| Comment # | (Base, 63A, Section | | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| | 63B | | | | Besides the cryptographic authenticators', authentication secrets of other types of authenticators can be synced (e.g., password and TOTP in a password manager). To avoid confusion, it may be better to rephrase "syncable authenticators" with "synched cryptographic authenticators" in the guidelines. | Replace all "synched authenticators" with "synched cryptographic authenticators" in the guidelines. "Synched" directly implies that the cryptographic key "was exported". |
| | 63B | 3.1.7.1 | 27 | 1153 | Users are able to use private keys for WebAuthn synced to another device without user verification under certain conditions (e.g., if a WebAuthn RP is setting UV as discouraged and the authenticator is not conducting user verification), which means that syncable authenticators can be also applied to single-factor cryptographic authentication. | Copy the paragraph regarding syncable authenticators (line 1153-1155) to section 3.1.6.1 Single-Factor Cryptographic Authenticators. |
| | 63A | 2.1.2 & 3.13.1 | 7 & 31 | 555-571 & 1354-1387 | While the section describes the responsibilities of Proofing Agent and Trusted Referee, this section does not provide clear requirements to qualify individuals to perform these tasks on behalf of CSP. These individuals are in trusted position and yet, we do not have explicit requirements on vetting these individuals to assume the critical task of identity proofing, authenticity detection, error handling, etc. Yet, it is required for CSP to identity proof an applicant reference to the same or higher IAL intended for the applicant. | Suggest to add the explicit requirements for CSP to Identity Proof their Proofing Agent and Trusted Referee at the same or higher IAL intended for the Identity Proofing service. |
| | 63A | 2.4 | 10 | 649 | An expired identity evidence can accepted as valid identity evidence and can be use for Identity validation is problematic as it is unclear if an expired identity edvidence represent the same categoriy of a non-expired one. Expired Identity edvidence will likely present outdated identity attributes. And in some use case such as the issuance of digital identity credentials, the use of expired identity evidence is not | Recommend NIST to specify that the use of expired identity evidence is only permitted for IAL1. |
| | 63A | 3.1.12 | 31 | 1337 | Throughout the volume A, there are requirement for CSP to have Proofing Agents and trusted referees be trained, assessed and certified annually | Please kindly clarify the term "certified". Is it sufficient for CSP self-attest that the specific trainings have taken place and provide documentation of such training assessment? |
| | 63A | Appendix A.1 | 78 | | Not all fair evidence listed as examples presents validatable physical security features. Therefore, a note should be added to clarify that only Student ID/Corporate ID card/Snap Card with machine readable security features can be accepted as a form of fair evidence. In some case, some physical security features cannot be evaluated for tampering due to the proprietary nature of the security feature. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 63A | Appendix A.3 | 82 | | mDL is listed as an example for Superior Evidence with the assumption that proofing is done leveraging State Issuance Processes, Compliant with AAVMA Guidance "**AND**" Real ID Act. This is assuming that mDL issued are based on Real ID compliant driver license which is not necessarily the case in many jurisdiction. Once the Real ID act enforcement date starting on May 7 2024, please clarify whether will a non Real ID mDL or mID still be considered as superior evidence? In additional, State DMVs can elect not to comply with AAMVA mID implementation guidelines as they elect not to take part in the AAMVA Digital Trust Service. | Please kindly clarify if "AND" is compounding all 3 proofing requirements. |
| | 63C | 5.1 | 69 | 2508 | According to the current ISO 18013-5 standard that the majority of US mDL is based on, there is no defined or approved protocol to present an activation factor | Please provide an example of a proof for Wallet's signing key. |
| | 63C | 5.2 | 70 | Fig 13 | The figure shows that Subscriber-Controlled Wallet would provide "Wallet Key" to CSP. | Assuming Wallet key refers to Wallet Signing Key, please clarify how is this guidance comply with the current ISO 18013-5 standard AND AAMVA mDL Implementation guideline. |