

This **(First)** DRAFT of Special Publication 800-73-4 (Part 1-3) document has been superceded by the following draft publication:

Publication Number:     **Second Draft Special Publication 800-73-4 (Part 1, Part 2, and Part 3)**

Title:                   **Interfaces for Personal Identity Verification:**  
                              **Part 1- PIV Card Application Namespace, Data Model and Representation**  
                              ⇨ **Part 2- PIV Card Application Card Command Interface**  
                              **Part 3- PIV Client Application Programming Interface**

Publication Date:         **05/19/2014**

- Second Draft Publication:  
<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-73--4>
- Information on other PIV publications and programs can be found at:  
<http://csrc.nist.gov/groups/SNS/piv/>

The following information was posted with the attached DRAFT document:

**SP 800-73-4, DRAFT Interfaces for Personal Identity Verification (3 Parts)**

**Part 1- PIV Card Application Namespace, Data Model and Representation**

**Part 2- PIV Card Application Card Command Interface**

**Part 3- PIV Client Application Programming Interface**

*May 19, 2014*

NIST announces that Revised Draft Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, is now available for public comment. This document has been updated to reflect the disposition of comments that were received on the first draft of SP 800-73-4, which was published on May 13, 2013. The complete set of comments and dispositions is provided below (see last link for this draft below titled "Comments Received & Disposition from May 2013 draft to Revised Draft SP 800-73-4").

High level changes include:

- A new data object has been created from which the value of the pairing code may be read, and additional clarifying information about the use of the pairing code has been provided.
- In collaboration with the FICAM FIPS 201 Test Program (in response to comment # GSA-3), reduced some of the PIV Card options where possible, including deprecating:
  - rarely used data elements Buffer Length, DUNS and Organization Identifier in the CHUID data object
  - legacy data element MSCUID in all X.509 Certificate data objects and
  - legacy data elements Extended Application CardURL and Security Object Buffer in the Card Capability Container
- Removed the two new optional data elements from the Discovery Object and created new data objects to store this new information.
- Modified the key-establishment protocol to add additional details and to address security issues that were raised in the public comments and in "[A Cryptographic Analysis of OPACITY.](#)"

NIST also requests comments on the pairing code, which is part of the new Virtual Contact Interface (VCI) of the PIV Card. Its purpose is to prevent skimming of cardholder data in wireless environment by an unauthorized wireless reader in the vicinity of the cardholder and to ensure that 'cardholder consent' for the release of cardholder data is enabled. The pairing code is part of the Virtual Contact Interface that provides for communication and enables wireless transactions between the PIV Card and NFC-enabled devices for authentication, signing or encryption. . NIST assesses that the pairing code concept is the optimum method available to provide mitigation against a skimming threat.

NIST has received some comments objecting to the use of a pairing code to protect data against skimming in wireless environment and strongly recommending that this be removed. NIST is interested in receiving feedback on whether the new skimming protection measure shall be included on all PIV Cards that implement the VCI, or if it departments and agencies that issue

the cards shall have the ability to disable this security control if there are specific use cases that conflict with pairing code function and alternate mitigating controls are available and identified. (Endnote: Until now, signing and encryption functionalities have been restricted to the PIV Card's contact interface and thus skimming has not been an issue)

NIST requests comments on Revised Draft Special Publications 800-73-4 by 5:00pm EDT on **June 16, 2014**. Please submit comments on Revised Draft SP 800-73-4 using the SP 800-73-4 comments template form (lnk to comment form in Excel spreadsheet is 2nd to last link below for this draft document) to [piv\\_comments@nist.gov](mailto:piv_comments@nist.gov) with "Comments on Revised Draft SP 800-73-4" in the subject line.

Link to Draft on CSRC website:

<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-73--4>