From: [redacted]
To: dig-comments@nist.gov
Subject: [dig-comments] Brief comments on 63B-4
Date: Monday, October 7, 2024 4:30:39 PM

Dear SP800-63-4 team,

I would like to make brief comments on some biometrics aspects. And additionally, below please see a general comment 3/ with respect to MFA that can be improved to my opinion.

1/ Related to PAD:
Line 1277 “Presentation attack resistance SHALL be tested in accordance with Clause 13 of [ISO/IEC30107-3].”
Unfortunately, this is well known that the testing based evaluation that have been developed so far are not able to catch the vulnerabilities of the state of the art solutions. Instead, security evaluation methodologies exist to ensure an evaluator will focus on trying to find vulnerabilities (and, as a bonus, not only on PAD but also on other kind of biometric vulnerabilities). Thus requirement related the being evaluated following security evaluation methodologies ISO/IEC 19792 or ISO/IEC 19989 (all parts) should be added.

2/ Related to local vs central processing of biometrics
Line 1298 “Since the potential for attacks on a larger scale is greater at central verifiers, comparison SHOULD be performed locally.”
The statement is not fully correct – attacks against the authentication process are different if biometrics are processed centrally vs locally but there are implementations for which it becomes way easier to do an attack locally, and that may also be replicable at scale (large scale RCE on weak end points for instance). While the statement seems to be more related to privacy risks (that may lead to security threats, sure, but depending as well on other security controls). Instead, I think we should here follow the approach taken by ISO/IEC 27553-1 vs ISO/IEC 27553-2 where the choice of central processing has to be justified, and if so additional security controls have to be implemented centrally to reduce the risk of the central verifiers to become an appealing target for hackers or to represent a huge risk of privacy leakage.

The reference to the use of ISO/IEC 24745 has disappeared compared to previous version of SP800-63. This should be corrected as this is very important to ensure the right level of protection is in place to protect biometric information.

Remark: “Line 1278 The PAD decision MAY be made either locally on the claimant’s device or by a central verifier.” Note that for some use cases, for instance mobile or lightweight endpoints, current solutions when not relying on specific additional sensors for PAD, so when using regular sensor with no specific hardware based PAD embedded, are often more robust to attacks when deployed on central rather than local, due to the computation/processing limitations on local vs resources available on central (and the capability to more easily update to cope with new presentation attacks species). Thus PAD often happens on central verifier.

Which implies that it is more logical to then make the comparison on central too.

3/ General comment: some multi-factor cases in the document are wrongly stated as multi-factor. They include the use of different factors but this is not necessarily a multi-factor authentication. Instead they are often related to a preliminary unlocking step before using the unlocked factor for single factor authentication toward the verifier. For instance line 2377 case of OTP unlock by a 1st factor.
Although we have been using the concept of MFA to cover those cases, they are weaker and led to weak choices for levels of security risks that would require strong MFA. Consequently, we should clearly make the distinction between what is really verified by the verifier and what is related to the protection of the primary authentication factors. To avoid confusion, we should use different terminology or add extra security recommendations if one of the factors is used only locally.

Feel free to contact me if some additional clarifications would be required.

Best regards,
[redacted]