

Document Number: NMSAC-TWIC-READER Feb2007

TWIC Smart Card Reader Hardware Specification DRAFT v 1.0

Feb. 16, 2007

Sponsor

National Maritime Security Advisory Committee TWIC Working Group

Abstract: The document describes the hardware requirements for smart card readers supporting the Transportation Worker Identification Credential (TWIC). This credential is used to access secure areas and information in transportation facilities according to a facility's security plan control requirements.

Keywords: TWIC, smart card, biometrics, fingerprint.

Status summary

Contacts

Lisa Himber, Vice-Chair, National Maritime Security Advisory Committee (NMSAC)
Maritime Exchange for the Delaware River and Bay
Tel: (215) 925-2615
Email: lisa.himber@maritimedelriv.com

Basil Maher, President & Chief Operating Officer
Maher Terminals, Inc.
Tel: (908) 665-2100
Email: basil@maherterminals.com

Table of contents

Contacts.....2

1. Overview7

 1.1 Scope and purpose.....7

2. References8

 2.1 Normative References8

 2.2 Informative References9

3. Definitions10

 3.1 Conformance levels.....10

 3.2 Glossary of terms10

 3.3 Acronyms and abbreviations11

4. TWIC Modes of Operation.....12

 4.2 System Perspective.....12

 4.2.1 Physical Access Control.....12

 4.2.2 Portable Identity Verification.....15

 4.3 Portable Verification15

5. Fixed Reader Requirements.....17

 5.1 Physical Requirements17

 5.1.1 Device Dimensions17

 5.1.2 Environmental17

 5.1.3 Impact Resistance.....18

 5.2 Electrical Requirements18

 5.3 Safety.....19

 5.4 Electromagnetic/Vibration Compatibility19

 5.4.1 47CFR18 and/or CISPR 11 (Emissions).....19

 5.4.2 IEC 61000-4-2 (Electrostatic Discharge)19

 5.4.3 IEC 61000-4-3 (Radiated RF Immunity)20

 5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst).....20

 5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode).....20

 5.4.6 IEC 61000-4-5 (Surges)20

 5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)20

 5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions).....20

6. Portable Reader Requirements22

 6.1 Portable Reader Specific Requirements:22

 6.1.1 Operational Features22

 6.1.2 Environmental Requirements22

 6.1.3 Electrical Requirements23

7. Operational Requirements24

8. Performance Requirements.....27

9. Operational Availability28

10. Delivery29

Appendix A Authentication Processing.....30

A.1 CHUID Authentication.....	30
A.2 TWIC Biometric Authentication	31
A.3 Card Authentication Key Authentication	32
Appendix B TWIC Privacy Key Network Processing.....	36
Appendix C MARSEC Level Processing	38
Appendix D TWIC Reader Compatibility With Other Card Types.....	39
Appendix E Description of Concept for Contactless Biometric Data Protection for TWIC	40
E.1 Scope.....	40
E.2 Purpose	40
E.3 Overview.....	40
E.3.2 Advantages	41
E.3.3 Disadvantages	41
E.3.4 Placing the TPK Code on the Magnetic Stripe	42
E.4 Alternative Implementations.....	42
E.4.1 Readers Connected to a PAC System with Two-way Communications.....	43
E.4.2 Readers Connected to a PAC System with One-way Communications	43
E.4.3 Readers Not Connected to a PAC System	44
E.4.4 Operational Biometric as a Viable Alternative to TPK.....	44

List of figures

Figure 4.1 Generic Biometric-based Access Control System.....	13
---	----

List of tables

Table 4.1 MARSEC Requirements12
Table 4.2 Biometric Access System Key Descriptions14
Table 4.3 Portable Card Reader Hardware Requirements16
Table 7.1 75-bit Wiegand Output Format.....24
Table 7.2 48-bit Wiegand Output Format.....25

1. Overview

1.1 Scope and purpose

This document specifies the requirements for smart card readers, both fixed and portable, supporting the Transportation Worker Identification Credential (TWIC). 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 has been 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 is comprised of 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.

2. References

2.1 Normative References¹

- [R1] Security Policy for DAL C3 Applet Suite, Dreifus Associates, Ltd.
- [R2] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers
- [R3] ANSI/INCITS 378-2004, Information Technology – Finger Minutiae Format for Data Interchange
- [R4] ANSI/INCITS 358-2002, Information Technology – BioAPI Specification
- [R5] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)
- [R6] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts
- [R7] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards
- [R8] SIA AC-01 (1996.10), Access Control – Wiegand Card Reader Interface Standard
- [R9] FIPS 186-2, Digital Signature Standard
- [R10] FIPS 197, Advanced Encryption Standard
- [R11] FIPS 46-3, Data Encryption Standard
- [R12] FIPS 140-2, Security Requirements for Cryptographic Modules
- [R13] UL 294, Standard for Safety of Access Control System Units
- [R14] EN 50081-1 (1992), European Standard, “Electromagnetic Compatibility – Generic Emission Standard, Part 1: Residential, Commercial and Light Industry”
- [R15] IEC 60068-2-64, “Environmental Test – Part 2: Test Methods – Test FH: Vibration Broadband Random (Digital Control) and Guidance
- [R16] IEC 61000-6-1 “Electromagnetic Compatibility – Generic Immunity \Standard, Part 1: Residential, Commercial and Light Industry”
- [R17] IEC 61000-4-2 (Electrostatic Discharge)
- [R18] IEC 61000-4-3 (Radiated RF Immunity)
- [R19] IEC 61000-4-4 (Electrical Fast Transient/Burst)
- [R20] IEC 61000-4-6 (Radio Frequency Common Mode)
- [R21] IEC 61000-4-5 (Surges)
- [R22] IEC 61000-4-8 (Power Frequency Common Mode)

¹ Some normative references may only apply to certain reader configurations

- [R23] IEC 61000-4-11 (Voltage Dips and Interruptions)
- [R24] IEC 68-2-27 (1987), International Electrotechnical Commission, “Basic Environmental Testing Procedures, Part 2: Tests – Test Ea and Guidance: Shock”
- [R25] IEC 68-2-29 (1987), International Electrotechnical Commission, “Basic Environmental Testing Procedures, Part 2: Tests- Test Eb and Guidance: Bump”
- [R26] OSHA Regulation 1910.147 De-energizing Equipment
- [R27] 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
- [R28] NEMA 250-1997 standard (<http://www.nema.org>)

2.2 Informative References

- [R29] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)
- [R30] FIPS 201 Errata FIPS 201-1 Change Notice (<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)
- [R31] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)
- [R32] ICAO 9303 Machine Readable Travel Documents
- [R33] 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)
- [R34] TSA *Guidance Package – Biometrics for Airport Access Control* (30 September 2005)
- [R35] 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 stored on the TWIC card.

3.2.3 Minutiae template: A minutiae template is a mathematical representation of the pattern of ridge endings and branches in a fingerprint.

3.3 Acronyms and abbreviations

BAC Basic Access Control

CHUID Card Holder Unique Identifier

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 Identity 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 requirement for using various authentication mechanisms at certain MAESEC levels has yet to be decided. For the purposes of this specification, it is assumed that the MARSEC levels correspond to the following operational requirements:

MARSEC Level	Requirement
I	Card only (i.e., read of the CHUID only through the contactless interface)
II & III	Card + biometric (this will require that all TWIC readers include a fingerprint sensor; this can be bypassed during MARSEC I conditions).

Table 4.1 MARSEC Requirements

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

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

The following diagram 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.

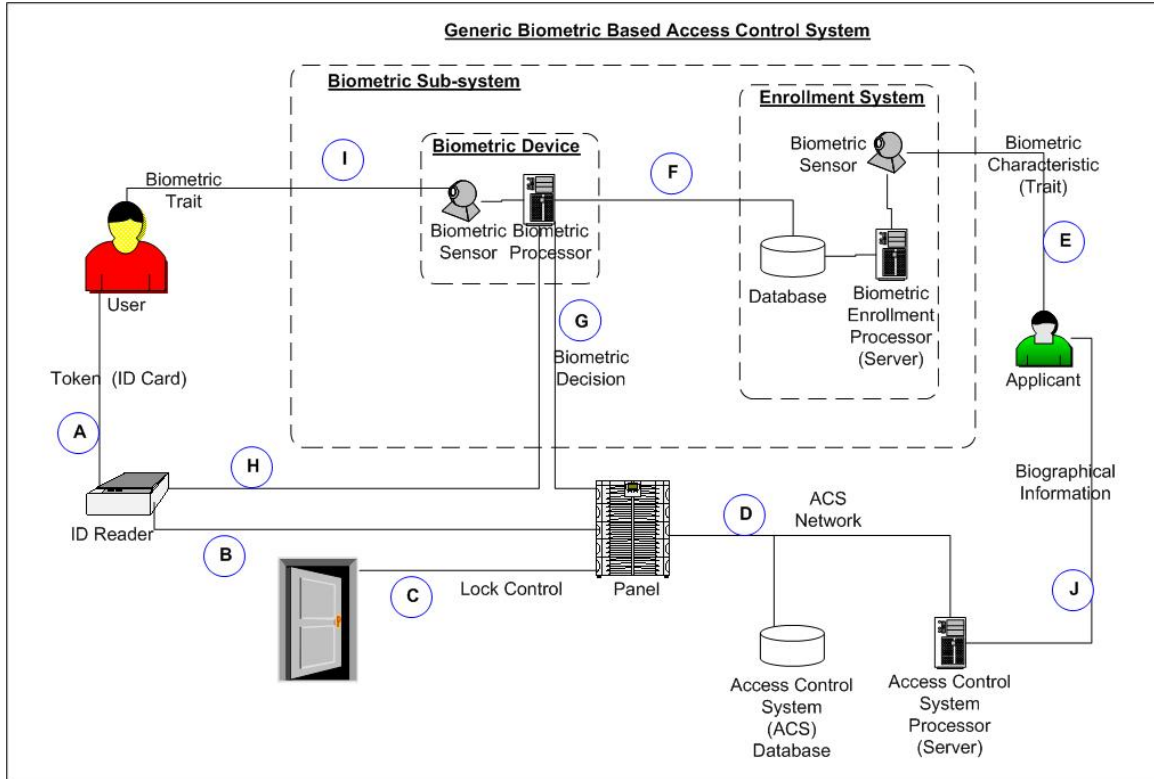


Figure 4.1 Generic Biometric-based Access Control System

Where:

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.
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

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 biometric will be encrypted when stored on the card and will remain encrypted during transmission to the reader over the contactless interface. The key used to decrypt the biometric, 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 it has been pre-registered.

4.2.1.2 Network Attached Reader

A network attached reader² 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 “card only” mode, or temporarily stores this information for transmission after a successful biometric match when in “card + biometric” mode. If the reader is in “card + 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.
- 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 authenticates the biometric against the template and signals the physical access control system.

4.2.1.3 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 “card + biometric” mode. If the reader is in “card only” mode no further information is required from the card.
- 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 to the template read from the card and signals the physical access control system.

Since the TWIC Privacy Key is also stored in the 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 terminal 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.

4.3 Portable Verification

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 used by the portable device as described below:

Card Reader Type:	Requirements to read card biometric template:
Contact	Access TWIC Privacy Key from contact
Contactless	Access TWIC Privacy Key from magnetic stripe

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.

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.

5.1.2 Environmental

5.1.2.1 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.

5.1.2.2 Indoor

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

5.1.3 Impact Resistance

Biometric device identification 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.

5.1.3.1 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.

5.1.3.2 Bump

Reader shall survive 100 bumps defined by IEC 68-2-29 (1987) each with a nominal peak accelerating of 10 g (100m/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 except 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.

If the portable reader has a contact interface, the TWIC Privacy Key can be accessed through this interface and there is no requirement for magnetic stripe reader.

If the portable reader has 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. Operational Requirements

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 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.

The reader 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.

The reader 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.

The Wiegand output format shall follow that specified for FIPS 201-based systems. The GSA Approved Products Listing tests 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

The reader 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 PACS system 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

The reader 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 the MARSEC level (see Appendix C for further details).

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 swipe a magnetic stripe that might be required in certain implementation configurations.

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 may provide liveness detection as a manufacturer's option.

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. No ability for enrollment interoperability between biometric readers is required for the TWIC program since enrollments will all be performed by TSA using a uniform methodology and not by individual biometric readers.

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.

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:	E.g. a badge, a metal key or a smart card
Something you know:	E.g. a PIN or a password
Something you are:	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 compromise. An access control system may achieve the required level of authentication security by checking factors against either the card or its own database.

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

1. CHUID data object – weak “something you have” authentication factor
2. TWIC biometric template – strong “something you are” authentication factor
3. PIV Card Authentication Certificate and Key – strong “something you have” authentication factor

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 PIN could be stored in the access control system and compared on entry, even though the card does not support this capability internally. However, these off-card authentication checks are outside the scope of this document.

A.1 CHUID Authentication

The CHUID is a freely readable data object that is digitally signed (to prevent forgery of the data itself), but is neither encrypted nor strongly bound to the physical card. The signed object contains the unique FASC-N identifier, which should be used as the primary identification number for the card.

In order to check the CHUID authentication factor from a TWIC card, an access control system may perform the following steps.

-
- 1) The reader selects card's TWIC applet
 - 2) The reader selects CHUID object.
 - 3) The reader gets the contents of the CHUID data object.
 - 4) The reader searches the CHUID object to find the FASC-N tagged (0x30) value.
 - 5) 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.
 - 6) The reader may decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the certificate for the document signer that is used to verify the signed objects on the card.

The CHUID authentication factor has the advantage of being relatively simple and quick to retrieve. This factor is considered relatively weak, since it would be very easy to copy a CHUID from a valid card and then copy it to a cloned or emulated card. This copy could be done without possession of the card by getting near a cardholder with a contactless reader.

A.2 TWIC Biometric Authentication

The TWIC contains a pair of fingerprint biometrics bound to the cardholder's FASC-N identifier via the digital signature of the card issuer. The signed fingerprint templates are stored on the card in a format that is encrypted using a card-specific "TWIC Privacy Key." 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) could happen 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 Privacy Key.
- 7) The CBEFF template 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 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 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-like applet 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 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.

This process requires that a credential presented to the system 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 internally represents a strong single factor (possession), and any additional authentication factors (PIN, biometric) would need to be managed externally to the card itself. To support local (on-card) second and third factor authentication with a FIPS-201 PKI credential, 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 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 misconfiguration 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 selects the Card Authentication container (Container ID 0x0500).
 - 3) The reader retrieves the binary contents of the Certificate value (tag: 0x70).
 - 4) The reader retrieves the content of the CertInfo value (tag: 0x71).
 - 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, 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:

The input request would something like:

```
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 MARSEC Level Processing

The reader needs to 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). The reader would need to 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 multiple authentication factors as may be required.

Appendix D TWIC Reader Compatibility With Other Card Types

It is important to recognize those situations where a TWIC reader may be required to read multiple card types such as Department of Defense Common Access Cards (CACs) and Federal Personal Identity Verification (PIV) cards as well as TWIC cards. In such an environment, a reader should be capable of discovering the application identifier (AID) associated with these different card types and then behaving according to the requirements of that card type. For a card that might have multiple card types, the TWIC reader should default to the TWIC AID.

Appendix E Description of Concept for Contactless Biometric Data Protection for TWIC

E.1 Scope

This appendix describes the method included in this specification for using the TWIC card for automated physical access that enables

- cryptographic protection of the biometric data when stored on the TWIC card or when transmitted through the contactless interface,
- the avoidance of key management responsibilities for the access control system operators, and
- optimum transaction throughput

E.2 Purpose

It is expected that Department of Homeland Security policy will require that the fingerprint template stored on the TWIC card be protected during contactless transmission using encryption technology that is appropriate to the operational requirements of the maritime industry. The method described in this specification is intended to meet this requirement.

E.3 Overview

This method requires that the biometric templates be stored as encrypted data on the TWIC card and that the encrypted templates be freely accessed from either the contactless or contact interface. The biometric templates will be encrypted and placed in a separate container linked to the TWIC application during the process of updating the TWIC cards from Version 1 to Version 2. This update process will take place at TWIC enrollment centers and will be performed by trusted agents of the TSA. During the update process, encryption of the biometric templates will be based on a randomly generated 16 byte binary number, hereafter referred to as the TWIC Privacy Key (TPK), which is unique to each TWIC card. The encryption process will use the strong AES encryption standard. As part of the update process, the TPK will be stored on the magnetic stripe in a track reserved by TSA for this purpose. The TPK will also be stored in a separate memory container on the TWIC card chip that can only be accessed through the contact interface. The TPK is used to decrypt the biometric templates at the time of user authentication. The TPK is not considered a “shared secret” in the cryptographic sense and therefore requires no special protection or key management protocol. Each TPK is only usable for the decryption of the templates stored on that specific TWIC card.

At the point of access using a fixed mount reader, a TWIC card holder will swipe the TWIC card through a magnetic stripe reader and will then place the TWIC card in close proximity to the contactless reader to transfer the unique ID and encrypted template to the reader. The TPK read from the magnetic stripe will be used to decrypt the template read from the contactless interface of the card. Then the card holder will place their finger on the fingerprint sensor and the reader will perform the matching function. If the match is successful, the reader will send the unique ID to the physical access control (PAC) system which will make the decision to open the gate based on the privileges associated with that unique ID.

E.3.2 Advantages

The primary advantage of this approach is that there is no requirement for storing secret keys in readers or requiring an elaborate scheme of key management. The approach will achieve the privacy and security objective by encrypting the biometric data when stored on the TWIC card such that it will remain encrypted during any contactless transmission and can only be decrypted by a reader that has obtained the TPK stored elsewhere in the card. It can be assumed that the reader is a valid TWIC reader because the card holder has made the decision to present the card to the reader for the purpose of access to a facility or vessel. Conversely, a contactless reader that does not have the ability to obtain the TPK data from the magnetic stripe or through the contact card interface would not be able to decrypt any biometric data read from the contactless interface of the card.

If a TWIC card is lost or stolen, the TPK on the card can be obtained. If the person now in possession of the card has detailed knowledge of the method used to generate the cryptographic key from the TPK, it would be feasible for that person to obtain the biometric template data over the contact or the contactless interface. But the card could not be used for access since the person now holding the card would not have the same fingerprint as the card holder. So the potential impact is limited to the privacy exposure of biometric data from one lost card and that card does not pose a security threat to the system. It should also be noted that privacy risk associated with the loss of a card would exist anyway since the name, photo and possibly other personally identifiable information is also printed on the surface of the card.

The proposed method effectively prevents “farming” a significant number of biometric templates without the card holder’s knowledge or consent because a rogue reader placed in close proximity to a TWIC card would not have the TPK from that card which is required to decrypt the templates.

E.3.3 Disadvantages

There are disadvantages to this approach. Requiring the reading of a magnetic stripe will impact:

- Reader cost
- Throughput
- Human factors issues associated with presentation of the card to multiple sensors

This approach assumes that magnetic swipe reader modules are commercially available that are capable of operating in an outdoor weather exposed environment. It is also assumed that commercial reader manufacturers are including magnetic swipe readers on some of their reader models that also read contactless smart cards and fingerprints. Since most users are more familiar with the use of magnetic swipe card readers at the retail point of sale, the motion of swiping the card should be natural and fast. However, if magnetic card swipe was added as a user action at high volume entry points, throughput will still be negatively impacted.

E.3.4 Placing the TPK Code on the Magnetic Stripe

Due to the schedule constraints for the launch of the Version 1 TWIC cards, it may not be practical for TSA to record the TPK code on a reserved track of the magnetic stripe at the time of initial card production. If this is the case, it will be necessary to generate and transfer the TPK to the magnetic stripe during the one-time process of updating the card to a Version 2 card. This update process will be required in any case to place the TWIC application software and data objects on the Version 1 TWIC cards. We assume that this update function will occur at a TWIC enrollment center staffed by TSA trusted agents using workstations configured for this purpose. Each of these workstations would require the addition of a magnetic stripe encoding device which otherwise would not be required to update the TWIC application software and data objects onto the smart card memory chip. This update function would only be necessary for TWIC version 1 cards. New cards issued as Version 2 cards would already contain the necessary TPK data on the magnetic stripe as well as the TWIC application software and data objects.

E.4 Alternative Implementations

This approach offers flexibility to the operator in how it can be implemented within a facility or vessel. These alternative implementations can support readers that are connected to a PAC system with two-way communications capability, readers connected to a PAC system with a one-way communications capability and readers that are not connected to a PAC system. Following is a description of each.

E.4.1 Readers Connected to a PAC System with Two-way Communications

For those facilities that demand maximum throughput, we are assuming that the facility operator has a PAC system and that supports two-way communications with the reader. We also assume that the reader is capable of two-way communications with the PACS. The reader must have the ability to read contactless smart cards and fingerprints but does not need to have the capability to read magnetic stripes. The objective of this implementation is to eliminate the need to use a magnetic swipe device at the reader for every transaction in order to increase throughput. This implementation requires that each user be registered into the PAC system in advance. During the registration process, the unique identifier is read from the card's CHUID object on the smart card chip and the TPK is automatically read from the magnetic stripe or contact interface of the card. Both the unique identifier and TPK are then stored in the PAC system along with any other data related to access privileges for this card holder.

When a TWIC card is presented to the reader, the unique card holder identifier is read from the card through the contactless interface and sent to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system sends the TPK back to the reader. The reader uses the TPK to decrypt the biometric template read from the card. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends a signal to the PAC system. The PAC system opens the gate or turnstile.

Another permutation of this implementation can reduce the amount of data exchange between the reader and the PAC system. In this case, the reader has sufficient memory such that the PAC system can periodically broadcast all pre-registered user IDs and TPKs for storage at the reader. When a TWIC card is presented to the reader, the unique card holder identifier and encrypted templates are read from the card through the contactless interface. The unique ID is compared to the list stored in the reader. If the identifier is present, the reader uses the TPK code for that user (also stored in the reader) to decrypt the biometric templates read from the TWIC card. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends the unique ID to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system opens the gate or turnstile.

E.4.2 Readers Connected to a PAC System with One-way Communications

In this implementation, the TWIC reader only has one-way communication to the PAC system (e.g. Wiegand interface). The reader then must have the capability to read magnetic swipe cards, contactless smart cards, and fingerprints. While it is assumed that users will be pre-registered

into the PACS system, it will not be necessary to read and store the TPK in the card holder's record within the PACS system.

The card holder will swipe the card in the magnetic reader slot. The user then presents the card to the contactless reader surface and the reader reads the unique ID and encrypted template. The reader uses the TPK read from the magnetic stripe to decrypt the templates. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends the unique identifier to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system opens the gate or turnstile.

E.4.3 Readers Not Connected to a PAC System

This implementation is generally associated with a handheld mobile reader device that may or may not be connected to the PAC system through a wireless interface. For initial deployment of Version 1 TWIC cards, the Coast Guard may use such handheld readers for spot checking. Since the Version 1 cards will be similar in design to the Federal Employee Personal Identity Verification (PIV) card, it will not be possible to read the biometric data except through a contact interface and then only after entry of a six digit PIN. Therefore, at a minimum, the handheld reader used for this purpose must have the capability to read contact smart cards and fingerprints and must include a keyboard for PIN entry.

If handheld readers are deployed in the context of the proposed method, they only require a change to the application software. The card holder or operator will insert the card in the contact reader slot. The reader obtains the unique identifier, TPK and encrypted templates through the contact interface. The reader decrypts the templates using the TPK. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader checks its list of authorized users or sends a remote request to the PAC system to confirm that the unique identifier has been granted access privileges. The response will be displayed to the operator who will then grant access.

E.4.4 Operational Biometric as a Viable Alternative to TPK

Another alternative implementation is available that avoids the use of the TPK for each access transaction since there is no need to transmit the biometric template from the card to the reader. This implementation has been previously discussed as the concept called "operational" biometrics and would be available for those operators with PAC systems with either one-way or two-way communications with the reader. This concept requires that each user be registered into the PAC system in advance. During the registration process, the unique identifier is read from the card's

CHUID object on the smart card chip and the encrypted biometric template on the TWIC card is also read and decrypted using the TPK stored in either the magnetic stripe or obtained through the contact card interface. The decrypted biometric templates are then stored in the PAC system along with any other data related to access privileges for this card holder. In addition to the option of using the enrolled fingerprint templates stored on the TWIC card for this registration process, it is also possible to enroll a different type of biometric to store in the PAC system (e.g., iris or hand geometry).

When a TWIC card is presented to the reader, the unique card holder identifier is read from the card through the contactless interface and sent to the PAC system as an index pointer to the biometric data stored on the PAC system. The card holder presents their finger to the sensor. The reader generates a template and sends the template to the PAC system. The PAC system matches the presented biometric to the biometric stored in the PAC system. If the match is good and the card holder has privilege to enter, the PAC system opens the gate or turnstile. It is important to note that this operational biometric implementation can be used in conjunction with Version 1 TWIC cards. The disadvantage to this approach is that some card holders might object to the operator maintaining a database of their biometric template for privacy reasons.