From: [redacted]
To: dig-comments@nist.gov
Cc: [redacted]
Subject: [dig-comments] Public Comment on 800-63-4 [redacted]
Date: Monday, October 7, 2024 4:54:03 PM

Hello. We would like to submit a public comment to NIST publication 800-63-4 (including SP 800-63B). This comment is based on work being done by our company, Dapple Security, under a NIST SBIR Phase I project. This project aims to look at the security of using biometric data as a source of randomness to create and/or recover cryptographic keys. As such, we want to try to ensure that 800-63-4 would allow for this. In particular, we could consider the following 3 modes:

1. biometric as the only source of randomness for key generation
2. biometric as a partial source of randomness for key generation
3. biometric used as a factor in key recovery

We concede that it is likely far too early to consider including 1. in the standard as there is much to be understood about the security performance of this mode. However, Modes 2. and 3. would require more minor changes to the standard as written. In particular:

800-63-4
The definition of 'sync fabric' and 'syncable authenticators' assume that authentication keys will be cloned or exported from the user's device in their entirety. It does not contemplate the possibility that keys could be *synced via a recovery process* on different/new devices, where the recovery process does not rely on stored keys nor stored/issued recovery codes. See comment below on recovery.

SP 800-63B
Section 4.2.1 Account Recovery Methods requires recovery codes to be either Saved or Issued, or to use recovery contacts or identity proofing. It does not contemplate a recovery code being reproduced by some other means, such as using a biometric reading to reproduce a recovery code, or combining a biometric reading with a partially-stored code to reconstitute the full recovery code. That said, if either of these ways of using a biometric could be considered identity proofing, then no changes would need to be made to the standard as written to accommodate this use case.

Thank you for your consideration.
Gadalia

Gadalia Montoya Weinberg O'Bryan
[redacted]