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:	*Cisco Security Business Group*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	5.1.3.2			Requiring 20 bits of entropy for the random authentication secret has usability implications. Analyzing real usage trends for Duo Security's Verified Push feature over a 28 day period (we can provide this data if needed), authentication failure rates increase 3-5% when end users must enter a 6 digit code instead of a 3 digit one.	Current best practice is to match user friction with risk/trust (i.e. it's a spectrum). Specifying 20 bits of entropy as a hard, unconditional requirement disregards other signals that may otherwise tip the trust calculation in favor of a better user experience. Indeed, in Section 5.2.2 ("Rate Limiting (Throttling)"), allowances are made for risk-based or adaptive authentication techniques to identify user behavior that falls within typical norms. It would be useful to implementors if these same affordances were applicable to the specifics of the actual claimant verification process.
2	63B	5.1.3.2			It would be helpful to clarify if implementors are permitted to "round up" with respect to the 20 bit entropy requirement for out-of-band device secrets. Specifically, when the secret is composed only of the digits 0-9, then 6 digits has an entropy of (log2(10) * 6 == ~19.31) which falls just short of 20. It would be unfortunate to require additional digits or an expanded character set just to satisfy the remaining delta of 0.69. Note that we prefer to stick with 0-9 as the only entry options since it is simpler for the user and allows for less error-prone entry modalities such as numerical keypads (think of e.g. the Apple Watch as a UI).	Add text to explicitly allow for these parameters and/or provide examples to make it clearer.
3	63B	5.1.3.2			In analyzing various attack schemes, we've concluded that transfer of secret from the primary to the secondary channel is more phishing-resistant than secondary to primary because it increases the complexity for the attacker. Specifically, consider a scenario where the primary channel is the web and the secondary channel is a smartphone app. If the authentication secret is sent to the user's phone, an attacker can build a phishing experience that collects both the user's password and secret through a fake web site. If the authentication secret is instead displayed through the web app for the user to enter into their phone, it increases the complexity for the attacker because they'll need to implement additional interactions to collect the code from the real service, display it to the user through the fake site, and still trick them into entering the secret into their phone.	In the 800-63B document, these two options are prefaced with the text "depending on the type of out-of-band authenticator", but there's no further guidance on which one is preferable based on all of the possible authenticator types and authentication scenarios. Perhaps this is intentional for brevity and flexibility's sake, but there may be room for expansion here.
4	63B	5.1.9.1			The description of the multi-factor cryptographic device authenticator type is clearly noted to "use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator that SHALL NOT be exportable". However, FIDO passkeys are typically adopted as multi-device credentials in practice, and despite it being an emerging standard, has a decent shot at wide adoption as a strategy to replace passwords. That said, there is a new WebAuthn extension called "devicePubKey" which allows multi-device user credentials to be paired with an automatically-generated device-bound credential which restores the strong binding to a particular device.	Consider whether the devicePubKey extension could be employed by a CSP to meet AAL3 requirements for FIDO passkeys.
5	63-Base	4.1	11-14		there is no clear distinction between a non-federated versus a federated model. The figures show a subtle difference by the location of the RP within a box (non-federated) and separated in a federated.	Consider including a richer explanation, perhaps by example to more clearly define the locality and trust relationships as required when the RP, Verifier and CSP are not "co-located" specifically as their trust domains are not rooted by the same organization and thus trust must be specified between them to comply with the different assurance levels.
6	63B	5.1.3.2	22	903	As the authenticator is requesting the 2nd factor over a secured channel, we'd like to better understand the rationale for the 20bit entropy minimum requirement as we believe the rate limiting cadence can help reduce the required entropy if the window is small enough. This is especially the case for the multi-factor use case.	Consider including the rate limit window as a factor to allow the entropy to be something less given a much shorter verification time and rate limit window.
7	63B	5.1.3.4	23	933	As this refers to section 5.1.3.2 it may be that this section SHOULD relax the entropy considerations as the out-of-band authenticator is used as a multifactor.	
8	63B	5.1.6.2	27	1086	Software verifiers should have more considerations by nature that software is more susceptible to attacks than hardware. I believe the rationale is that as both are "verifiers" the nature of the verifier role, whether software or hardware is independent.	Suggest clarifying or providing a rationale for why security remains whether the verifier is software or hardware based
9	63B	5.2.2	31	1235	Is there quantitative data for why the number attempts may go to 100? Or perhaps better guidance is to provide a minimum?	