Overview and Summary of Changes made from Special Publication 800-73-1 to Special Publication 800-73-2

NIST is pleased to announce the release of NIST Special Publication 800-73-2, *Interfaces for Personal Identity Verification*. Special Publication 800-73-2 (SP 800-73-2) specifies the PIV data model, command interface, client application programming interface and references to transitional interface specifications. The four parts that comprise SP 800-73-2 supersede the single document SP 800-73-1, published in April 2006. Comments received for first and second public draft of SP 800-73-2 have been addressed as are the errata items in SP 800-73-1. The high-level technical changes in SP 800-73-2 are summarized below.

Part 1: End-Point PIV Card Application Namespace, PIV Data Model and Representation

- A possible PIN interoperability conflict has been identified and corrected. SP 800-73-1 allowed the PIV card application PIN and optionally a Global PIN to satisfy access control rules for reading PIN-protected data object. SP 800-73-1, however, did not provide a mechanism for card readers to discover which of the PINs to use for PIN verification. To correct the deficiency, SP 800-73-2 Part 1 has provided an optional Discovery Object data element, containing the PIN usage policy sub-element, allowing card readers and relying systems to discover which PIN to use for verification.

- All PIV cryptographic keys types, cryptographic algorithm identifiers and key sizes previously listed in SP 800-73-1, are now specified in SP 800-78-1 *Cryptographic Standards and Key Sizes for Personal Identity Verification*. Neither SP 800-78-1 nor SP 800-73-2 specify a mandatory/default algorithm and key size for the PIV key types. Instead, each PIV key types can be implemented from a small subset of algorithms and key sizes as specified in Table 3.1 of SP 800-78-1. To help readers and relying systems discover the key size and algorithm on a particular PIV card, SP 800-73-2, Appendix C, provides a suggested procedure for cryptographic algorithm and key size discovery for each PIV key type.

Part 2: End-Point PIV Card Application Card Command Interface

- The Global PIN access control rules for PIV Data elements in SP 800-73-1 restricted the optional Global PIN to be verified outside the PIV card application, when the PIV card application is de-selected. In addition to the PIV card application PIN, SP 800-73-2 Part 2 now allows Global PIN verification, while the PIV card application is the current selected application, provided, that the Global PIN format is the same as the PIV card application PIN format. SP 800-73-2 further requires the PIV Discovery object to be implemented with the PIN usage

Policy sub-element set to 0x60 for PIV card applications implementing Global PIN verification while the PIV card application is in active state.

- Because the Discovery object uses inter-industry tags from ISO/IEC 7816-6, the GET DATA and PUT DATA Application Protocol Data Units (APDUs) differ from the GET DATA and PUT DATA APDUs of other PIV data objects. As a result, Part 2 of SP 800-73-2 specifies the GET DATA and PUT DATA APDU command specifically for the Discovery Object.

Part 3: End-Point PIV Client Application Programming Interface

- Part 3 adds the pivMiddlewareVersion() function call to the PIV client-application programming interface (API). New SP 800-73-2-based PIV Middleware are required to implement the pivMiddlewareVersion() function call.

- The function declarations of the PIV Client API contain new length arguments for the reference types in the parameter list. These length arguments were previously missing in SP 800-73-1. The new arguments are aligned with the length arguments specified in SP 800-85-A *PIV Card Application & Middleware Interface Test Guidelines.*

Part 4: The PIV Transitional Interfaces and Data Model Specification

- The G.S.C.-I.S.-based transitional card interface specifications and transitional PIV Middleware specifications have been removed. Instead, \references are provided to existing specifications of transitional middleware API and transitional card interfaces.