). In that case, a subscriber will not receive more than one request and cannot be the victim of an authentication fatigue attack. Further, if the subscriber is presented with an authentication prompt from a malicious website, the numbers will not match because they are generated by a shared secret between the primary and secondary devices. While this is still not phishing resistant because it involves user interaction, it is arguably more resistant than inputting an out-of-band secret from a secondary device to the primary. -- Matching secrets as suggested above more effectively demonstrates user control of the secret and the authentication session than inputting a secret from the secondary device. In the latter circumstance, physical possession of the device is only required to retrieve the secret, not to authenticate with it, and provides zero to low assurance that the party authenticating physically	3. Update this section and/or other relevant sections to discuss the nuanced security considerations of transferring a secret fr
	63B	3.1.3			"A third method of out-of-band authentication compares secrets received from the primary and secondary channels and requests approval on the secondary channel.This method is no longer considered acceptable because it increased the likelihood that the subscriber would approve an authentication request without actually comparing the secrets as required. This has been observed with “authentication fatigue” attacks where an attacker (claimant) would generate many out-of-band authentication requests to the subscriber, who might approve one to eliminate the annoyance. For this reason, an authenticator that receives a push notification from the verifier and simply asks the claimant to approve the transaction (even if they provide some additional information about the authentication) does not meet the requirements of this section." The two bolded sections are not equivalent. Simply asking for approval does not require the comparison of secrets. Push notifications that simply ask for approval are the typical avenue for authentication fatigue attacks. However, comparing secrets (typically implemented as matching displayed numbers) should be acceptable at least at lower assurance levels for implementations that disallow additional notifications or implement additional verification measures if an incorrect match is received (such as a notification to an approved email address or secondary contact method). In that case, a subscriber will not receive more than one request and cannot be the victim of an authentication fatigue attack. Further, if the subscriber is presented with an authentication prompt from a malicious website, the numbers will not match because they are generated by a shared secret between the primary and secondary devices. While this is still not phishing resistant because it involves user interaction, it is arguably more resistant than inputting an out-of-band secret from a secondary device to the primary. -- Matching secrets as suggested above more effectively demonstrates user control of the secret and the authentication session than inputting a secret from the secondary device. In the latter circumstance, physical possession of the device is only required to retrieve the secret, not to authenticate with it, and provides zero to low assurance that the party authenticating physically	4. Update the paragraph cited to either: - If items 1 and/or 2 are accepted: narrow the disallowed use case to simply asking for approval and update relevant sections to describe acceptable conditions for use of compared secrets - If items 1 and 2 are rejected: align the highlighted sections of the paragraph to clarify that both use cases are disallowed