



## Transportation Security Administration

*NOTE: This Technical Advisory describes a card platform update that may impact your product.*

# TWIC<sup>®</sup> Technical Advisory

TA-2011-TWIC002-V1.0

## RELEASE OF NEW TWIC CARD AND CARD APPLICATIONS

---

### Introduction

This Technical Advisory details a change in the TWIC smart card platform.

### Background and Definition

This Technical Advisory is precipitated by the fact the electronic chip used on the previous TWIC card has gone end of life and requires replacement.

### Problem Statement

The previous TWIC card electronic chip has reached its end-of-life (EOL) and requires replacement. The new electronic chip incorporates NIST SP 800-73-2 requirements which impact card behavior.

The audience for this Technical Advisory is TWIC reader manufacturers and other entities that communicate with TWIC cards.

### Description of New or Unique Process

This advisory provides notice that the TWIC program shall begin issuing the new TWIC card in July 2011. No

changes to the TWIC data model (other than stated herein) shall be made. The new TWIC card can be identified in one of three ways:

- A) Physically by examining the back of the card for the TWIC Version number ("TWIC vX.Y MM.YY"). For the new TWIC card this version number shall initially be "TWIC v2.0 06.11". The month (06) and Year (11) may be changed as required at a future time.
- B) Electronically by reading the PIV Version number from the PIV card application (after selecting the PIV card application). This value is retrieved using GET DATA (Odd byte INS form) with proprietary Tag '3F F0'. (See technical notes below). For the new TWIC card the Version number shall be "02.32". The previous TWIC card Version number is "01.08".
- C) For contact mode only, examining the Answer To Reset (ATR) value (See technical notes below). The ATR field TA4 shall be '83' for the new TWIC card. The previous TWIC card ATR TA4 value is '03'. (See technical notes below).

The card response status of the new TWIC card has been changed from the previous TWIC card to more closely align with the International Standard ISO/IEC 7816 Part 4 as well as the NIST SP 800-73-2. Specifically the response codes of '6A 81' and '69 82' are used differently in the new TWIC card than used in the previous TWIC card. (See technical notes below).

All APDU command headers require the explicit declaration of the expected response length (Le) if the TWIC reader requests response data. Otherwise a status of '61 xx' shall be returned by the TWIC card indicating response data is available. TWIC readers that follow the SP800-73 APDU command format should see no change in card behavior. (See technical notes below).

For those TWIC readers that perform a query for the number of PIN retries remaining, a change in behavior of the new TWIC card has been made to satisfy the requirements of SP 800-73-2 (see Part 2 page 11, Note 3). Specifically a PIN query shall return either the status of '63 Cx' (where "x" represents the number of retries remaining) or '90 00' indicating the PIN has been previously verified. A response code of '63 C0' shall indicate the PIN is blocked as no retries remain. The status code '69 83' will no longer be returned on the new TWIC card for a PIN Query request. Status code '69 83' may still be returned as a result of a PIN presentation. (See technical notes below).

## **Use of New or Unique Process**

The new TWIC card may impact TWIC reader functionality in the cases where:

- A) The Le byte was not specified in an APDU command yet the TWIC reader expected data. This is especially sensitive for the GET RESPONSE command in the new TWIC card as a lack of an Le field in the command header will result in no data being returned with a status of '61 xx' thereby indicating use of GET RESPONSE; an infinite logic loop.
- B) Exception processing depends upon the exact status code returned (instead of the class of the status being either Error or Warning).

Use of SP 800-73-2 APDU command syntax and generalized error handling will ensure a TWIC reader will function as expected regardless of the vintage of the TWIC card.

## **Design Features of New or Unique Process**

What is unique about this change is the closer alignment of the new TWIC card to ISO/IEC 7816 Part 4 and SP 800-73-2.

## **Comments**

Questions on this Technical Advisory should be addressed to the TSA TWIC PMO TWIC Reader Hardware and Card Application Specification Project Editor, [Gerald.Smith@associates.dhs.gov](mailto:Gerald.Smith@associates.dhs.gov).

## **Subject References**

TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, 30 May 2008.

## **Keywords**

TWIC  
APDU  
ISO/IEC 7816 Part 4  
SP 800-73-2 Part 2  
Le  
PIN Query

## **Standard Details**

Refer to Section 2 *References* in the Subject Reference document.

## **Specifications or Special Provision**

TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, 30 May 2008.

## **Supersedes Dates**

There is no previous Technical Advisory issued that addresses this unique change.

This Technical Advisory shall be active until revised or withdrawn by the TWIC PMO.

## **Obtain more Information**

More technical information on TWIC can be obtained at:

[http://www.tsa.gov/what\\_we\\_do/layers/twic/pilot\\_test.shtm](http://www.tsa.gov/what_we_do/layers/twic/pilot_test.shtm)

**END**

## Technical Notes

### Version Number

The PIV card application version number may be retrieved from a TWIC card by selecting the PIV card application and performing an Odd INS byte form of the GET DATA command for a Data Object with Card Manufacturer specific proprietary Tag '3F F0'.

The format of this APDU command is:

CLA	INS	P1	P2	Lc	<Data>	Le
00	CB	3F	FF	04	5C 02 3F F0	00

The expected card response is

<Response Data>	SW1	SW2
7C 02 XX yy	90	00

Where

XX is the Major version number expressed as a binary number  
yy is the Minor revision number expressed as a binary number

For the previous TWIC card the Version number is '01 08'.

For the new TWIC card the Version number is '02 32'.

NOTE: The new TWIC card supports the version number Data Object in both the TWIC card application and the PIV card application.

NOTE: For the previous TWIC card, there is no version number Data Object instantiated in the TWIC card application. A GET DATA command for the version number while the TWIC card application is selected will return an Error of '67 00' *Wrong Length*.

Answer To Reset (ATR) values (contact communications only)

The ATR of the new TWIC card has been changed to identify a new TWIC card from a previous TWIC card when used in contact communications mode. Specifically the TA4 value field and the corresponding check digit of the new TWIC card have changed from the values of the previous TWIC card.

The ATR values of previous and new TWIC cards are detailed below. The use of **bold and underlined** is to visually illustrate where the differences reside.

The ATR value of the new TWIC card is:

3B DB 96 00 81 B1 FE 45 1F **83** 80 F9 A0 00 00 03 08 00 00 10 00 **98**

The ATR value of the previous TWIC card is:

3B DB 96 00 81 B1 FE 45 1F **03** 80 F9 A0 00 00 03 08 00 00 10 00 **18**

Response status when accessing data or performing operations

The new TWIC card supports card applications that have been changed to more closely align with ISO/IEC 7816 Part 4 and NIST SP 800-73-2 Part 2.

As such, the status codes returned by the new TWIC card, for some operations, differ from the previous TWIC card.

Specifically, the previous TWIC card returns a status code of '69 82' *Security Status Not Satisfied* when attempting to access a Data Object using the contactless interface that is restricted to the contact interface. This same status code is returned when using the GENERAL AUTHENTICATE command over the contactless interface with a key reference that is NOT the Card Authentication key pair. All contact interface commands requiring a security condition to be satisfied returns '69 82' *Function Not Supported* when said condition has yet to be satisfied.

The previous TWIC card returns a '6A 81' *Function Not Supported* when attempting to use the VERIFY command to verify the PIN over the contactless interface as this operation is restricted to the contact interface.

The new TWIC card returns '69 82' *Security Status Not Satisfied* when there exists the possibility of satisfying the security conditions specific for a given Data Object or operation; else the new TWIC card returns '6A 81' *Function Not Supported*.

**CHANGE #1:** The new TWIC card, when using the GENERAL AUTHENTICATE command over the contactless interface with a key reference that is NOT the Card Authentication key pair, will return '6A 81' *Function Not Supported*.

**CHANGE #2:** The new TWIC card will return '6A 81' *Function Not Supported* when attempting to access Data Objects using the contactless interface that are restricted to the contact interface.

Function over Contactless	Previous TWIC	New TWIC
GET DATA	'69 82'	'6A 81'
VERIFY	'6A 81'	'6A 81'
GENERAL AUTHENTICATE	'69 82'	'6A 81'

Status Code returned when access conditions are not met

APDU command header syntax

The new TWIC card supports card applications that have been changed to more closely align with ISO/IEC 7816 Part 4 and NIST SP 800-73-2.

Per ISO/IEC 7816, use of a Case 2 or Case 4 APDU command where response data is expected, the expected response length field (labeled Le) in the APDU command header is required to be present when a smart card reader requests response data to be returned as part of the command. A smart card shall return response data and status (or an error status).

Absence of the Le field indicates to a smart card a smart card reader is not requesting response data. A smart card shall only return status.

The Le field is required to be present in all NIST SP 800-73 version documents for those commands where response data is expected.

The new TWIC card enforces this behavior as per the ISO Standard and NIST SP 800-73-2.

The previous TWIC card supports this behavior per the ISO Standard and NIST SP 800-73-1 when an Le value is present.

However, the absence of an Le value in the previous TWIC card is processed as if the Le field were present with a value 0 (interpreted as 256). With the Le field absent the previous TWIC card returns response data and status (or an error status).

**CHANGE #3:** A missing Le field in the APDU command header will result in the new TWIC card returning only status.

CAUTIONARY NOTE: TWIC Readers that omit the Le field when communicating with a new TWIC card via the GET RESPONSE command will likely experience an infinite logic loop as follows:

```
GET RESPONSE (Le = null)    ->  
                           <- 61 xx  
GET RESPONSE (Le = null)    ->  
                           <- 61 xx  
GET RESPONSE (Le = null)    ->  
                           <- 61 xx
```

...

PIN Query status codes

The new TWIC card supports card applications that have been changed to more closely align with ISO/IEC 7816 Part 4 and NIST SP 800-73-2.

Per SP 800-73-2 Page 11, Note 3 describing the VERIFY command:

“If Lc=0x00 and the command data field is empty, the command can be used to retrieve the number of further retries allowed ('63 Cx') or to check whether verification is not needed ('90 00')”

There was no requirement to support PIN Query in SP 800-73-1 and the VERIFY command was limited to a PIN presentation (i.e. command data of length Lc = 08).

The new TWIC card supports PIN Query (with no command data and Lc = 00) per SP 800-73-2. A status code of '63 C0' shall be interpreted as the PIN is blocked (requiring the issuer to intervene to Reset the PIN). A status code of '90 00' shall be interpreted as the PIN was verified prior to this PIN Query request.

The new TWIC card will return status code '69 83' *Authentication Method Blocked* when a wrong PIN presentation was made and the PIN retry counter has expired.

The previous TWIC card supports PIN query by either returning '63 Cx' where 'x' represents the number of retries remaining or '69 83' *Authentication Method Blocked* if the PIN retry counter has expired.

The previous TWIC card will return status code '69 83' *Authentication Method Blocked* when a wrong PIN presentation was made and the PIN retry counter has expired.

**CHANGE #4:** The PIN Query request (VERIFY with Lc = 00) will no longer return '69 83' *Authentication Method Blocked* if the PIN retry counter has expired; the status '63 C0' shall be returned and should be interpreted as the PIN is blocked.

###