From: Kyle Neuman
Sent: Tuesday, August 11, 2020 7:49 AM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Subject: NIST 800-63-4 Comments

Hello,

We are please to have the opportunity to suggest input on a future revision of NIST 800-63. We acknowledge this is a late submission and hope you will still read and consider our comments below:

- Remote Proofing Maturation – SAFE Identity recommends further development of performance requirements for facial recognition utilizing the camera image from a smart phone, tablet or webcam (live-selfie).

  Today, SP 800-63 directs developers and implementers to use biometric matching FMR numbers – but this approach is less than optimal for the live-selfie topic. There are increasing numbers of vendors attempting performance requirements for live-selfie-to-credential face matching and it's difficult to determine whether the binding verification step is being done in a manner that meets the spirit of SP 800-63.

  SAFE Identity believes capitalizing on the capabilities of smart phones and other devices for facial recognition will greatly expand the applicability and usefulness of biometrics with the general public. This is particularly valuable in healthcare applications for doctor/patient communication.

- One of the primary decisions made when the SP 800-63-3 suite of documents replaced SP 800-63-2 was reimagining the (4) four Levels of Assurance found in SP 800-63-2 into three (3) Identity Assurance Levels (IAL), three (3) Authenticator Assurance Levels (AAL) and three (3) Federation Assurance Levels (FAL). However, this has resulted in a very broad IAL 2 which does not provide any delineation between a remote identity proofing event and an in-person (or supervised remote) identity proofing event. In addition, this category is so broad it encompasses a large majority of the actual identity proofing solutions/processes.

  On a related note, IAL3 is exceedingly narrow and almost impossible to achieve. Within the Federal Government, the PIV credential meets IAL3 only because of "compensating controls." Establishing an IAL that is out of reach even for Federal organizations would seem to be self-defeating.

  SAFE Identity recommends reconsidering the IAL requirements and offers three suggestions.

1. Return to four (4) IALs by dividing the IAL2 to separate remote proofing from in-person proofing; or
2. Reconsider the requirements of IAL3 to make them more achievable for industry and government implementers and move all in-person proofing into that IAL; or
3. A combination of 1&2 above – Return to four (4) IALs, dividing IAL 2 to separate remote proofing from in-person proofing *and* reconsidering the requirements of the highest IAL (IAL4?) to make them more achievable for industry and government implementers.

- In the three tables in Section 5 of SP 800-63A – Table 5-1 Strengths of Identity Evidence, Table 5-2, Validating Identity Evidence, and Table 5-3, Verifying Identity Evidence – *Weak* Identity Evidence is defined. It sits between *Unacceptable* and *Fair*. However, there is no further reference to a process that would utilize *Weak* identity evidence, validation or verification. This begs the question as to why it is included and is *Weak* synonymous with Unacceptable (and if so, why are they not a single category)?

SAFE Identity recommends removing the reference to *Weak* identity evidence, validation and verification from the document.

- In Section 6 of SP 800-63-3, *Selecting Assurance Levels*, an assessment of various impact categories is established for each of the three assurance levels, which can be applied across identity, authenticator and federation. However, there is no discussion of *likelihood* in association with the impact categories. The Low, Medium and High designations would seem to be limited to the actual impact, not its likelihood.

SAFE Identity recommends including the likelihood of an impact occurrence in Section 6 through the use of a heat map or other device.

If you would like to discuss any of the above items or have need of clarification, please don't hesitate to contact me as indicated below.

Sincerely

Kyle Neuman