Comment on Draft FIPS 201 Standard (HSPD-12)

Point of Contact

Mark L. Silverman

Comment Type

Technical

Section and Page Number

4.2, Page 25

Comment and Rationale

The PIV card must have a persistent Federal identification number (PFID) associated with each card holder. A PFID is necessary to support the PIV-1 identity proofing and registration process (section 2.2, page 4) and enable the use of the PIV card's digital certificate to provide logical access to Federal IT systems.

A PFID is needed to cross-reference and link the various stages of the identity proofing process together. The PFID will provide linkage between PIV data and other Agency personnel records. The PFID will enable reference to historical data, such as the subject's previous criminal and background checks (section 2.2.2, page 7). Without the PFID, it will be very difficult to correlate an individual's PIV actions across multiple Agencies and/or employment relationships (e.g., contractor becoming Federal employee).

Logical access is almost impossible without a PFID. A digital certificate binds the holder's identity to their public key. As proposed (section 4.3, page 29), the authentication digital certificate does not contain a persistent identity except for the common name (CN), which is seldom unique. Therefore, Federal IT systems will be forced to do a series of directory lookups in order to match the holder's current PIV FASC-N with some other usable persistent identifier. A PFID will enable strong logical authentication is a single step and simplify authentication to Agency independent Federal IT systems (e.g., OPM online).

Proposed Change

A possible approach for implementing a persistent Federal identification number (PFID), within the construct of the current FIPS 201 standard, would be to have the “optional” 16 character GUID field of the CHUID (PACS 2.2 Guidance, page 10), become the “required” PFID. The format of this number could be similar to the FASC-N, in that the first 8 characters be the Agency and System code of the original issuer. Once issued, the first 8 characters would have no special meaning other than to ensure uniqueness. Alternatively, the 10 character PI field of the FASC-N could serve as the PFID, except that the longer GUID field provides a better mechanism (as suggested) to ensure uniqueness.

The GUID field could replace the FASC-N in the certificate’s subject alternative name extension or be added to the subject’s distinguished name (DN) as a UID attribute (OID 0.9.2342.19200300.100.1.1). This later approach would help ensure name uniqueness within the DN and also provide out-of-the-box interoperability with commercial authentication solutions (e.g., Netegrity’s Siteminder).