TWIC Reader Hardware
and
Card Application Specification

September 11, 2007

Department of Homeland Security
Transportation Security Administration
Transportation Threat Assessment and Credentialing Office
601 S. 12th Street
Arlington, VA 22202

Table of contents

List of figures

List of tables

1. Overview

1.1 Abstract

This document specifies the behavior at the card interface of the TWIC card application as well as the requirements for TWIC smart card readers, both fixed and portable to be used with the Transportation Worker Identification Credential (TWIC).

1.2 Scope and purpose

The mission of the TWIC program is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation's transportation system and their associated information systems. In its development, the TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document. This specification enables varying levels of control in support of threat level risk mitigation plans.

This specification was initially developed by the National Maritime Security Advisory Committee (NMSAC) in response to a request from the Transportation Security Administration (TSA) and the U.S. Coast Guard. The NMSAC TWIC Working Group included members of the maritime industry with support from representatives from the security technology industry who are affiliated with such organizations as the International Biometric Industry Association (IBIA), the Security Industry Association (SIA) and the Smart Card Alliance. The original specification developed by the NMSAC TWIC Working Group has been modified to accommodate TSA security and privacy requirements.

1.3 Summary of Changes to the NMSAC Specification

This specification is based upon the NMSAC Alternate TWIC Reader Hardware and Card Application Specification, Feb 28, 2007 specifying encryption of biometric templates using a TWIC Privacy Key (TPK). Summary of additional changes is as follows:

1) Section 2.1 Normative References. NIST SP-800-76-1, NIST SP-800-73 Revision 1 and SP 800-78-1 added as normative references.

2) Section 4, TWIC Modes of Operation. Requirement for specific authentication modes to be used at specific MARSEC levels has been removed and available authentication modes have been clarified.

3) Section 4, TWIC Modes of Operation. Ability to configure specific authentication modes to be used at differing MARSEC levels has been added.

4) Section 4, TWIC Modes of Operation. Verification of CHUID signature changed to mandatory. CHUID signature is either verified once, at the time of Physical Access Control System (PACS) enrollment (white list) or by the TWIC reader each time the CHUID is read.

5) Section 5.1.1, Device Dimensions. Note added to stress contactless reader sensitivity to location and electromagnetic conditions of their environment.

6) Section 6, Portable Reader Requirements. Requirements for confidentiality and authentication added for wireless devices used in physical access systems.

7) Section 6, Portable Reader Requirements. Requirement added for handheld devices to have a contactless interface and a mag-stripe reader, or a contact interface for TPK and biometric access or a contact only interface using the PIV card application requiring PIN support to access the biometric template.

8) Section 7, Operational Requirements. Contactless transmission speed requirement changed to support 106kbit/s, 212kbit/s or 424kbit/s, based on the card's capabilities.

9) Section 7, Operational Requirements. Requirement added to reject transaction if multiple cards are simultaneously detected in the reader's contactless field.

10) Section 8, Performance Requirements. Support for biometric liveness detection strengthened from "may" to "should" indicating a strong preference for liveness detection rather than an option.

11) Section 11, TWIC Card Application. As for PIV, the TWIC application does not need to be the default selected application. This requires an explicit Application Select of the application. It has been added to the specification the Select Application Protocol Data Unit APDU command issued by the TWIC terminal should ask only for the 9 first bytes of the TWIC application AID allowing to find out from the card the TWIC version and nature (test or not) of the application in the card.

12) Section 11.2 Key reference. An explicit reference to SP 800-78-1 has been added.

13) Section 11.3 ICC Data Model. Modification of the Transportation Worker Unique Information data object into Unsigned Cardholder Unique Identification data object in order to align TWIC on the SP800-73-2. Structure, Tag reference and Container ID aligned on the next version of SP800-73. Maximum length of buffers has been adjusted to take into account the TWIC requirements.

14) Section 11.3 The Unsigned Cardholder Unique Identifier has been aligned on the next version of SP 800-73.

15) Section 11.4 The Magstripe Model has been completed and detailed.

16) 11.5.1 Select Command. The requirement for terminals to use a partial select (TWIC AID truncated) has been added to the specification. The information returned by the Select command has been corrected to be in line with ISO/IEC 7861-4. Possible Return codes have been added.

17) 11.5.2 Get Data APDU command. Information about the Length of requested data objects as well as return codes have been added.

18) Section 11.6 Sample Card Data removed from the specification.

19) Appendix A.1, CHUID Authentication. CHUID authentication clarified.

20) Appendix A.2, TWIC Biometric Authentication. Biometric authentication clarified.

21) Appendix A.3, Card Authentication Key Authentication. Card Authentication data object reference corrected.

22) Appendix A.3, Card Authentication Key Authentication. Card Authentication Key usage clarified to indicate that it is only available via the PIV application, and is not shared with the TWIC application.

23) Appendix C, MARSEC Level Processing modified to indicate the reader needs to be adaptable to various changes (security threat level and revision of software)

24) Appendix D, TWIC Reader Compatibility With Other Card Types. Reader compatibility and default card support clarified and modified to allow configuration of default AID in the reader selection mechanism.

25) Appendix E, Description of Concept for Contactless Biometric Data Protection for TWIC provided redundant and out of scope information and was deleted.

26) Appendix F (now Appendix E), Proposed TWIC AID Structure. TSA RID added, AID structure clarified.

27) Appendix F added describing the use of the Get Response APDU at the application layer interface.

2. References

2.1 Normative References[1]

[R1] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers

[R2] ANSI/INCITS 378-2004, Information Technology – Finger Minutiae Format for Data Interchange

[R3] ANSI/INCITS 358-2002, Information Technology – BioAPI Specification

[R4] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)

[R5] NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007

[R6] NIST Special Publication 800-73 Revision 1, Interfaces for Personal Identity Verification, March 2006 (updated April 20, 2006)

[R7] NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for PIV, August 2007

[R8] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts

[R9] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[R10] SIA AC-01 (1996.10), Access Control – Wiegand Card Reader Interface Standard

[R11] FIPS 186-2, Digital Signature Standard

[R12] FIPS 197, Advanced Encryption Standard

[R13] FIPS 46-3, Data Encryption Standard

[R14] FIPS 140-2, Security Requirements for Cryptographic Modules

[R15] UL 294, Standard for Safety of Access Control System Units

[R16] EN 50081-1 (1992), European Standard, "Electromagnetic Compatibility – Generic Emission Standard, Part 1: Residential, Commercial and Light Industry"

[R17] IEC 60068-2-64, "Environmental Test – Part 2: Test Methods – Test FH: Vibration Broadband Random (Digital Control) and Guidance

[R18] IEC 61000-6-1 "Electromagnetic Compatibility – Generic Immunity \Standard, Part 1: Residential, Commercial and Light Industry"

[R19] IEC 61000-4-2 (Electrostatic Discharge)

[R20] IEC 61000-4-3 (Radiated RF Immunity)

[1] Normative references apply only to the extent specifically cited in this document.

[R21] IEC 61000-4-4 (Electrical Fast Transient/Burst)

[R22] IEC 61000-4-6 (Radio Frequency Common Mode)

[R23] IEC 61000-4-5 (Surges)

[R24] IEC 61000-4-8 (Power Frequency Common Mode)

[R25] IEC 61000-4-11 (Voltage Dips and Interruptions)

[R26] IEC 68-2-27 (1987), International Electrotechnical Commission, "Basic Environmental Testing Procedures, Part 2: Tests – Test Ea and Guidance: Shock"

[R27] IEC 68-2-29 (1987), International Electrotechnical Commission, "Basic Environmental Testing Procedures, Part 2: Tests- Test Eb and Guidance: Bump"

[R28] OSHA Regulation 1910.147 De-energizing Equipment

[R29] MIL-STD 810F Series of standards are issued by the United States Army's Developmental Test Command, to specify various environmental tests to prove that equipment qualified to the standard will survive in the field

[R30] NEMA 250-1997 standard (http://www.nema.org)

2.2 Informative References

[R31] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)

[R32] FIPS 201 Errata FIPS 201-1 Change Notice (http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf)

[R33] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)

[R34] ICAO 9303 Machine Readable Travel Documents

[R35] Global Platform Messaging Specification, Version 1.0, Nov. 2003 (Provides a definition of all the roles and responsibilities for all the actors (systems) in a multi application smart card infrastructure and defines reference standard on information exchange (message) between actors)

[R36] TSA *Guidance Package – Biometrics for Airport Access Control* (30 September 2005)

[R37] ANSI/SIA OSIPS ACOV-01:200x (Under Development). The OSIPS (Open, Systems Integration and Performance Standards) data models are defining interoperability between components in traditional access control systems.

3. Definitions

3.1 Conformance levels

3.1.1 expected: A key word used to describe the behavior of the hardware or software in the design models *assumed* by this specification. Other hardware and software design models may also be implemented.

3.1.2 may: A key word indicating flexibility of choice with *no implied preference.*

3.1.3 shall: A key word indicating a mandatory requirement. Designers are *required* to implement all such mandatory requirements.

3.1.4 should: A key word indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase *is recommended*.

3.2 Glossary of terms

3.2.1 TWIC card: A smart card that corresponds to the specifications laid out for the Transportation Workers Identity Credential Program.

3.2.2 TWIC Privacy Key: A 128-bit AES key value used to encrypt the biometric templates that are stored on the TWIC card.

3.2.3 Minutiae template: A minutiae template is a mathematical representation of the friction ridge characteristics that are used to individualize a fingerprint image. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes.

3.3 Acronyms and abbreviations

APDU	Application Protocol Data Unit
BAC	Basic Access Control
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Card Holder Unique Identifier
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
IBIA	International Biometric Industry Association
IP	Ingress Protection (rating)
MARSEC	Marine Security Level
NEMA	National Electrical Manufacturers Association
NMSAC	National Maritime Security Advisory Committee
PACS	Physical Access Control System
PIV	Personal Identity Verification
SIA	Security Industry Association
TPK	TWIC Privacy Key
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Credential

4. TWIC Modes of Operation

The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels commensurate with the HSAS.

The TWIC is designed to be used in various systems at different levels of security depending on the requirements of each site and under specific threats levels. This document does not make any recommendation on the specific levels which need to be used by the sites but indicates the different modes of operations available allowing each site to create its own authentication security policy in accordance with the TWIC Rule and Coast Guard requirements. The TWIC physical access readers will allow authentication modes to be configured for each MARSEC level, based upon Coast Guard and site requirements. Specific authentication modes that should be supported by TWIC physical access control readers are identified in Table 4.1, TWIC Identification and Authentication Modes.

Mode	Identification/Authentication	Comments
1	CHUID Verification	Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user's CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from the TWIC card.
2	CHUID Verification + Active Card Authentication	Protects against Card/CHUID cloning. Provides single factor authentication.
3	CHUID Verification + Biometric User Authentication	The cardholder's live biometric sample is compared to a stored biometric reference. The biometric reference template may be read from the TWIC at each use or stored in the PACS system during PACS registration of the user. Provides single factor authentication.
4	CHUID Verification + Active Card Authentication + Biometric User Authentication	Provides dual factor authentication

Table 4.1 TWIC Identification and Authentication Modes

Note: This specification assumes that Personal Identity Numbers (PINs) are not a requirement for authentication at any MARSEC level.

It is important to note that the version 2 TWIC is based upon a PIV compatible smart card and carries both a PIV card application and a TWIC card application that can be independently selected. This allows the TWIC to operate both in PIV mode in PIV compatible readers as well as TWIC mode in TWIC compatible readers. TWIC contactless CHUID verification and TWIC contactless biometric user authentication are supported directly by the TWIC card application. Active card authentication over the contactless interface is supported through selection of the PIV application and is not available directly within the TWIC card application.

4.2 System Perspective

This specification describes two types of devices can be used to verify the user's TWIC card. They are:

- Fixed Physical Access Control Reader – a TWIC reader installed in a wall, turnstile or similar type installation. It communicates with an external access control system to control a door, gate, turnstile, etc. Fixed readers can operate in indoor environments or in outdoor environments exposed to the weather.
- Portable Verification Device – a handheld device that can be used for portable, spot-check identity verification.

A TWIC card can also be verified using reader devices attached to a personal computer in an office environment for such functions as privilege granting, registration into a physical access control system and for logical access control. This specification only describes readers that will be used for physical access into a facility or vessel.

4.2.1 Physical Access Control

4.2.1.1 Biometric Access Control System Overview

Figure 4.1, Generic Biometric-based Access Control System provides a graphical view of the relationship between the physical access control system (as a whole), the biometric sub-system boundary, and the biometric reader device. Note that this is a generic diagram and that specific implementations may vary from this particular depiction. Key elements of Figure 4.1 are described in Table 4.2, below.

Generally a TWIC card will be used at a door or gate that may or may not be manned. The ISO 14443 contactless interface will be used to transfer the unique ID number assigned to the cardholder and the biometric data between the TWIC card and the reader. The cardholder biometric template stored on the card is encrypted with a key unique to the card and remains encrypted during transmission to the reader over the contactless interface. The key required to decrypt the reference biometric template of the user, called the TWIC Privacy Key (TPK), shall be derived from one of several sources. These include the magnetic stripe encoded on the TWIC card, the TWIC card memory (but only accessible through the contact interface) or from the physical access control system where the card key has been registered.

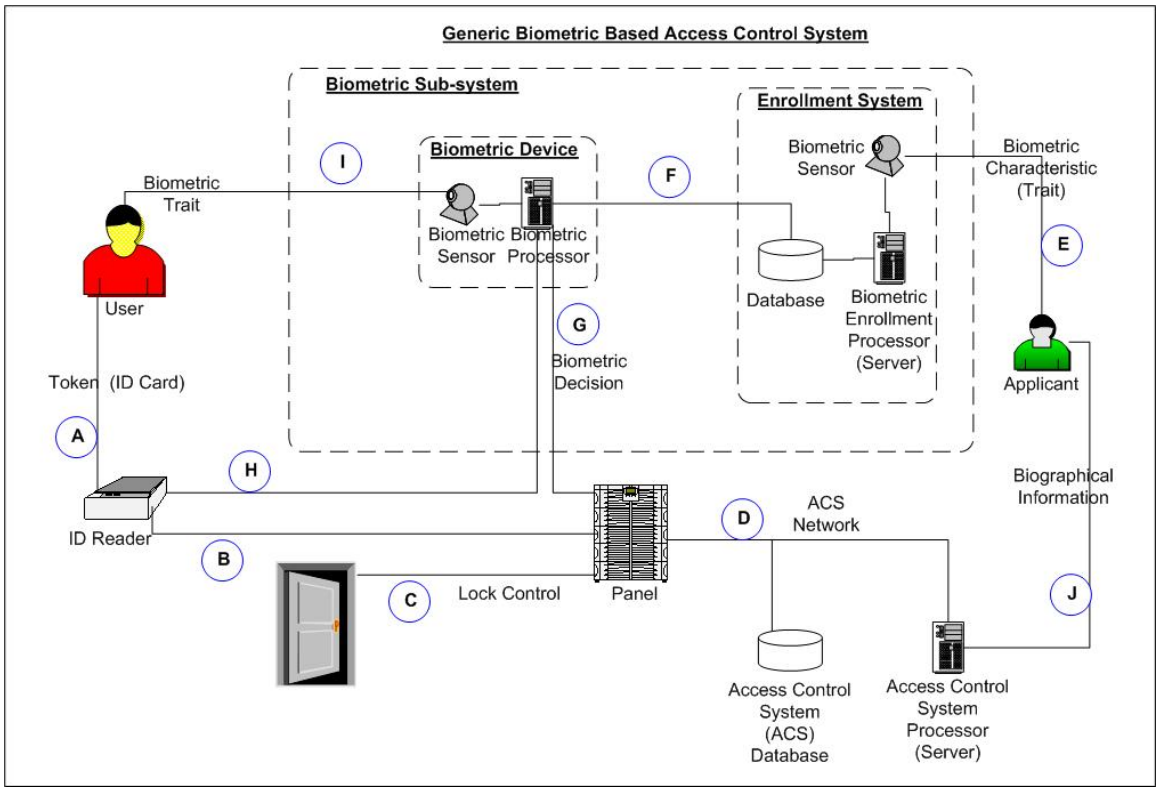

Figure 4.1 Generic Biometric-based Access Control System

Key	Description
A	Any form of machine-readable credential (TWIC card) presented by the user to the ID reader to claim an identity.
B	User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the panel for the ACS to determine access privilege (part of typical legacy ACS).
C	Electrical signal from the panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy ACS).
D	(Physically) communication channel (Ethernet, RS485, etc.) enabling data interchange between the panel and ACS processor and database. (Logically) depends on site-specific implementation and includes user identity code from panel and user access authorization from ACS processor.
E	Body part or human behavior presented by the applicant to the biometric sensor during enrollment (e.g., fingerprint, iris, voice, signature). This function may also include interactions between applicant and sensor, i.e., indicator lights, audio cues.

Key	Description
F	Biometric template data from enrollment database to biometric processor for implementations using server- stored templates. (This flow is architecture-specific, may be per user transaction or periodic pre-loads.)
G	Y/N indication (electrical signal or message) from biometric processor to panel conveying the result of the user verification transaction.
H	User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the biometric processor as claim of identity (also includes user template data for template on card architectures).
I	Body part or human behavior presented to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, signature, etc.). This may also include interactions between applicant and sensor such as indicator lights or audio cues.
J	Applicant-supplied information (name, address, etc.) obtained during ACS enrollment via the ACS processor (part of typical legacy ACS).

Table 4.2 Biometric Access System Key Descriptions

4.2.1.2 Biometric Verification - Network Attached Reader

A network attached reader[2] supports two-way communication between the reader and the physical access control system (PACS). The reader can use this communication channel to access the user's TWIC Privacy Key information that was stored during the process of registering the user for routine access. TWIC verification consists of the following steps (assuming a user has previously enrolled in the local physical access control system). When a TWIC card must be verified, the following steps shall be followed:

- Present card to contactless reader
- Reader reads unique ID number from the card and either sends this directly to the PACS when in "CHUID only" mode, or temporarily stores this information for transmission after a successful biometric match when in "CHUID + biometric" mode. If the reader is in "CHUID + biometric" mode, the reader uses the unique ID number from the card to retrieve the user's TWIC Privacy Key previously stored in the PACS when the user enrolled/registered at the facility.
- The reader may execute an active card authentication (using the PIV Card Authentication Key) at this point of the procedure depending on the level of security required
- Reader gets the user's biometric template from the contactless interface on the card and decrypts the biometric using the TWIC Privacy Key.
- User presents their biometric.

[2] Note that the term, "Network Attached" here indicates a bi-directional communication path between the reader and the PACS, it is not intended to specify any particular network fabric or protocol.

- Reader compares the biometric against the template read from the card and signals the physical access control system to grant or deny entry.

4.2.1.3 Biometric Verification - Standalone Reader

A standalone reader is one that has no two-way communications channel available or is connected to a PACS through a one-way communications connection. In this case, when a TWIC card is presented to the reader, the TWIC Privacy Key must first be read from the magnetic stripe on the card. The following steps shall be followed:

- Swipe TWIC card through magnetic stripe reader to read TWIC Privacy Key from TWIC card.
- Present card to contactless reader
- Reader reads unique ID number from the card and temporarily stores this information for transmission after a successful biometric match when in "CHUID + biometric" mode. If the reader is in "CHUID only" mode no further information is required from the card.
- The reader may execute an active card authentication (using the PIV Card Authentication Key) at this point of the procedure depending on the level of security required.
- Reader reads the user's biometric template from the contactless interface on the card and decrypts the biometric using the TWIC Privacy Key obtained from the magnetic stripe.
- User presents their biometric.
- Reader matches the presented biometric against the template obtained from the card.
- Reader displays that the verification was confirmed or denied and signals the physical access control system.

Note: Since the TWIC Privacy Key is also stored in the ICC memory of the TWIC card, it can alternatively be accessed through the contact interface by inserting the TWIC card into a contact read slot.

4.2.2 Portable Identity Verification

A handheld reader can also be used to verify worker credentials in a portable environment. This can be in conjunction with or as a substitute for the fixed access control readers described above. Smaller installations might not have, nor need, a complete physical access control system. In this case, a portable reader would provide an alternate means of identity verification. By nature the handheld reader is attended and operated by a qualified verification agent.

A TWIC card can be interrogated and verified using a portable handheld unit. The interface between the TWIC card and the reader may be via the contact and/or the contactless interface. The mobile device is envisioned to be used in a minimum of two operational modes:

- At a gate control location to interrogate credentials within a vehicle with multiple occupants
- Authorized security personnel performing a random challenge throughout the facility

Access to the biometrics on the card depends on the card reader interface used by the portable device to access the encrypted biometric template as described in Table 4.3 below.

Interface used to access the Biometric Template	Requirements to access the card biometric template
Contact Interface	Using the PIV Card application: Presentation of a PIN is required to access the user biometric reference template stored in clear text in the PIV card application. Using the TWIC card application: Obtain through the contact interface the encrypted biometric template as well as the key (TPK) used to cipher it. No PIN or other key material is required from the reader.
Contactless Interface	The encrypted biometric reference template being free readable over the TWIC contactless interface, the key required to decipher it (TPK) can be obtained from three possible sources: the magstripe of the card, the contact interface of the TWIC card application, or from the PACS system if the key was stored at enrollment.

Table 4.3 Portable Card Reader Hardware Requirements

5. Fixed Reader Requirements

Beyond these control objectives are electrical and physical interoperability requirements. These are objectives that state the nature of the environment and technologies in place that the fixed reader must interoperate with to be compliant and successful.

The purpose of the fixed reader unit is to provide the physical interface between the TWIC card and the physical access control system controlling access to that portal (turnstile, door, gate, ramp, etc.).

5.1 Physical Requirements

5.1.1 Device Dimensions

There are no specific recommendations regarding device dimensions. For practicality, the biometric device should be reasonably compact and versatile as to mounting in relation to the access point being controlled.

5.1.2 Device Mounting

Mountings provided shall be tamper-proof. This means that the reader will have the ability to send an external signal in the event that there is an attempt at unauthorized entry into or removal of the device.

> Note: TWIC readers using a contactless RF technology (13.5MHz) are sensitive to location and electromagnetic conditions of their environment. Installers should work in coordination with reader manufacturers to make sure no electrical field or metallic element will interfere with the reader RF communication field.

5.1.3 Environmental

5.1.3.1 Outdoor:

The reader shall conform to a NEMA 4 rating.

The reader shall operate within a temperature range of -20°C to +70°C (-4°F to +158°F).

The reader shall operate in a humidity range of 5-100%, condensing.

The reader shall be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources.

The reader components may be offered in an enclosing cabinet that achieves the rating required.

The reader may be required to function in a hazardous materials environment. Intrinsically safe readers may be offered to meet this requirement.

5.1.3.2 Indoor

The reader shall operate in a humidity range of 5-90%, non-condensing.

5.1.4 Impact Resistance

Reader device verification function shall not be degraded by low frequency vibration typical at terminals stemming from sources such as vessel departure/landings, heavy foot traffic, electric carts, large HVAC systems, sub-floor bag conveyors, and outdoor truck traffic. Alternatively, reader manufacturer may base compliance on IEC 60068-2-64 or equivalent commercial practice or analysis.

5.1.4.1 Shock

Reader shall survive a shock event defined by IEC 68-2-27 (1987) using one half-sine pulse with a nominal peak acceleration of 5 g (50m/s^2) and nominal pulse duration of 30 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

5.1.4.2 Bump

Reader shall survive 100 bumps defined by IEC 68-2-29 (1987) each with a nominal peak accelerating of 10 g (100 m/s^2) and nominal pulse duration of 16 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

5.2 Electrical Requirements

The reader shall operate within a range of 8-48 VDC. Where necessary to operate from line voltage, a power supply approved for use with the reader shall be provided. The reader shall optionally support PoE or PoE+ (Power over Ethernet or Power over Ethernet Plus) in accordance with IEEE 802.3af (48VDC/15.4W max) or 802.3at (48 VDC/56W max).

Current requirements shall not exceed 2.0 Amps.

The reader shall provide reverse voltage protection.

The reader shall be FCC certified.

The reader shall return automatically to normal operation after loss of power.

5.3 Safety

The reader shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.

The reader shall not possess:

- Sharp corners or edges that can puncture, cut, or tear the skin or clothing or otherwise cause bodily injury. All device corners and edges should have at least a 1mm exposed radius of curvature.
- External wires, connectors, or cables other than the power and data cable and the optional TWIC Privacy Key reading device (magnetic stripe)
- Loose coverings and cowlings

5.4 Electromagnetic/Vibration Compatibility

Readers shall comply with the following requirements. For immunity tests the equipments shall operate normally or if operation is interrupted it shall not grant access.

5.4.1 47CFR18 and/or CISPR 11 (Emissions)

5.4.2 IEC 61000-4-2 (Electrostatic Discharge)

- Contact Discharge Mode at 2 kV and 4 kV Air Discharge Mode at 2 kV, 4 kV and 8 kV

- Assumes 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.
- Performance Criteria B

5.4.3 IEC 61000-4-3 (Radiated RF Immunity)

- 10 V/meter, 80 MHz to 1 GHz,
- Four sides of EUT, 1% steps, 2.8 sec. dwell. AM Mod., 80%,1 kHz.
- Performance Criteria A

5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst)

- AC and DC Power Ports at 0.5kV, 1kV and 2kV
- Signal Lines over 3 meters at 0.25 kV, 0.5kV and 1kV
- Performance Criteria B

5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode)

- 10 Vrms, 150 kHz to 80 MHz,
- Power ports and signal lines over 3 meters, 1% steps, 2.8 sec. dwell.
- Performance Criteria A

5.4.6 IEC 61000-4-5 (Surges)

- AC power port at 2kV line to earth, 1kV line to line at 0, 90 and
- 270 deg.
- DC Power Ports at 0.5 kV line to earth, 0.5 kV line to line
- Signal Lines over 30 meters at 1 kV line to earth
- Positive and negative polarity, 5 surges per mode of appearance.
- Performance Criteria A

5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)

- 30 A/m, 50 or 60Hz
- Performance Criteria A

5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions)

- 30% reduction for 0.5 periods (10 ms), Performance Criteria B
- 60% for 5 periods (100 ms), Performance Criteria C
- 60% for 50 periods (1 sec), Performance Criteria C

- 95% for 250 periods (5 sec), Performance Criteria C

6. Portable Reader Requirements

The reader may support a wireless interface to provide direct access to the Physical Access Control System. In such a case the wireless connection shall have the following security attributes: confidentiality (session key) and active authentication of the reader or the operator using the reader,

If the reader has only a contact interface, the PIV card application may be used to verify the biometric information of the user. This application requires the user PIN to be presented in order to release the reference biometric information to the reader. Using the TWIC card application over the contact interface allows the reader to access the encrypted biometric reference template along with the key (TPK) used to cipher it.

If the portable reader does not have a contact interface but only a contactless card read capability it shall also have a magnetic stripe reader in order to access the TWIC Privacy Key from the TWIC card needed to decrypt the biometric on the TWIC card. The reader shall be capable of confirming whether a TWIC card has been revoked.

6.1 Portable Reader Specific Requirements:

The portable reader shall meet the same specifications as the fixed reader where appropriate with the exception of the following differences:

6.1.1 Operational Features

The portable reader shall have a display suitable for user interaction

The portable reader shall be able to display the current battery level.

The portable reader may use a touch screen or other suitable means for user input/control.

The portable reader should have a hibernation mode for protection against data loss.

6.1.2 Environmental Requirements

A portable reader certified for harsh conditions must meet the following specifications:

- MIL-STD 810F, Method 514.5 – Vibration
- MIL-STD 810F, Method 501.4 – High temperature (to +70°C/+158°F)
- MIL-STD 810F, Method 502.4 – Low temperature (to -10°C/-14°F)
- MIL-STD 810F, Method 507.4 – Humidity
- MIL-STD 810F, Method 503.4 – Temperature shock
- MIL-STD 810F, Method 516.5, Procedure IV (Transit Drop Test) – 26 drops at 4 feet

6.1.3 Electrical Requirements

The portable reader should be supplied with a rechargeable battery with 12 hours minimum operational time.

The portable device shall be operable while charging.

The portable device should have a maximum battery recharge time of 2 hours.

7. Reader Operational Requirements

Reader operational requirements apply to all reader types except as noted.

The contactless reader component shall conform to the ISO14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1.

The reader shall have a maximum read range of 10cm when used with the contactless card media.

The contactless reader shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s, based on the card's capabilities.

If two or more cards are presented at the same time in the reader's contactless field, the reader shall reject all of the cards.

The reader shall require that a card, once read, must be removed from the RF field for one second before it will be read again to prevent multiple reads from a single card presentation.

Fixed readers shall be capable of reading the access control data from the card, performing the necessary authentication steps, and transmitting the credential data as required by the PACS.

Fixed readers shall have communications ports as required by the PACS cable plant and control panels. Minimum options required are:

- Wiegand port for connection to standard access control panels.
- RS-485 or 10/100baseT (Ethernet) for connection to computer systems or access control systems.

For fixed readers, the Wiegand output format shall follow that specified for FIPS 201-based systems. The GSA Approved Products Listing test for Federal Employee Personal Identity Verification defines a 75-bit “transparent mode” which includes 2 parity bits and 25 bits for the date. The reader shall output the following 75-bits:

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Expiration Date	50-74	25
Parity Bit P2	75	1

Table 7.1 75-bit Wiegand Output Format

Fixed readers may also support a 48-bit Wiegand output format when the reader includes a real time clock that can be used to verify the expiration date. In this case, it is assumed that the reader has the ability to process the expiration date. Some PACS control panels may not be able to support both 48-bit and 75- bit Wiegand input at the same time, so the reader must provide a method of setting this as appropriate. The 48-bit Wiegand format is the same as the 75-bit transparent mode but drops the expiration date and the two parity bits as shown below:

Description	Position	Length
Agency Code	1-14	14
System Code	15-28	14
Credential Code	29-48	20

Table 7.2 48-bit Wiegand Output Format

Fixed readers may support other alternate Wiegand formats for legacy systems at a particular location as required.

The reader should clearly and continuously display power status (on, ready or out of service).

The reader may contain additional user indications including lights, text messages, audible indicators, etc.

Reader visual indicators shall be visible in daylight.

The reader should have a finger guide to aid in proper finger placement on the sensor.

For biometrically enabled readers, the fingerprint sensor should be embedded in the same chassis as the reader. If a separate fingerprint sensor module is used, the wiring between the reader and biometric unit must not be exposed.

The reader shall allow for future enhancements to be added in the field. A mechanism should be provided that assures that only authorized/authenticated firmware/software updates are permitted.

The reader shall provide a means to create a log of operations for use in assessing exception conditions such as fingerprint rejections.

The reader shall provide an automated alert or lockout after a configurable number of biometric matching attempts (facility chooses).

The reader may support a means of alerting the PACS/operator if the reader has been tampered with.

The reader shall support a method of changing its mode of authentication according to the current security threat level of the protected site.

8. Performance Requirements

The reader should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to reader and completion of the biometric match) of three seconds. This does not include the time required to acquire the TPK through swipe of a magnetic stripe or through download from a PACS that may be required depending on the implementation configuration.

The biometric sub-system should provide an equal error rate (EER) of 1% (1% false rejections at a setting of 1% false acceptance) on a per transaction basis. This assumes up to three attempts as a minimum standard error rate. The reader should provide a mechanism to adjust the security level sensitivity as required.

Any alternatives to use of fingerprint biometrics will be addressed in the local operator's security plans.

Biometric devices should provide liveness detection. This is particularly important when readers are used in unattended operations.

Biometric processes and performance is further described in ANSI/INCITS 383.

It should be noted that biometric interoperability is defined as the ability of a biometric reader to perform a match from a presented biometric with the ANSI/INCITS 378 formatted enrolled templates provided on the TWIC card by the TSA. Such templates shall be in compliance with NIST Special Publication 800-76-1 INCITS 378 profile for PIV Card templates.

9. Operational Availability

The biometric reader shall be able to handle 1 million touches without degradation.

The reader shall be designed to yield a Mean Time Between Failure (MTBF) of 25,000 hours or greater.

10. Delivery

The reader shall include technical manuals covering installation, operation and maintenance of the units. Units will be packaged suitable for shipment to installation point.

11. TWIC Card Application

11.1 Card-application Identifier

TWIC card-application AID		
RID	**PIX**	**State**
A0 00 00 03 67	20 00 00 01 xx xx (See Appendix E : xx xx = 81 01 = TWIC test xx xx = 01 01 = TWIC live)	Needs to be selected explicitly with a PIX length of 4 bytes

Note: Both PIV and TWIC specifications allow another application to be the default selected application in a card. As not all TWIC cards may be issued with the TWIC application as the default selected card-application, the reader shall explicitly select the TWIC card-application.

11.2 Key Reference(s)

Algorithm Identifier*	Key Reference	Key Name	Authenticatable Entity	Security Status	Retry Reset Value	Number of Unblocks
08	'Kp'	TWIC card-application Privacy Key	TWIC Card-application Biometric data and Cardholder	Application	N/A	N/A

*Reference FIPS 201-1 document SP 800-78-1: algorithm identifier 08 indicates this key is to be used with an AES algorithm in ECB mode.

Notes:

1. This key is not used by the card for any cryptographic function but is used by the client application to cipher (for storage in the card) or decipher (for use in the terminal) the user's reference biometric template.
2. The Key reference is a field (tag 0xC1) found in the TWIC Privacy Key Buffer.

11.3 ICC Data Model

Buffer Description	Data Object (BER-TLV tag)	Maximum Length	Access Rule	Contact/ Contactless	M/O
Unsigned Cardholder Unique Identifier	0x5FC104 (0x3002)**	64	Always Read	Contact and Contactless	M
TWIC Privacy Key Buffer	0xDFC101 (0x2001)**	40	Always Read	Contact (and Magstripe also)	M
Card Holder Unique Identifier	0x5FC102 (0x3000)**	3000	Always Read	Contact and Contactless	M
Card Holder Fingerprints	0xDFC103 (0x2003)**	2500	Always Read	Contact and Contactless	M
Security Object	0xDFC10F (0x9000)**	920	Always Read	Contact and Contactless	M

** The containerIDs are provided in this data model as they are required for the Security Object Data Group (DG) mapping.

Notes:

1. The maximum length of data objects in the above table does not include the BER-TLV structural information attached to each data object. This structural information consists at a minimum of the tag itself (three bytes) , the length of the data object value which may be one or three bytes, and applet internal data information which may vary from one applet to the other (specific to applet implementation).
2. All the Data Objects in the TWIC card-application data model are elementary data objects with 3-byte ASN.1 BER-TLV encoded tags. The individual tags inside these data objects are not intended to follow ASN.1 coding rules in the interest of keeping backward compatibility with PIV data model. As a consequence, no ASN.1 constructed data object is used in this application.
3. The signatures used in the Signed Cardholder Unique Identifier and the Card Holder Fingerprint Templates are of type RSA 2048, SHA1. The signature belongs to the Card Management System which is responsible for preparing the personalization data.
4. The calculation of hashes of the individual data objects (except for TWIC Privacy Key Buffer), which are then to be used for creation of Security Object shall be based on the contents of Data Objects as stored in the TWIC card-application

Table 11.1 Unsigned CardHolder Unique Identifier

Unsigned CardHolder Unique Identifier		**0x5FC104**		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
FASC-N	0x30	M	Fixed Text	25
GUID	0x34	M	Fixed Numeric	16
Expiration Date	0x35	M	Date (YYYYMMDD)	8
Error Detection Code	0xFE	M	LRC	0

Note: The structural information required by this structure consist of two additional bytes per element (simple TLV tag byte plus one byte for length). This requires a minimum total of 57 bytes for this data object value.

Table 11.2 TWIC Key Privacy Buffer

TWIC Privacy Key Buffer		**0xDFC101**		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
TWIC Privacy Key (Kp)	0xC0	M	Variable	32
Algorithm Identifier	0xC1	M	Fixed Text	01
Key Index	0xC2	M	Fixed Text (00 = RFU)	01

Notes:

1. The current TWIC Privacy Key requires only 16 bytes of data storage. An additional 16 bytes have been added to the max size of the TWIC Privacy Key element (Tag 0xC0) to support future algorithms.
2. The structural information required by this structure consist of two additional bytes per element (simple TLV tag byte plus one byte for length). This requires a minimum total of 40 bytes for this data object value.

Table 11.3 Signed CardHolder Unique Identifier

Card Holder Unique Identifier		**0x5FC102**		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
FASC-N	0x30	M	Fixed Text	25
GUID	0x34	M	Fixed Numeric	16
Expiration Date	0x35	M	Date (YYYYMMDD)	8
Issuer Asymmetric Signature	0x3E	M	Variable	2400
Error Detection Code	0xFE	M	LRC	0

Note: The structural information required by this structure consist of some additional bytes per element (simple TLV tag byte plus one, two or three bytes for length). This requires a minimum total of 12 bytes for this data object value.

Table 11.4 CardHolder Encrypted Fingerprint Templates

Card Holder Fingerprints		**0xDFC103**		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
Encrypted Fingerprint template (2 fingers)	0xBC	M	Fixed	2500

Notes:

1. The fingerprint templates are encoded in accordance with the INCITS 378 standard.
2. Tag 0xBC shall contain the encrypted data and biometric templates. The CBEFF integrity option is required per 800-76, section 6, therefore the data includes the digital signature of the Card Management System. The data is padded per PKCS#7 section 10.3, note 2, and encrypted using the TWIC card-application Privacy Key (Kp).
3. Four additional bytes of structural information are to be added to the data object size for its value.

Table 11.5 Security Object

Security Object		**0xDFC10F**		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
Mapping of DG to Data Objects	0xBA	M	Variable	12
Security Object	0xBB	M	Variable	900
Error Detection Code	0xFE	M	LRC	0

Notes:

1. The security object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1. [8] .Tag “0xBA” is used to map the Data Objects in the TWIC data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD). The objects hashed are: the Unsigned CHUID (0x3002), The TWIC Privacy Key (0x2001), the Signed CHUID (0x3000), and the signed fingerprint templates (0x2003). This enables the TWIC security object to be fully compliant for future activities with identity documents.
2. The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object. The signature field of the security object shall omit the issuer’s certificate, since it is included in the CHUID. Card Issuer’s Digital Signature is in accordance with FIPS 201-1 using the SP-800-78-1 document as reference with the key sizes in accordance to the TWIC card life.
3. Eight additional bytes of structural information are required for this data object.

11.4 Magstripe Data Model

The TWIC Privacy Key (TPK) used to cipher/decipher the reference biometric template stored in the TWIC card application is stored on the magstripe of each TWIC card and shall be encoded as follows:

- The TPK is a 16 byte string used by an AES encryption/decryption algorithm.
- Track 1 of the TWIC magstripe is reserved exclusively for the TPK character string. The TPK character string is to be encoded on the high-coercivity magstripe track 1 of the card as defined in ISO/IEC 7811-6.

- Each nibble of the 16 bytes of the TPK are to be encoded as ASCII alphanumeric characters (0 to 9 and A to F) giving a total of 32 characters representing the 32 hexadecimal digits of the TPK .
- The TPK is to be encoded as one data field starting with a start sentinel (';') followed by 32 data characters and ending with one end sentinel ('?').
- An LRC field calculated according to ISO/IEC 7811-2 is to be coded after the end sentinel.

11.5 TWIC Card Application Command Set

The TWIC card application shall support the following APDU commands:

- SELECT
- GET DATA

Notes:

1. As for PIV, the Get Response APDU command does not appear at the application command layer but may be required if the application layer does not use an extended length in the APDUs. The use of the Get Response by the application layer is described in Appendix F.
2. Other APDU commands may be required to handle application management features but as they are not required for interoperability in TWIC terminals, they do not appear in this specification.
3. Beyond the tag described in this document, some ISO/IEC 7816-6 tags may be available at the card interface in response to a Get Data command (e.g. Card Related Information). As these tags are not required for interoperability in TWIC terminals, they are not described in this document and are specific to the applet implementation or the management features of such applet.

11.5.1 SELECT

Command Syntax

CLA	'00'
INS	'A4'
P1	'04'
P2	'00'
Lc	'09' (Select on a partial TWIC AID length)
Data Field	TWIC AID (= TSA RID || TWIC first four bytes of the PIX)
Le	Length of TWIC card-application property template

Note: In terminals using the TWIC card, the Select AID APDU command shall always ask for a partial TWIC AID and analyze the information returned from the card when the select is successful. The information returned provides the version of the TWIC card application as well as if the card is a test card or a live TWIC card. A full select with a length of 11 bytes (c = 0x0B) shall, nevertheless, be supported by the card in order to be ISO/IEC 7816-4 compliant.

Card-application Property Template

Upon selection, the TWIC card-application shall return the application property template described below.

Tag Name	Tag	Length	M/O	Value field of the tag
Application Template	'61	'Var	M	See ISO/IEC 7816-6
Application identifier of application	‘4F’	'0B'	M	The PIX of the AID includes the encoding of the version of the TWIC card-application.
Coexistent tag allocation authority	‘79’	'0B'	M	Coexistent tag allocation authority template.
Application AID coexistent with ISO/IEC 7816 name space for tags	'4F'	'09'	M	PIV AID root (without the version information) A0 00 00 03 08 00 00 10 00

Table 11.6 Data Objects in the TWIC Card-application Property Template (Tag '61')

Response Syntax

Data Field	Card-application property template (see above)
SW1-SW2	Status Word

SW1	SW2	Description
‘6A’	**‘82’**	Card-Application not found
'6A'	**'86'**	P1.P2 combination not supported
'6A'	**'87'**	Incorrect Data Field length (Lc =0 or Lc > 16)
‘90’	**‘00’**	Successful execution

11.5.2 GET DATA

Command Syntax

CLA	‘00’
INS	‘CB’
P1	‘3F’
P2	‘FF’
Lc	‘05’ for TWIC related data objects
Data Field	‘See table A
Le	Number of data content bytes to be retrieved

Command Data Field

Name	Tag	M/O	Comment
Tag List	5C	M	BER-TLV tag of the data object to be retrieved

Response Syntax

Data Field	BER-TLV with the tag ‘53’ containing in the value field the requested data object
SW1-SW2	Status Word

SW1	SW2	**Description**

'61'	**'XX'**	Successful execution where SW2 encodes the number of response data bytes not returned in the response
'62'	**'82'**	Warning, End of File Reached before reading the requested Le bytes. Returned data block may contain padding bytes for some types of transmission protocol
'69'	**'82'**	Security status not satisfied
'6A'	**'88'**	Data Object not found
'6C'	**'XX'**	Execution aborted (no data returned) SW2 encodes the number of response data bytes available not returned in the response
'90'	**'00'**	Successful execution

Notes:

1. The use of return codes SW1-SW2 = 61 xx and SW1-SW2 = 6C xx are explained in Appendix F of this document.
2. TWIC terminal manufacturers should note that it is not reliable to use the Le field (expected information length) to limit the amount of time it takes to transmit information from the card. Some cards, depending on the transport protocol used may not accept truncation in the response of the amount of data constituting a data object. In such a case the complete data object would be transmitted anyway and truncated only at the application layer presentation with no benefit in transmission time. For this reason the unsigned CHUID is part of this specification, allowing read of such information quickly. ISO/IEC 7816-4 allows the application layer to ask for a truncated value field of data objects but requires use of another format of the Get Data command (Tag list 5D instead of 5C) in order to do so and PIV does not support this parameter in the Get Data command.

Appendix A Authentication Processing

In order to determine the identity of a cardholder, an access control system must check one or more authentication factors. The overall assurance of the authentication process is determined by the number and quality of each authentication factor used. These factors are typically divided into three categories:

- Something you have - An object hard to copy (e.g. a badge, a metal key or a smart card)
- Something you know - An element hard to guess (e.g. a PIN or a password)
- Something you are - An element hard to share (e.g. your fingerprint, your iris or your voice)

A check against an authentication factor is considered "strong" if it would be hard for an attacker to gain control, clone or compromise that factor. An access control system may achieve the required level of authentication security by checking factors against the card presented, the user presenting it, and information stored in its own database.

An authentication factor is bound to an identifier used to uniquely identify an individual within a system. For example, a username used to login to a computer system is assigned to identify an individual as a user of a computer. The username is bound to a password which is used to authenticate that the person logging in to the computer is the same person who was assigned the identifier and given the password. This is a simple example of single factor authentication where the password represents a single, "something you know" authentication factor and the username represents an identifier.

Identifiers, such as the TWIC CHUID can be strengthened through the use of digital signature. A digitally signed identifier can be verified, to determine that is a genuine identifier of an individual that was issued by the system authority and has not been revoked or invented. However, the identifier by itself is generally public information and does not provide authentication that the person using it is the person to whom it was issued without an authentication factor, such as a password, known only by the authorized individual.

The proposed TWIC card itself offers three different elements that may be used to support authentication via the contactless interface of the card:

1) CHUID data object – A strong, digitally signed identifier issued by the TWIC Program after vetting the identity and an individual and determining that the individual is trustworthy.
2) TWIC biometric template – A strong "something you are" authentication factor that is strongly bound (unique) to the individual. The TWIC biometric template is strongly bound to the CHUID (identifier) and protected against alteration (counterfeit) through digital signature.
3) PIV Card Authentication Certificate and Key – A strong "something you have" authentication factor that is strongly bound to the user's smart card through proof of possession of a private key that exists only on the user's smart card and is never revealed. The use of the card authentication certificate and associated key provide strong proof that the card being presented to the TWIC reader is the genuine card that was issued to the individual by a trusted authority.

Note: While sometimes the CHUID may be referred to as a "weak" authentication factor, it should be noted that without biometric verification or card authentication, the CHUID is simply publicly available data that is transmitted over the TWIC contactless interface in clear text and can easily be captured, copied to another card or replayed, along with the digital signature attached to it. Caution should be exercised in relying on the CHUID as a "weak" authentication factor, even in low assurance applications since it can be captured by an attacker without user consent or knowledge.

This appendix describes the process that would be required to authenticate one or more of these factors against the card. An access control system could choose to supplement or replace these with off-card

authentication information in a database if desired. For example, a PACS PIN could be stored in the access control system and compared on entry, even though the TWIC card application does not support this capability internally. However, these off-card authentication checks are outside the scope of this document.

A.1 CHUID Verification

The CHUID is a freely readable data object that is digitally signed (to prevent such a number from being modified or invented by an un-authorized party), but is neither encrypted nor strongly bound to the physical card. The signed object contains the unique Federal Agency Smart Credential Number (FASC-N) identifier, which should be used as the primary identification number for the card. The FASC-N may also be found in the Transportation Worker Unique Information data object (tag = 0xDFC100) without any digital signature.

Before using a CHUID (or the FASC-N it contains) the digital signature of the issuer should be verified in order to make sure the credential number is not altered or invented. This verification may take place when the CHUID is downloaded from a trusted source to the PACS for insertion in the authorized CHUID access control list (a white list in the PACS) or can be done when the CHUID of a new worker is enrolled in the PACS, or at the first time a CHUID is used by a PACS. Under no condition should a CHUID be used if its digital signature has never been verified by the PACS or a reader attached to the PACS.

The first time a CHUID is found in a PACS system (enrolment, download, or first use), the digital signature shall be verified and the access control system shall perform the following steps to use the CHUID for authentication:

4) The reader selects the TWIC card application
5) The reader gets the complete contents of the CHUID data object.
6) The reader shall decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the certificate for the document signer (guaranteeing the CHUID was created by an accredited issuer) that is used to verify the signed objects on the card.
7) The reader searches the CHUID object to find the FASC-N tagged (0x30) value.
8) The reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or all or part of selected elements of the FASC-N.

In some operations the FASC-N of a CHUID may be used for access control by a PACS when previously registered (white list verification). In such a case, the access control system would perform the following steps for authentication:

1) The reader selects the TWIC card application.
2) The reader gets the contents of the Transportation Worker Unique Information data object (which contains an unsigned FASC-n along with the expiration date).
3) The reader searches the data object to find the FASC-N tagged (0x30) value.
4) The reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or all or part of selected elements of the FASC-N.

A.2 TWIC Biometric Authentication

The TWIC card application (as well as the PIV card application in the same card) contains a pair of fingerprint templates bound to the cardholder's FASC-N identifier via the digital signature of the card issuer. The signed fingerprint templates are stored in the TWIC card application in a format that is encrypted using a card-specific TWIC Privacy Key (TPK). This key is not itself available via the contactless interface, although it could be retrieved via either the magnetic stripe interface or contact interface of the card. This retrieval of the TWIC Privacy Key from the card could occur at each reader during each access transaction, or the TWIC Privacy Key could be obtained by the reader from the Physical Access Control System (PACS) where the corresponding TPK would be stored as a one-time operation during card registration in the local access control system.

In order to confirm that the cardholder matches the stored biometrics, the data must be retrieved, decrypted, verified, and then matched against a live finger.

1) The reader loads the Privacy Key for the card from memory, a server, the magnetic stripe of the card, or the contact interface of the card.
2) The reader selects the card's TWIC applet
3) The reader selects the fingerprint object.
4) The reader gets the contents of the fingerprint data object.
5) The encrypted fingerprint template TLV (tag: 0xBC) is retrieved from the fingerprint data object.
6) The encrypted fingerprint template is decrypted using the TWIC Privacy Key.
7) The CBEFF record is parsed into the ANSI/INCITS 378-2004 fingerprint body, FASC-N and the digital signature.
8) The reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the reader have a verified copy of the document signer's X.509 digital certificate. The public key from this verified document signing cert must verify the signed biometric data. There are two options for the reader to obtain the document signing certificate for the card.
    a) The reader could retrieve the document signer's certificate from the CHUID signature field, since the CHUID must be signed by the same entity as the biometric. The reader must verify that the CHUID signing certificate from the card was signed by one of the trusted card issuing Certificate Authorities from the TSA or another locally trusted issuer. The CHUID signing certificate must also be verified for expiration, and the certificate must contain the id-PIV-content-signing keyPurposeID extendedKeyUsage extension.
    b) The reader could be locally configured with a copy of every trusted document signing certificate. This may improve performance, since the certificate does not need to be retrieved from the card, but may increase the local management burden as document signing certificates are added and removed.
9) An index finger is sampled from the cardholder. This image must be matched against one of the fingerprint templates stored in the signed biometric object at an appropriate level of confidence (see section 8). If the fingerprint does not match the template on the first attempt, the reader may prompt for subsequent attempts without requiring the card to be re-read.
10) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object can be used as the identification number. This value must match the FASC-N from any other authentication factors that are matched to know that they are bound together by the card issuer.

A.3 Card Authentication Key Authentication

In addition to a TWIC card application, every TWIC card also contains a separate application with its own application identifier (AID) that conforms to the Personal Identity Verification (PIV) specification as referenced in the NIST FIPS 201-1 standard and its associated special publications. The PIV card application includes a Card Authentication Key and Certificate that can be used from the contactless interface for the purpose of authenticating that the card was issued by a trusted authority and is not cloned or faked. This provides a tool that strongly binds the cardholder's identity (via the FASC-N) to the physical card token by embedding a piece of secret data in the chip that cannot be copied via any interface. This key data can be used in conjunction with the freely readable certificate to prove that the card has not been cloned or spoofed. Note that this key is defined as a local key to the PIV application, only available after selection of the PIV application and shall not be accessible via the TWIC card application.

This process requires that a credential presented to the system (or the reader it is connected to) must be capable of performing an asymmetric Private Key operation such as RSA signature generation. This requires that the token be issued with the optional Card Authentication Key and Certificate as specified in NIST SP 800-73. The certificate profile standardizing the contents of the Card Authentication Certificate is documented by the Federal Identity Credentialing Committee's Shared Service Provider subcommittee.

Note that, unlike the Certificate/Key containers used exclusively on the contact interface of the FIPS-201 credential, the Card Authentication Certificate does not require or support a PIN to unlock for usage. This means that the contactless FIPS-201 card only represents a strong single factor (possession), and any additional authentication factors (PIN, biometric) would need to be managed externally to the card application itself (either in the PACS with a PACS PIN, or using another application such as TWIC in the card for biometric authentication of the user). To support local (on-card) second and third factor authentication with a FIPS-201 PKI credential, having only the PIV card application, the contact interface of the card must be used.

The reader (or panel, with bi-directional wiring) must be locally configured with the public keys (or, more typically, a full X.509 certificate containing the public keys) for one or more Certificate Authorities (CAs) that are trusted for issuance of TWIC Card Authentication Certificates. This could be limited to the issuing CAs for the TSA, or could include external CAs from other agencies to authenticate federated identities. This would likely be the same set of trusted CAs that must be stored on the reader in order to authenticate the CHUID signing certificate on a card, as required for biometric verification. The cryptographic operations performed by the reader (e.g., RSA signature verification) would be of the same type as those required by the biometric verification, so would require an equivalent level of computing resources at the reader (e.g. a 32 bit embedded processor or cryptographic coprocessor).

The public key information in the reader is not treated as a secret or sensitive data, so extraction of this data from a reader would not create a security risk, but incorrect configuration of a reader with illegitimate Authority Keys could result in that reader accepting the authenticity of an illegitimate token.

The reader (or bi-directional panel) would also need to have access to a system clock capable of providing the current date and time in order to determine the expiration status of the credential.

The output of the reader upon successful authentication would depend on the infrastructure capabilities and requirements. At a minimum, the reader could produce the encoded FASC-N for the card, which is pulled from the Card Authentication Certificate. Alternately, the entire verified Card Authentication Certificate could be passed to the access control system for more advanced processing.

1) The reader selects the PIV Applet
2) The reader gets the content of the Card Authentication data object (tag = 5FC101).

3) The reader retrieves the binary contents of the Certificate value (tag: 0x70).
4) The reader retrieves the content of the CertInfo value (tag: 0x70).
5) If the least significant bit of the CertInfo value is '1', then the contents of the Certificate value are compressed using the "gzip" algorithm, and are decompressed by the reader to produce the raw DER-encoded X.509 certificate. Otherwise, the contents of the Certificate value can be used without decompression.
6) The "issuer" name in the Certificate is compared against the "subject" name in each trusted issuing CA certificate stored on the reader. For each CA with a matching name, the Public Key is used to attempt to verify the signature on the token's Certificate. If no matching CA certificate is found on the reader with the same name and with a Public Key that verifies the signature on the certificate, then the Certificate is rejected.
7) If the date encoded in the Certificate's "notBefore" validity date is after the current date/time, or if the Certificate's "notAfter" validity date is before the current date/time, the Certificate is rejected.
8) If the Certificate's "keyUsage" extension does not contain the "digitalSignature" flag, the Certificate is rejected.
9) If the Certificate's "extendedKeyUsage" extension does not contain the "id-PIV-cardAuth" keyPurposeID (2.16.840.1.101.3.6.8), the Certificate is rejected.
10) If the Certificate's "subjectAltName" extension is present,j with the "pivFASC-N" name entry, this value shall be retrieved from the certificate for optional transmission to a panel or back-end (e.g. IdMS infrastructure).
11) If the Certificate contains any unknown extensions with the Criticality flag set to TRUE, the Certificate is rejected.
12) The reader generates a random or pseudo-random challenge of at least 127 bytes of unique data and transmits this to the container's GENERAL AUTHENTICATE command.
13) The response (i.e. the card's signature) from the GENERAL AUTHENTICATE command is verified using the Public Key from the Certificate. If verification fails, the card is rejected.
14) If verification has succeeded, the Certificate is accepted as an assurance factor. Identifying information (e.g. the Certificate, the FASC-N, or other unique identifying components) may be immediately used locally or at a panel as input for the access control rules, or supplemental second and third factors (e.g. PIN, biometric) may be independently evaluated.
15) If the biometric authentication factor was also verified, then FASC-N identifier from the biometric must be identical to the FASC-N contained within the Card Authentication Certificate. If they do not match, then the biometric and card does not belong together, so one must be rejected.

Appendix B TWIC Privacy Key Network Processing

This describes the method used to perform the TWIC Privacy Key retrieval from the PACS system.

This is based on a simple XML-RPC (see http://www.xmlrpc.com/) based Request/Response message:

An example input request would be:

```
POST /RPC2 HTTP/1.0
User-Agent: reader
Host: reader1
Content-Type: text/xml
Content-length: xx

<?xml version="1.0"?>
<methodCall>
  <methodName>KeyLookup</methodName>
  <params>
    <param>
      <value><base64>eW91IGNhbid0IHJlYWQgdGhpcyE=</base64></value>
      </param>
  </params>
</methodCall>
```

The input parameter value corresponds to the unique user ID that was read from the TWIC card as a binary value and base64 encoded.

The response would be the base64-encoded 128-bit (16-byte) AES encryption key:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 158
Content-Type: text/xml
Date: Fri, 17 Jul 1998 19:55:08 GMT
Server: UserLand Frontier/5.1.2-WinNT

<?xml version="1.0"?>
<methodResponse>
  <params>
    <param>
      <value><base64>39dWTDDSQewqrsdfdesaqsa=</base64></value>
      </param>
  </params>
</methodResponse>
```

Appendix C Reader Adaptability

C.4 Change of operation mode

The reader shall support multi-mode operation and be able to accept external triggers for the mode change. A mode change would apply to applications such as a threat level change (e.g., maritime security or MARSEC levels).

C.5 Accepting new operating modes

The reader should be capable of various modes whether currently defined by the Coast Guard or not. Also, it is anticipated that TWIC will be expanded to all transportation modes in the future. Therefore, readers should be capable of supporting secure firmware modification allowing definition of new modes of operations as may be required.

Appendix D TWIC Reader Compatibility With Other Card Types

Some sites may need to use TWIC readers and the associated PACS with other cards in addition to the TWIC. In some situations, a TWIC reader may be required to read multiple card types such as the Department of Defense Common Access Cards (CACs) and the Federal Personal Identity Verification (PIV) cards as well as TWIC cards. In such an environment, a reader should be capable of selecting the application identifier (AID) associated with these different card types and then behaving according to the requirements of that card type. For a site that may use multiple card types, the TWIC reader should support configuration of default AIDs.

As no standard mechanism exists to recognize the card type presented based only on the ATS (answer to select) or ATR (answer to reset), each reader has to use a sequence in which it will select the card application. For example, at an access point where most cards are CAC cards, the TWIC reader could be configured by default to first start by selecting the CAC application, then the TWIC if no CAC application is found in the card, then the PIV if no TWIC or CAC application is found. In most situations, the TWIC is expected to be the prevalent card used and for this reason, the TWIC should be the configured as the default application by the reader manufacturer unless otherwise specified by the site.

Note: As the PIV Card application and the TWIC card application are using the same data object identifier (tag value) for the CHUID, it is also possible, for a reader which needs only the CHUID to make a decision, to first try to get the CHUID (Get Data CHUID) without knowing which application was selected by default in the card presented. If the request is successful and the CHUID is known by the PACS, this is the fastest way to recognize multiple card application types. If this request is unsuccessful, a full application selection process is required before rejecting the card.

Appendix E TWIC AID Structure

This section presents how the TIWC Application Identifier is defined and how it should be used in the TWIC applications developed in readers and terminals.

The AID used for the TWIC application will consist of a 5 bytes RID and a 6 bytes long PIX.

E.6 Registered Identification and Application Identifier

TSA has obtained an international Registered Identifier (RID) according to ISO/IEC 7816-5 represented by the string "A0 00 00 03 67". This string is also called the TSA RID.

E.7 PIX Structure

All TSA applications using the RID "A0 00 00 03 67" will have a similar structure.

The first two bytes of the PIX are used to define the group to which the application belongs. The values '00 00' and 'FF FF' are not defined for now and reserved. The following group values are defined:

- applications used by TSA employees or contractors: group = '10 00'
- applications used by non TSA employees or contractors: group = '20 00'

The following two bytes of the PIX are used to identify the application within a group. The values '00 00' and 'FF FF' are not defined for now and reserved. The following applications are allocated:

Group '20 00'

- TWIC application number '00 01'

The following byte of the PIX is used to identify the release of the specification as well as the nature of the card. If the first most left bit of this byte is set to one ('1') it indicates the card is a test card. If the leftmost bit is set to zero it is a normal application card. This allows the terminal to set itself in diagnostic mode and execute some more testing/diagnostic functions (when not disabled) when a test card is presented. The current release of this specification is defined as release '1' (or '000 0001' in binary format.

The following and last byte of the PIX is used by the card to indicate the version of the specification. The values '00' and 'FF' are so far reserved for future use and not defined. The current TWIC card specification is version '01.

Bytes of the AID	Symbol	Value	Comment
1 to 5	RID	A0 00 00 03 67	TSA RID
6 & 7	Grp	00 00 & FF FF	Reserved values
		10 00	TSA employees & contractor group
		20 00	non TSA employees or contractors group
8 & 9	App	00 00 & FF FF	Reserved values
		00 01	TWIC application in group 20 00
10	Release	00 & 7F	Reserved values
		1xxx xxxx	If bit on indicates test card
		01 or 81	TWIC specification release 1
11	Version	00 & FF	Reserved values
		01	TWIC application version 01

Note: the AID may use up to 16 bytes and TSA reserves the right to use all the possible 11 bytes of the PIX in other applications.

The current possible AIDs for a TWIC card are:

A0 00 00 0x xx 20 00 00 01 01 01	Operational TWIC Card
A0 00 00 0x xx 20 00 00 01 81 01	Test TWIC card

Only one TWIC AID per card will ever exist but a given card may have a different TWIC application version than another card.

Note: The terminal looking for the TWIC application should always use a partial select command and ask for the first 9 bytes of the TWIC AID.

The card will respond with the full AID of the TWIC application it has (including release and version as well as the test bit indicator) and the terminal will have to verify it can work with the version returned by the card. Specifications expect to be upward compatible.

In case a new TWIC application specification cannot be made upward compatible, (thus creating a potential problem for existing terminals) a new application will have to be used (App bytes of the PIX).

Appendix F Use of the Get Response APDU at the application layer

Most cards in use today, as well as interface drivers or card readers, are using short length fields in APDU coding thus limiting the amount of data which can be received (256 bytes) in a single APDU command. This creates a protocol limitation of data block exchanges between the client application and the card application. Such cases are explained in ISO/IEC 7816-3 and some options are available in ISO/IEC7816-4 to address the issue.

When cards, drivers and readers will all be able to use the extended length of APDUs, data blocks of up to 64Kbytes of information will be exchanged without having to deal with such low level concerns. In the meantime, it is important to separate clearly this issue at the transport layer and not impact the application layer when cards will be more powerful.

Two different mechanisms are available in ISO/IEC 7816-4 to address this short length APDU issue. One is the command chaining, commonly used for case 3 commands (e.g. Put data DA in PIV) but this is not always supported by the same card for case 2 commands (e.g. Get Data CA) or case 4 commands (e.g. odd INS bytes such as Get data CB). The other possibility is the use of the Get Response command at the application layer interface.

The recommended mode operation is to use the command chaining process but as this mode is not mandated for commands retrieving information from the card by any ISO, PIV or this TWIC specification, the card may not support such behavior. And, unfortunately other than trying the command, there is no simple way to know if the card will accept command chaining for retrieval of information (i.e. Get Data odd INS byte).

It seems most PIV compliant cards (either T=0 or T=1) do use the Get Response either for each elementary block (T=0 at the transport protocol layer) or for blocks larger than 256 bytes at the application layer (T=1 and T=CL) in order to retrieve the next data block when Le = 00 and the data size to be returned is larger than 256 bytes. This is why this solution is explained in order for TWIC terminal manufacturers to implement TWIC application in a coherent manner their.

In most TWIC terminal implementations, the limit between the TPDU layer (transport layer dependent on the transport protocol) and the APDU (application layer interface) may be difficult to establish but it is highly recommended to terminal manufacturers to keep these two layers separated as they are between ISO/IEC 7816-3 and ISO/IEC 7816-4. This will allow better interoperability and less dependencies on a given card implementation. This appendix describes how terminals should implement the use of the Get Response command in their interface layer for various cards.

This specification does not address (or use) the Get Response and length management defined is secure messaging modes (e.g. Global platform). The description below should be compatible but does not cover all secure messaging behavior of smart cards.

In the description below, it will be assumed the following:

- The application layer has a maximum buffer size available of 64Kbytes. This means the application layer places the requests in extended length format. The application does not know the type of protocol the card is using.
- The interface layer (driver) has a maximum buffer size of 256 bytes. It means that all requests to the card are placed using a short length format.
- The card may or may not support extended length but receives all the requests in short length formats.

- For any layer, a length of Le = 00 in short format or a length of Le = FF 00 00 in extended format always means "all you can get" up to the size of my receiving buffer (00 = 256 or FF 00 00 = 64K bytes)

For T=1 cards the driver layer will:

1. Issue a Get Data command to the card with a maximum length of Le = '00'.
2. If the data object length is smaller than 256 bytes, the card will respond with the data object, the actual length of the data object in the block returned and a return code of 62 82 in response indicating there are less data than expected.
3. If the data object is larger than 256, the card will respond with the first 256 bytes of data and send a return code of SW1-SW2 = 61 xx. The driver layer will then re-issue a get Response command for a length of Le = xx until it receives the return code 90 00 (all data retrieved) or until it has reached the maximum data required by the application layer (64K bytes).

For T=0 cards, the driver layer will translate APDUs to TPDUs

1. Issue the Get Data command odd INS Byte to the card (without any Le)
2. The card returns no data (not possible in T=0) in response to the Get Data and provides a return code of 61 xx indicating the command has been successful and xx bytes of information are available. The driver then issues a Get Response with a length Le = xx. If the return codes are again 61 xx, the driver loops on this function until it gets a return code of 90-00 or it reaches the maximum of bytes required by the application layer (64K).