NRI Secure Technologies, Ltd

I think there are several uncertain/ambiguous expression in 63B, so I comment as follows:

1) Some authenticators named "Device" are ambiguous as to whether they are hardware or software
Single-Factor OTP Authenticators are mentioned that "This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones." in Sec 5.1.4.
However other "hardware" authenticators(e.g., "Single-Factor Cryptographic Device Authenticators") are all named "Device" and explicitly distinct from "software" authenticators(e.g., "Single-Factor Cryptographic Software Authenticators")

Thus, I think that "Single-Factor OTP Authenticators" should be divided into "Device"(hardware) and "Software".

2) NIST should explain the difference between "Multi-Factor" and "Multi-Step" authentication.
PCI-DSS introduces "Multi-Step" authentication in the following documents.

NIST has no responsibility to mention about a specific industry, however the insight should be provided by NIST.
Technically speaking, some kinds of action need an email ID prior to inputting the 2nd factor value.
In fact, GAFA's authentication flow is not multi-factor but multi-step in the view of PCI and ambiguous.

Because of the above reason, I think that 63B should mention multi-step authentication.

3) Double standard about "memorized secret periodically changed" in
5.1.1.2 Memorized Secret Verifiers should be mentioned.
63B stated that 'Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)', then this policy transition caused lots of discussion.
NIST's new policy is acceptable especially for Web sites(e.g,. EC), however it conflicts with PCI-DSS's policy.

I propose that 63B show the difference between end-users and administrators/operators.
To show my intention, please see the following example.
- For end-users including US government staff, 63B's approach works well.
- For administrators/operators, traditional periodical password renewal policy may also work well because such persons can renew their password complicated enough according to the policy.

4) Use case of some OOB methods which do not prove possession should be mentioned.
63B says that "Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication." in Section 5.1.3.1.
Actually, Google and Microsoft don't use such purpose, but use email OOB as a method of end-user account recovery flow with additional countermeasures.
For example, in Google's flow, if google account chooser memorize "logged-in" history, account recovery successfully finished right away, and if not, additional information is required.

I recognize that such an account recovery flow is one of the implementations of "Replacement of a Lost Authentication Factor".

If my understanding is correct, I offer to add the following example:
"Such a OOB method MAY be used for the purpose of account recovery, and then the verifier should verify other additional attributes implicitly to confirm whether user access from customary environment or not. "

5) How csp does Identity Proofing to rebind authenticators for account recovery is ambiguous.
63B says that "As an alternative to the above re-proofing process when there is no biometric bound to the account, the CSP MAY bind a new memorized secret with authentication using two physical authenticators, along with a confirmation code that has been sent to one of the subscriber's addresses of record." in Sec6.1.2.3.

The word "physical authenticators" is first occurrence in 63-3 publication and 63A doesn't mention "physical authenticator".
AAL doesn't mention the number of physical authenticators, but multi-factor.
Please consider adding concrete examples to clear up any ambiguity I mentioned at the above.

Related to 6, my understanding is that Google and Microsoft using email(login ID) for account recovery don't comply with rebinding using two \"physical" authenticators and that is because IAL is 1 (Self-Evident).
Because some people might have questions about it, please consider mentioning this point.

That's all.

Regards
Tatsuya KATSUHARA