

TECHNICAL

1. What is the rationale behind the selection of smart card, fingerprint, and PKI technologies?

The presidential directive required a standard for secure and reliable identification and authentication of federal employees and contractors that incorporates rapid electronic validation, but did not specify how to achieve it. Several organizations (most notably DOD) had on-going smart card programs that demonstrated the efficacy of this technology in meeting the needs of HSPD-12. The decision to include PKI and fingerprint technologies was made to improve the security profile of the smart card for both physical and logical access. PKI provides a digital credential that can be used to electronically verify the identity of the cardholder, while the fingerprint ties the card irrevocably to a specific individual and can be used to ensure the cardholder is the individual to whom the card was issued. Of the several potential means of personal biometric marker verification (e.g., DNA, iris scans, hand geometry, handwritten signatures, facial images, or fingerprints), fingerprints were chosen as being the least invasive and most cost-effective, reliable, repeatable, and accurate means of verification available using publicly available technology.

2. What information must be stored on the card?

The PIV Card must contain the following mandatory Personally Identifiable Information:

1. Personal Identification Number (PIN)-this data is used to authenticate the cardholder to the card--in the same way a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card.
2. A Cardholder Unique Identifier (CHUID)-this number uniquely identifies the individual within the PIV system.
3. Two fingerprint biometrics that are PIN protected.
4. One asymmetric cryptographic key pair used to authenticate the card to the PIV system.

3. PIN Reset requires biometric authentication. Can this be accomplished remotely by providing unlock codes during in-person enrollment or issuance or is in-person appearance required?

For PIN resets, in-person appearance to authenticate identity is required. Identity authentication is accomplished through a biometric match to verify identity at the time of PIN reset. This is a security feature of the process. (Ref: FIPS 201 Section 5.3.2.3)

4. If password manager products are considered a related subsystem, do these related subsystems need to be FIPS 201 compliant?

FIPS 201 does not specify password manager product requirements. However, where such products are considered PIV applications, the PIV authentication use cases in FIPS 201 Section 6 apply.

5. How should the PIV enrollment systems, issuance systems, and other clients communicate with and transfer these records to and from the Identity Management System (IDMS)?

A set of standard interfaces is currently being developed. Information on these can be found at <http://www.idmanagement.gov>.

6. Are PIV cards limited to the PIV card applications described by FIPS 201 or can additional applications and data objects be stored on the PIV card?

It is possible for a PIV card to contain non-PIV card applications, and those applications may contain non-PIV data objects. However, non-PIV applications and data objects cannot be used to supersede the operational use of the PIV application and data objects thereby hampering

interoperability.

7. Should the PIV Data Model be considered fixed or can any Issuing Agency add more buffers (or containers) to meet their specific requirements?

New data objects may only be added to the PIV data model via formal revisions to the PIV standards and specifications, to ensure strict interoperability. In these cases NIST will assign new labels from the PIV namespace. However, it is possible to add proprietary data objects to non-PIV applications that reside on a PIV card.