Approved PACS Topology Mapping Form (PACS 13.01 13.02)

PIN Usage Policy Testing Addendum

VERSION 1.3.3 Rev. F

FIPS 201 EVALUATION PROGRAM

August 21, 2018

FINAL

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Final	1.3.3	9/8/2017	Initial release.	Public
Final	1.3.3 Rev A	11/3/2017	Updated Discovery Object tests to reflect that max retries of test cards are set to 10, not 5.	Public
Final	1.3.3 Rev. D	4/24/2018	Synched with Rev. D.	Public
Final	1.3.3 Rev. F	8/21/2018	Deprecated 14.01 and 14.02 categories.	Public

Table of Contents

1 Background

In the PACS FRTC there are two sets of PIN Usage Policy tests (time of registration and time of access) to ensure that E-PACS correctly interpret the Discovery Object and select the correct PIN when they attempt to unlock a PIV card. In SP 800-73-3, the PIN Usage Policy is described as:

"+ Tag 0x4F encodes the PIV Card Application AID as follows:

{'4F 0B A0 00 00 03 08 00 00 10 00 01 00'}

+Tag 0x5F2F encodes the PIN Usage Policy as follows:

First byte (Bits 1-8):

0x40 (Bit 7 only) indicates that the PIV Card Application PIN alone satisfies the PIV Access Control Rules (ACRs) for command execution and object access.

0x60 (Bits 6 and 7) indicate that both the PIV Card Application PIN and Global PIN satisfy the PIV ACRs for command execution and object access.

The second byte of the PIN Usage Policy encodes the cardholder's PIN preference for PIV Cards with both the PIV Card Application and the Global PIN enabled:

Second byte (Bits 1-8):

0x10 (Bit 5) indicates that the PIV Card Application PIN is the primary PIN used to satisfy the PIV Access Control Rules (ACRs) for command execution and object access.

0x20 (Bit 6) indicates that the Global PIN is the primary PIN used to satisfy the PIV Access Control Rules (ACRs) for command execution and object access.

Note: If the first byte is set to 0x40, then the second byte is RFU and shall be set to 0x00.

PIV Card Applications that satisfy the PIV ACRs for PIV data object access and command execution with both the PIV Card Application PIN and Global PIN shall implement the Discovery Object with the PIN Usage Policy set to 0x60 zz where zz is set to either 0x10 or 0x20."

This means:

- If there is no Discovery Object, the *PIV Application PIN* is to be used for command execution and object access. PIN Usage Policy is undefined.
- If the first byte is 0x40, the second byte is always 0x00, meaning the *PIV Application PIN* is to be used for command execution and object access. There is no cardholder

preference. This does not imply that there is no Global PIN. It means that to access the PIV applet, only the PIV PIN shall be used.

- If the first byte is 0x60 and the second byte is 0x10, then the *PIV Application PIN* is to be used for command execution and object access. Note that this is a cardholder preference.
- If the first byte is 0x60 and the second byte is 0x20, then the *Global PIN* is to be used for command execution and object access. Note that this is a cardholder preference.
- *There is no case in which the Global PIN alone is to be used for command execution and object access*.

The procedure that the E-PACS should use is simply this: Unless the first byte is 0x60 and the second byte is 0x20, then the E-PACS should always use the *PIV Application PIN*.

The way that the E-PACS tells the smart card it's using the *PIV Application PIN* is to determine whether it should be using the *Global PIN*. If the *Global PIN* is preferred, then the E-PACS sends the *Verify* APDU with P2 set to 0x00. Otherwise, it should set it to 0x80.

It has been observed that some E-PACS use a strategy for discovering the preferred PIN without reading the Discovery Object. Using this technique, they specify in the APDU that the user-supplied PIN is the *PIV Application PIN* by setting P2 to 0x80, and if the response indicates the PIN is incorrect, it auto-resends the APDU, first setting P2 to 0x00. If the Discovery Object indicates that the Global PIN is the preferred PIN, then the PIV Application PIN retry counter will have been silently decremented each time the card is used with such a system.

Consider this scenario:

The cardholder that knows that the Global PIN is preferred, enters his/her Global PIN and will not realize that the PIV PIN is what the card is matching against on the first attempt. Why? Because they gained access when the Global PIN matched on the second (silent, automatic) attempt. At some point, the number of retries of the PIV PIN will be zeroed, and now the card is unusable for network access and other important things -- all unbeknownst to the cardholder.

2 Objectives

The purpose of this addendum is to provide a method for successfully running the PIN usage policy test cases and determining that the E-PACS complies with the Discovery Object's PIN usage policy on the PIV card.

Vendors have commented that the Discovery Object testing is not practical, given there is no way to determine the number of retries. In fact, it is possible to obtain the number of retries by sending a *Verify APDU* targeting the desired PIN and omitting the PIN. The response to that APDU is the number of retries. After the APDU is sent, the corresponding retry counter is *not* decremented.

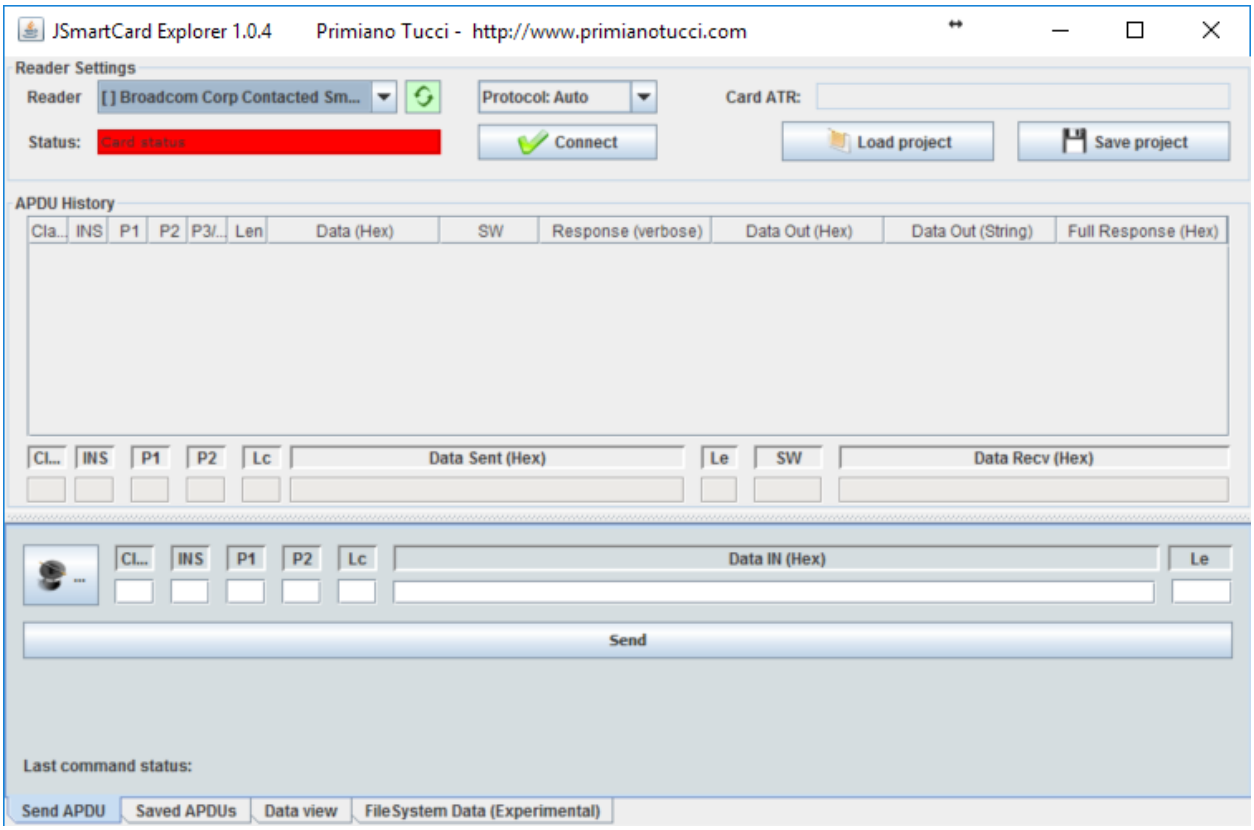
This method allows vendors and the GSA EP PACS lab to test whether a system is properly following the card's PIN usage policy by determining the number of retries remaining on both counters after each test.

In FRTC 1.3.3, those test cases have been re-worded and are in a sequence so that vendors and the lab can use an open source tool, such as the one described in the next section, to send two APDUs and evaluate the responses to determine how many retries are available.

3 Technique for Determining Retries

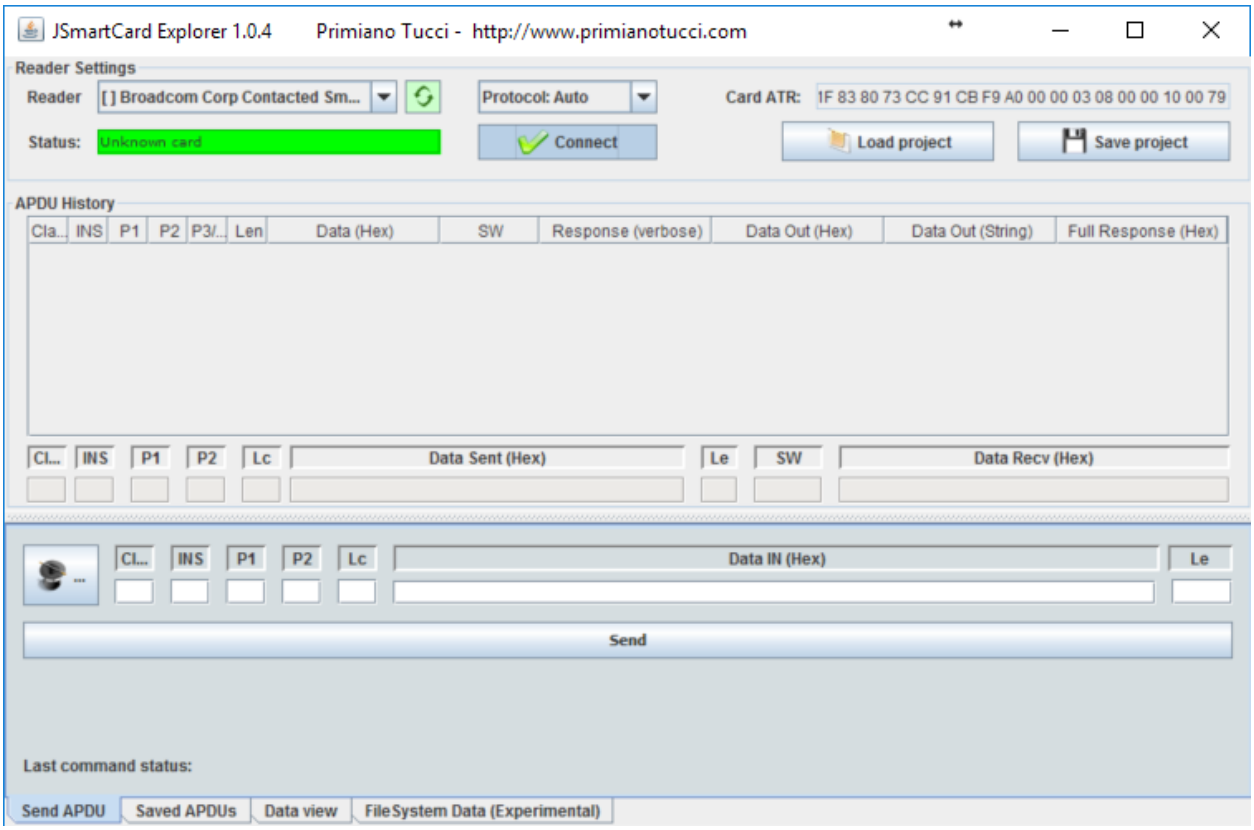
This section describes a technique for determining the number of retries on each PIN after each PIN Usage policy test.

1. Start from a PC with a contact smart card reader connected and operational. Remove any smart cards from your smart card reader and download the *JSmartCardExplorer* application from https://sourceforge.net/projects/jsmartcard/.
2. The application is inside an executable Java jar file. In your download directory, locate the file named `JSmartCardExplorer.jar`. Run it either by clicking on it or executing it from your command line. The window below is displayed. Note that the card ATR is empty.



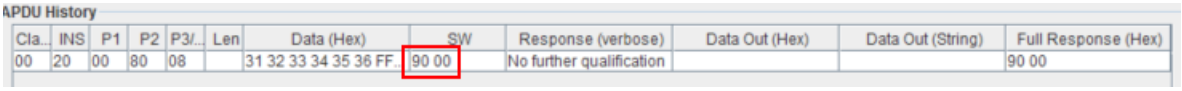
3. Using the reader drop-down, select the contact reader on your PC.

4. Even if a Discovery Object is not present, PIV cards have a Global PIN, 12345678. Therefore, you must reset both PIN retry counters on each ICAM card before running any test cases. Insert each of the Discovery Object ICAM cards (Cards 25-28) into your PC's smart card reader. Click *Connect*. You should see this:



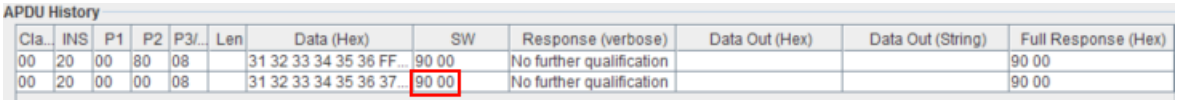
5. Reset the *PIV Application PIN* retry counter by setting CL = 00, INS = 20, P1 = 00, P2 = 80, Lc = 08, and entering "31 32 33 34 35 36 FF FF" (omitting quotes) in the *Data IN* text box and clicking *Send*.

Observe the results in the APDU history box. 90 00 means the command was successful and the card is now unlocked with the *PIV Application PIN*.



6. Reset the *Global PIN* retry counter by setting CL = 00, INS = 20, P1 = 00, P2 = 00, Lc = 08, and entering "31 32 33 34 35 36 37 38" (omitting quotes) in the *Data IN* text box and clicking *Send*.

7. Observe the results in the APDU history box. 90 00 means the command was successful and the card is now unlocked with the *Global PIN*.



APDU History

Cla...	INS	P1	P2	P3/...	Len	Data (Hex)	SW	Response (verbose)	Data Out (Hex)	Data Out (String)	Full Response (Hex)
00	20	00	80	08		31 32 33 34 35 36 FF...	90 00	No further qualification			90 00
00	20	00	00	08		31 32 33 34 35 36 37...	90 00	No further qualification			90 00

8. Now let's run a test case and observe the retry counters for both PINs. For a concrete example, we'll start with *Test Case 2.16.01*.

   > *Discovery object not present. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). (E-PACS is using Application PIN).*

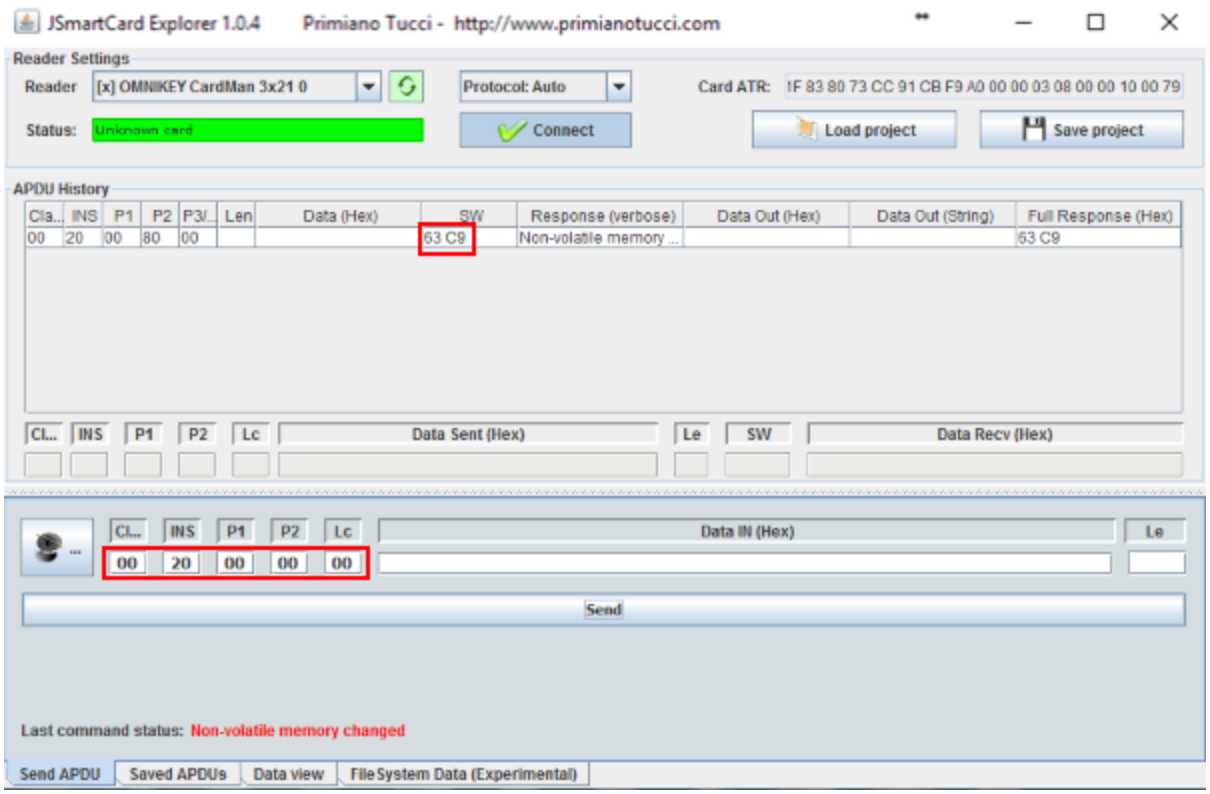
9. Run the test case by inserting ICAM Card 25 into the E-PACS registration reader and entering 999999 when prompted for the PIN. The E-PACS should reject the PIN and the PIV Application PIN should be decremented. We will verify that in the next step.

10. It is possible to check the retry counter by formulating the VERIFY APDU without sending the PIN. The smart card will return the number of retries in the SW2 byte. Immediately after a test case is run, with *JSmartCardExpolorer* running, insert the smart card into your PC.

    Send the APDUs below to check the *PIV Application PIN* and *Global* retry counters.

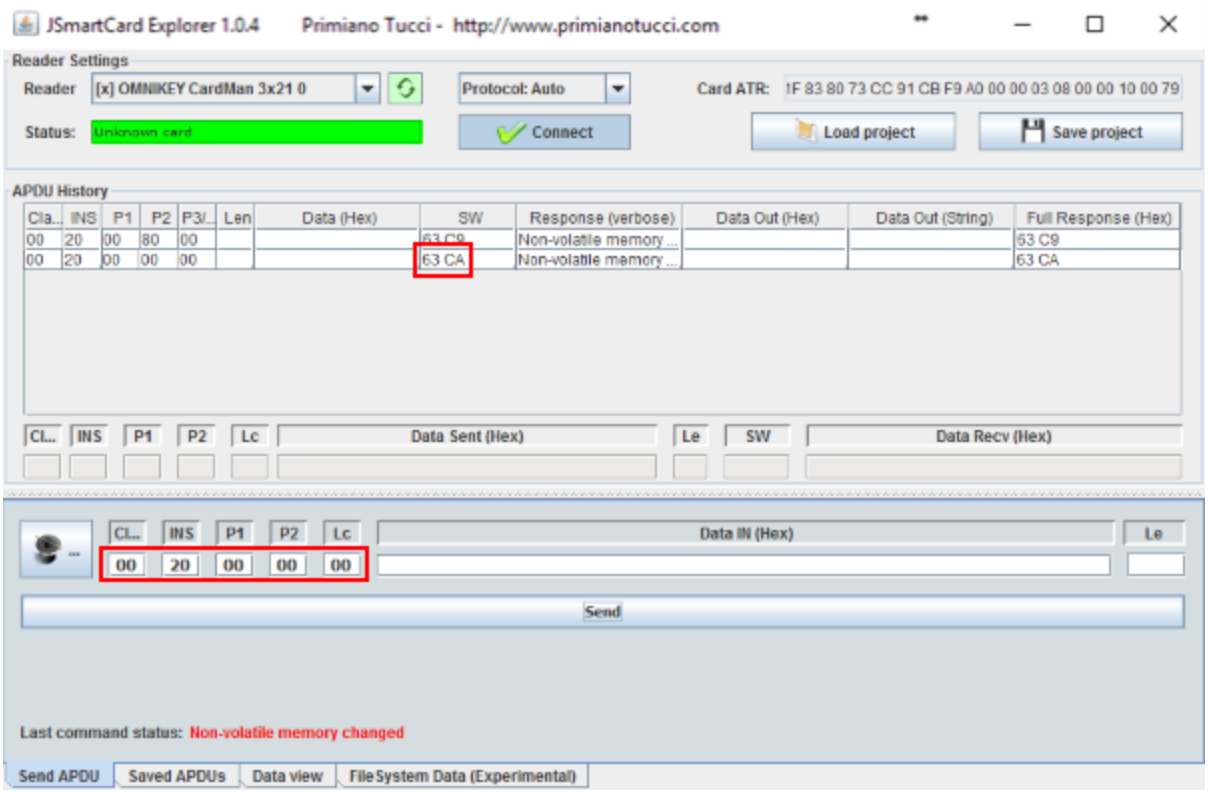
    a. Verify the *PIV Application PIN* retry counter by setting CL = 00, INS = 20, P1 = 00, P2 = 80, Lc = 00 and clicking *Send*.

    b. Observe the SW values returned by the smart card. In this case, it's 0x63 0xC9. The retry counter is the hex value in the lower order 4 bits of SW2 (0xC9), so there are 9 retries remaining in this case. If your results are also "0x63 0xC9" then the E-PACS followed the PIN usage policy for a card with no Discovery Object (as is the case with the first test of the series), and this test case passes.



c. Verify the *Global PIN* retry counter by setting CL = 00, INS = 20, P1 = 00, P2 = 00, Lc = 00 and clicking *Send*.

d. Observe the SW value returned by the smart card. In this case, it's 0x63 0xCA. The retry counter is the hex value in the lower order 4 bits of SW2 (0xCA), or 10 in this case. This second APDU verifies that the *Global PIN* retry counter for the card wasn't changed.



11. Repeat Steps 10 and 11 for each test case, observing the retry counters for both PINs. The results will vary depending on the card being used and the test case being run. Ensure that the test cases are run in strict sequence. Do not perform any deprecated test cases.