CARDHOLDER AUTHENTICATION

Comments Accepted

- Flexibility is added in authentication mechanisms to allow for implementation variations.
- The output of all authentication mechanisms have been changed from FASC-N to a unique identifier.
- CHUID is inherently weak as an authenticator. CHUID is deprecated as an authentication mechanism.
- Added hooks to reference other activation mechanisms (e.g., On-Card Biometric Comparison) as specified in [SP 800-73].
- VIS and CHUID has been down graded to “LITTLE or NO CONFIDENCE" assurance level.

Comments Accepted (cont'd)

- All authentication mechanisms are updated to ensure card expiration date is checked. In some cases, authentication mechanism characteristics are updated to highlight that card revocation is not checked.
- Added a note that "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document."

Comments Declined

- Use on-card biometric authentication is not wise. Recommend the on-card biometric authentication be eliminated.
- The document should mention authentications which can be done by external systems (e.g., PIN-to-PACS) using the PIV card as an index to a previously established authentication mechanism.
- Define a separate electronic secure VIS authentication.
- The requirement to obtain VERY HIGH Confidence is inadequate. Recommend Table 6-2 entry be modified to require BIO or BIO-A and PKI-AUTH.
- BIO needs to be part of remote/network system environment.

Questions (?)