From: Pivoris, Robert
Sent: Monday, August 10, 2020 3:00 PM
To: dig-comments-RFC <dig-comments-rfc@nist.gov>
Subject: Comment for NIST SP 800-63-4

Thank you for the opportunity to provide comments on potential changes to NIST SP 800-63-3 Digital Identity Guidelines.

Our comment pertains to NIST SP 800-63B Authentication and Lifecycle Management. SP 800-63B, Section 4.5, Table 4-1 outlines the following permitted authenticators for Authentication Assurance Level 2 (AAL2):

- MF OTP Device;
- MF Crypto Software;
- MF Crypto Device;
- or Memorized Secret plus one of the following:
    - Look-up Secret
    - Out-of-Band
    - SF OTP Device
    - SF Crypto Software
    - SF Crypto Device

We believe it is common practice to recognize a known, trusted device as a “something you have”/possession based authentication factor. As an example, when a user authenticates for the first time on **login.gov** using a device (let’s call it device A) that has not been associated with the user’s account in the past, the user is challenged with two factors (e.g., password and SF OTP Device). Subsequent authentications to that account from device A require just a single factor such as password as device A is implicitly considered as a possession factor; if the same account was accessed from device B that had not previously been associated with the user’s account, then the user would again be challenged with two authentication factors (e.g., password and SF OTP Device). We see similar security approaches in online banking and other online services (e.g., email, e-commerce). We believe that known, trusted device is a robust authentication factor and not highly prone to compromise.

We are asking NIST to consider the industry practices described above, and add language to BIST 800-63-4 that recognizes a known, trusted device as a “something you have”/possession based authentication factor that when used in conjunction with a Memorized Secret, meets the criteria for Authentication Assurance Level 2 (AAL2).

Regards,

Bob Pivoris.