Issues Identified after Completion of the Final Report

- Given the latest NIST draft do we want to deprecate or disallow SMS codes?
- Should there be guidance for “remembered/trusted devices”?
  - *In the new draft 800-63, AAL2 requires multi-factor authentication and requires a user to authenticate fully every 12 hours. In the Duo context, this would require 12 hour "trusted device" settings.*
- Any requirements or guidance about written backup codes?
  - Specifically, Duo allows for “bypass codes” which can have arbitrary lifetimes AND that can be reused. Is authenticating with a reusable bypass code acceptable?
- Any recommendations that vendors (I’m looking at you Duo…) provide more visibility to client applications as to what mechanism was used for MFA authentication?
  - E.g., a campus may allow the use of Duo Bypass codes, or “remember this device”, but the IdP has no way (AFAIK) to see that this was used. So if an IdP wanted to allow reusable Duo Bypass codes for access to some applications but not to others, I don’t think they can.
- In MFA Technologies, Threats, and Usage we don't explicitly allow for an IdP to separately (a) verify your device's access to a (non-password secured) locally installed private key and (b) authenticates the user via forms (username/password). It seems like this would be okay, however, we don't clearly identify it as acceptable because all of the explicitly listed PKI-challenge based solutions in Table 1 (#11-14) indicate that password protection exists at the cert/device level. (Non-password protected H/TOTP tokens are listed, but not PKI challenge based ones).

  - A future, updated version of this page should probably include enough information to clarify that this approach (IdP performs separate key and password challenges) is acceptable.