



**TWIC Reader Hardware
And
Card Application Specification**

March 28, 2008

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

TWIC Reader Hardware and Card Application Specification

VERSION CONTROL

<p>Version 1 September 11, 2007</p>	<p>Initial release of the specification.</p>
<p>Version 1.1 March 28, 2008</p>	<p>Clarification and technical corrigendum of Version 1 of the specification. Revisions are detailed in Section 1.3 of this document.</p>

Table of contents

1. Overview	7
1.1 Abstract	7
1.2 Scope and purpose	7
1.3 Summary of Changes to the September 11, 2007 Specification	7
1.4 Summary of Changes to the NMSAC Specification.....	9
2. References	12
2.1 Normative References	12
2.2 Informative References	13
3. Definitions	14
3.1 Conformance levels	14
3.2 Glossary of terms.....	14
3.3 Acronyms and abbreviations	15
4. TWIC Modes of Operation	16
4.2 System Perspective	17
4.2.1 Physical Access Control	17
4.2.2 Portable Identity Verification	20
5. Fixed TWIC Reader Requirements.....	22
5.1 Physical Requirements	22
5.1.1 TWIC Reader Dimensions	22
5.1.2 TWIC Reader Mounting.....	22
5.1.3 Environmental	22
5.1.4 Impact Resistance.....	23
5.2 Electrical Requirements.....	23
5.3 Safety	23
5.4 Electromagnetic/Vibration Compatibility	23
5.4.1 47CFR18 and/or CISPR 11 (Emissions)	24
5.4.2 IEC 61000-4-2 (Electrostatic Discharge)	24
5.4.3 IEC 61000-4-3 (Radiated RF Immunity).....	24
5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst).....	24
5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode)	24
5.4.6 IEC 61000-4-5 (Surges)	24
5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)	24
5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions).....	25
6. Portable TWIC Reader Requirements	26
6.1 Portable TWIC Reader Specific Requirements:	26
6.1.1 Operational Features.....	26
6.1.2 Environmental Requirements	26
6.1.3 Electrical Requirements	27
7. TWIC Reader Operational Requirements	28
8. Performance Requirements.....	30
9. Operational Availability	31

TWIC Reader Hardware and Card Application Specification

10. Delivery	32
11. TWIC Card Application	33
11.1 Card application Identifier	33
11.2 Key Reference(s)	33
11.3 ICC Data Model	33
11.4 Magnetic Stripe Data Model.....	36
11.5 TWIC Card Application Command Set.....	36
11.5.1 SELECT	37
11.5.2 GET DATA	38
Appendix A Authentication Processing (NORMATIVE)	40
A.1 CHUID Verification	43
A.2 TWIC Biometric Authentication	44
A.3 Card Authentication Key Authentication	45
Appendix B TWIC Privacy Key Network Processing (INFORMATIVE).....	48
Appendix C TWIC Reader Adaptability (NORMATIVE)	50
C.1 Change of operation mode	50
C.2 Accepting new operating modes	50
Appendix D TWIC Reader Compatibility With Other Card Types (INFORMATIVE).....	51
Appendix E TWIC AID Structure (NORMATIVE).....	52
E.1 Registered Identifier (RID)	52
E.2 Proprietary Identifier Extension (PIX) Structure	52
Appendix F Use of Get Response APDU at the application layer (INFORMATIVE).....	54
Appendix G Interpretation of the Biometric Template CBEFF Header (NORMATIVE).....	56

List of figures

Figure 4.1 Generic Biometric-based Access Control System..... 18

List of tables

Table 4.1 TWIC Identification and Authentication Modes..... 16

Table 4.2 Biometric Access System Key Descriptions 19

Table 4.3 Portable Card TWIC Reader Hardware Requirements 21

Table 7.1 75-bit Wiegand Output Format 28

Table 7.2 48-bit Wiegand Output Format 29

Table 11.1 Unsigned Card Holder Unique Identifier.....34

Table 11.2 TWIC Key Privacy Buffer.....34

Table 11.3 Signed Card Holder Unique Identifier35

Table 11.4 Card Holder Enciphered Fingerprint Templates.....35

Table 11.5 Security Object35

Table 11.6 Data Objects in the TWIC Card application Property Template (Tag '61') 37

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 readers, both fixed and portable, to be used with the Transportation Worker Identification Credential (TWIC).

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.

1.2 Scope and purpose

The scope of this specification is:

- TWIC reader requirements
- TWIC card application data model
- TWIC card application card edge behavior during normal operation

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, 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.

1.3 Summary of Changes to the September 11, 2007 Specification

Version 1.1 of this specification is a clarification and correction of the September 11, 2007 release of the TWIC Reader Hardware and Card Application Specification. Section 1.4 of this document was not included in the editorial process so as to preserve the original comments as written in the September 11, 2007 release.

All comments, suggestions or additional change requests should be directed to the Project Editor, Gerald.Smith@associates.dhs.gov.

Summary of changes is as follows:

- 1) General editorial changes from "must" to "shall".
- 2) General editorial changes from "will" to "shall".
- 3) General editorial changes from "would" or "could" to "should".
- 4) General editorial changes from "might" to "may".
- 5) General editorial changes from "can" to "may".
- 6) General editorial changes from "terminal" to "TWIC reader".

TWIC Reader Hardware and Card Application Specification

- 7) General editorial changes from “device” to “TWIC reader”.
- 8) General editorial changes from “crypt” to “cipher”.
- 9) General editorial changes from “magstripe” to “magnetic stripe”.
- 10) General editorial changes to use “TWIC reader” instead of “reader” as appropriate for purposes of clarity.
- 11) General editorial changes to use the term “template” in a consistent manner throughout the document.
- 12) General editorial changes from “enrollment” to “registration” when referring to a PACS.
- 13) General editorial changes to correct spelling errors.
- 14) General editorial changes to provide alternate expression for the purpose of clarity.
- 15) General formatting changes for consistency.
- 16) Addition of a Version Control table at the beginning of the document.
- 17) Revised the date of the document on the cover and on each page to March 28, 2008.
- 18) Added Section 1.3 detailing the changes from the September 11, 2007 release of the specification.
- 19) Added definitions in Section 3.1 for the terms “informative” and “normative”.
- 20) General editorial changes to Table 4.2 for harmonization of the text to Figure 4.1.
- 21) Revised the sequence of steps in Section 4.2.1.3 to read the TPK from the magnetic stripe later in the sequence (as the magnetic stripe reading step is conditional upon TWIC reader mode and successful processing of the CHUID).
- 22) Modified the language in Section 5.1.2 on tamper evident means by the substitution of “will have the ability to send...” for “should have the ability to send...”.
- 23) Section 5.1.3.1, revised sub-headers to include the language “Use requirements” to clarify said requirements only apply when the TWIC reader is to operate in the specified environment.
- 24) Revised language in Section 7 related to an automated alert which now states “... lockout after a configurable number of consecutive failed biometrics matching attempts”.
- 25) Section 11.3 First Table header modified to indicate Maximum Length is in bytes.
- 26) Section 11.3 First Table corrects the length of the signed CHUID from 3000 bytes to 3377 bytes as specified in SP 800-73 Revision 1.
- 27) Section 11.3 First Table corrects the length of the Security Object from 920 bytes to 1000 bytes as specified in SP 800-73 Revision 1.
- 28) Section 11.3 First Table Note 4 revised to remove the incorrect reference to the TPK hash being present in the Security Object.
- 29) Section 11.3, Table 11.5 Note 1 removed the incorrect reference to the TWIC Privacy Key hash in the description of hashes represented in the Security Object.
- 30) Section 11.3, Table 11.5 Note 2 added the word “signed” just before CHUID for clarity.
- 31) Section 11.5 reworded Notes 2 and 3 for clarity.
- 32) Section 11.5.1 Table 11.6 modified to accurately reflect the contents of the card application property template.
- 33) Section 11.5.2 changed “See table A” to “refer to Section 11.3 ICC Data Model”.
- 34) Added for clarity an INFORMATIVE or NORMATIVE qualifier, as appropriate, to each Appendix title.

TWIC Reader Hardware and Card Application Specification

- 35) Added to Appendix A language describing the differences between TWIC and PIV OIDs to include the addition of a table detailing TWIC OID and PIV OID values.
- 36) Appendix A, section A.1 first paragraph corrected by changing “Transportation Worker Unique Information data object (tag = 0xDFC100) without digital signature” to “unsigned CHUID data object (tag = 0x5FC104)”.
- 37) Appendix A, section A.1 last bulleted list, bullet 2 changed “Transportation Worker Unique Information” to “unsigned CHUID”.
- 38) Appendix A, section A.2 changed language related to PACS storage of the TPK from “...is presumed to be stored...” to “...should be stored...”.
- 39) Appendix A, section A.2 changed Bullet #8 sub-paragraph a) by deleting “...also be verified for expiration, and the certificate shall...”. [The validity period check for the Issuer certificate is of limited value].
- 40) Appendix A, section A.2 changed Bullet #8 sub-paragraph a) by deleting “The CHUID signing certificate shall contain the id-TWIC-content-signing keyPurposeID extendedKeyUsage extension”. [There is no extendedKeyUsage extension in the Issuer Certificate].
- 41) Appendix A, section A.2, changed Bullet #9 from “An index” to “A”.
- 42) Appendix A, section A.3 Bullet #9 corrected from “id-PIV-cardAuth” to “id-TWIC-cardAuth”.
- 43) Appendix A, section A.3 Bullet #9 corrected OID from the PIV reference of “2.16.840.1.101.3.6.8” to the TWIC reference of “1.3.6.1.4.1.29138.6.8”.
- 44) Appendix A, section A.3 Bullet #10 corrected from “pivFASC=N” to “twicFASC=N” to include adding the relevant OID reference of “1.3.6.1.4.1.29138.6.6”.
- 45) Completely revised Appendix B to use actual TWIC sample data for the FASC-N and TPK instead of the random data used in the previous release.
- 46) Added a note in Appendix B encouraging the use of a fixed length response from a PACS for the TPK.
- 47) Revised Appendix E to define the meaning of the release edition bytes of the PIX (within the TWIC AID).
- 48) Editorial changes to Appendix F to include capitalization of APDU commands referenced.
- 49) Added Appendix G (NORMATIVE) which describes how to interpret the Biometrics template CBEFF header to determine if the 1:1 biometrics matching logic may be executed.

1.4 Summary of Changes to the NMSAC Specification

Version 1.0 of 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.

TWIC Reader Hardware and Card Application Specification

- 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)

TWIC Reader Hardware and Card Application Specification

- 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 References¹

- [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] GlobalPlatform 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 *presumed* by this specification. Other hardware and software design models may also be implemented.

3.1.2 informative: portion of the document that explains the specification or provides guidance on the use of the specification.

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

3.1.4 normative: portion of the document that details the requirements of the specification.

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

3.1.6 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 encipher 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. TWIC physical access readers shall 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 a 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 a TWIC card 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 presumes that Personal Identity Numbers (PINs) are not a requirement for authentication at any MARSEC level.

TWIC is based upon a PIV compatible smart card and carries both a PIV card application and a TWIC card application that may be independently selected. This allows a TWIC card 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. Card authentication is not supported by the TWIC card application. That said, card authentication over the contactless interface is supported through the selection of the PIV card application.

4.2 System Perspective

This specification describes two types of TWIC readers that may 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 TWIC readers may operate in indoor environments or in outdoor environments exposed to the weather.
- Portable Verification Reader – a handheld TWIC reader that may be used for portable, spot-check identity verification.

A TWIC card may also be verified using contact smart card readers 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 TWIC readers that shall 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 a physical access control system (as a whole), a biometric sub-system boundary, and a biometric TWIC reader. 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 shall be used at a door or gate that may or may not be manned. The ISO/IEC 14443 contactless interface shall be used to transfer the unique ID number assigned to the cardholder and the biometric data between a TWIC card and a TWIC reader. The cardholder biometric template stored on a TWIC card is enciphered with a key unique to each TWIC card and remains enciphered during transmission to a TWIC reader over the contactless interface. The key required to decipher the reference biometric template of the user, called the TWIC Privacy Key (TPK), shall be obtained from one of several sources. These sources include the magnetic stripe encoded on each TWIC card, the TWIC card memory (but only accessible through the contact interface) or from the physical access control system where the TPK has been registered.

TWIC Reader Hardware and Card Application Specification

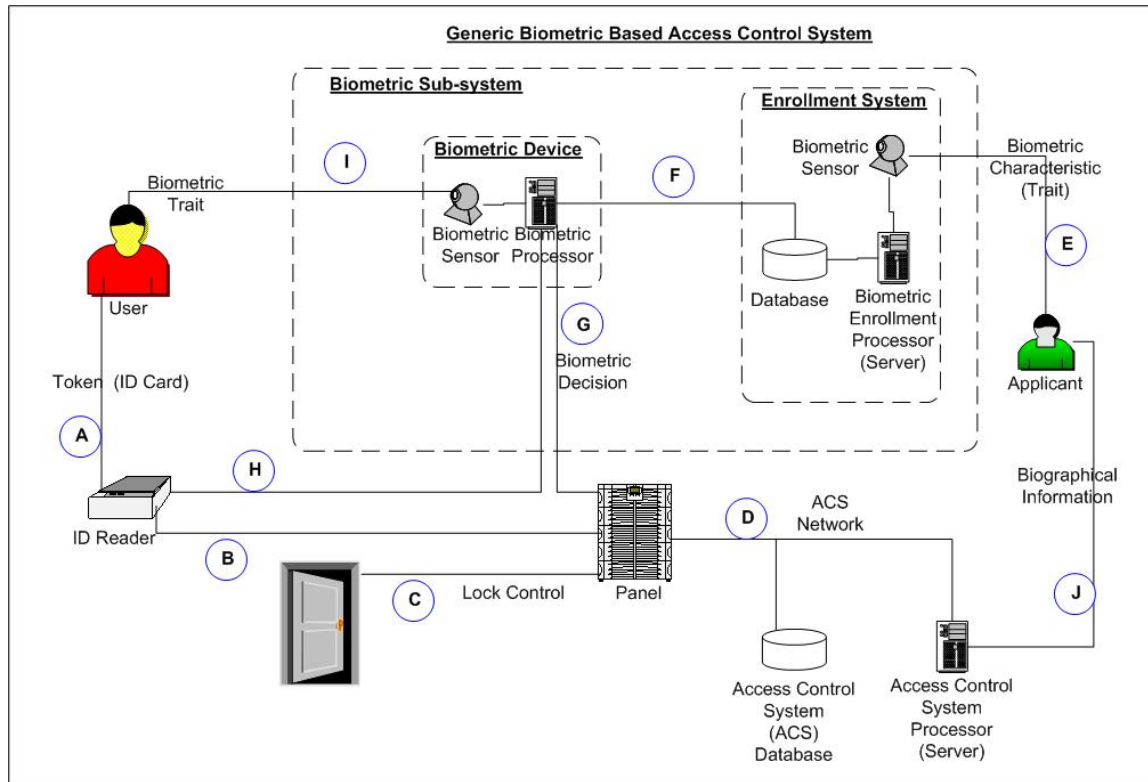


Figure 4.1 Generic Biometric-based Access Control System (ACS)

Key	Description
A	Any form of machine-readable credential (TWIC card) presented by the user to the ID TWIC reader to claim an identity.
B	User identity code (ID number, card number, ACS ID) read from the token by the ID TWIC 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	(Physical) communication channel (Ethernet, RS-485, etc.) enabling data interchange between the panel, ACS processor and database. (Logical) communications depends on site-specific implementation and includes user identity code data from the panel and user access authorization data from the 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.

TWIC Reader Hardware and Card Application Specification

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	YES/NO 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 an ID Card by the ID TWIC 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 the user and sensor such as indicator lights or audio cues.
J	Applicant-supplied information (name, address, etc.) obtained during ACS registration 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 TWIC Reader

A network attached TWIC reader² supports two-way communication between a TWIC reader and the physical access control system. A TWIC reader may use this communication channel to access the user's TWIC Privacy Key information that was stored during the process of registering the user into the PACS. TWIC verification consists of the following steps (presuming a user has previously registered with the local PACS). When a TWIC card needs to be verified, the following steps shall be followed:

- Present TWIC card to a contactless TWIC reader.
- TWIC reader reads the unique ID number from the TWIC 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 TWIC reader is in "CHUID + biometric" mode, the TWIC reader may use the unique ID number from the TWIC card to retrieve the user's TWIC Privacy Key previously stored in the PACS when the user registered into the PACS at the facility.
- The TWIC 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.
- TWIC reader gets the user's biometric template from the contactless interface on the TWIC card and deciphers 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.

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

4.2.1.3 Biometric Verification - Standalone TWIC Reader

A standalone TWIC 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 a contactless only TWIC reader, the TWIC Privacy Key shall be read from the magnetic stripe on the TWIC card. The following steps shall be followed:

- Present TWIC card to a contactless TWIC reader.
- TWIC reader reads unique ID number from the TWIC card and temporarily stores this information for transmission after a successful biometric match when in “CHUID + biometric” mode. If the TWIC reader is in “CHUID only” mode no further information is required from the card.
- TWIC reader reads the user’s biometric template from the contactless interface on the TWIC card and temporarily stores this information for use in a later step.
- The TWIC 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.
- User swipes their TWIC card through magnetic stripe reader to read the TWIC Privacy Key.
- TWIC reader deciphers the previously stored biometric using the TWIC Privacy Key obtained from the magnetic stripe.
- User presents their biometric.
- TWIC reader matches the presented biometric against the template obtained from the TWIC card.
- TWIC reader displays that the verification was confirmed or denied and signals the physical access control system.

Note: As the TWIC Privacy Key is also stored in the non-volatile electronic memory of the TWIC card, the TPK may alternatively be accessed through a smart card contact interface conditional upon said interface being supported by a stand-alone TWIC reader.

4.2.2 Portable Identity Verification

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

A TWIC card may be interrogated and verified using a portable handheld unit. The interface between the TWIC card and a TWIC reader may be via the contact or the contactless interface. A portable TWIC reader 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.

TWIC Reader Hardware and Card Application Specification

Access to the biometrics on a TWIC card depends on the TWIC reader card interface used. Biometrics access modes are described in Table 4.3 below.

Interface used to access the Biometric Template	Requirements to access the card biometric template
Contact Interface	<p>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.</p> <p>Using the TWIC card application: Obtain through the contact interface the enciphered biometric template as well as the key (TPK) used to decipher it. No PIN or other key material is required from the TWIC reader.</p>
Contactless Interface	<p>Using the TWIC card application: The enciphered biometric reference template being free readable over the TWIC contactless interface, the TPK required to decipher it may be obtained from three possible sources: the magnetic stripe of the card, the contact interface of the TWIC card application, or from the PACS system if the TPK was stored during TWIC card registration into the PACS.</p>

Table 4.3 Portable Card TWIC Reader Hardware Requirements

5. Fixed TWIC Reader Requirements

There exist electrical and physical interoperability requirements for fixed TWIC readers. These requirements detail the nature of the environment and in-place technologies a fixed TWIC reader shall interoperate with to be compliant and successful.

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

5.1 Physical Requirements

5.1.1 TWIC Reader Dimensions

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

5.1.2 TWIC Reader Mounting

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

Note: TWIC readers shall employ an ISO/IEC 14443 contactless RF technology (operating at 13.56 MHz). This RF technology is sensitive to location and electromagnetic conditions of the local environment. Installers should work in coordination with TWIC reader manufacturers to make sure no electrical field or metallic element shall interfere with the TWIC reader contactless RF communications field.

5.1.3 Environmental

5.1.3.1 Outdoor Use requirements:

TWIC readers shall conform to a NEMA 4 rating.

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

TWIC readers shall operate in a humidity range of 5-100%, condensing.

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

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

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

5.1.3.2 Indoor Use requirements:

TWIC readers shall operate in a humidity range of 5-90%, non-condensing.

5.1.4 Impact Resistance

TWIC reader verification functionality 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. TWIC reader manufacturers may base compliance on IEC 60068-2-64. Equivalent commercial practice or analysis may be substituted subject to approval by TSA.

5.1.4.1 Shock

TWIC 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 subject to approval by TSA.

5.1.4.2 Bump

TWIC 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 subject to approval by TSA.

5.2 Electrical Requirements

TWIC readers shall operate within a range of 8-48 VDC. Where necessary to operate from line voltage, a power supply approved for use with a TWIC reader shall be provided. TWIC readers may 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).

TWIC readers shall not exceed a 2.0 Amperes current requirement.

TWIC readers shall provide reverse voltage protection.

TWIC readers shall be FCC certified.

TWIC readers shall return automatically to normal operation after a loss of power event.

5.3 Safety

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

TWIC readers shall not possess:

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

5.4 Electromagnetic/Vibration Compatibility

TWIC 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)

- As per Section 5.2, TWIC readers shall be FCC certified.

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.
- Presumes 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 TWIC Reader Requirements

A portable TWIC reader may support a wireless interface to provide direct access to a PACS. In such a case, the wireless connection shall have the following security attributes:

- confidentiality (session key)
- active authentication of the TWIC reader or, the operator using the TWIC reader.

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

If a portable TWIC reader has only a contactless card read capability, the portable TWIC reader shall also have a magnetic stripe reader in order to access the TWIC Privacy Key. The TPK is needed to decipher the biometric information held within the TWIC card application. A portable TWIC reader shall be capable of confirming whether a TWIC card has been revoked.

6.1 Portable TWIC Reader Specific Requirements:

A portable TWIC reader shall meet the same specifications as a fixed TWIC reader, as appropriate, with the exception of the following differences:

6.1.1 Operational Features

Portable TWIC readers shall have a display suitable for user interaction.

Portable TWIC readers shall be able to display the current battery level.

Portable TWIC readers may use a touch screen or other suitable means for user input/control.

Portable TWIC readers should have a hibernation mode for protection against data loss.

6.1.2 Environmental Requirements

Portable TWIC readers certified for harsh conditions shall 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

Portable TWIC readers should be supplied with a rechargeable battery with 12 hours minimum operational time.

Portable TWIC readers shall be operable while charging.

Portable TWIC readers should have a maximum battery recharge time of 2 hours.

7. TWIC Reader Operational Requirements

TWIC reader operational requirements apply to all TWIC reader types except where noted.

The contactless smart card TWIC reader component shall conform to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1.

TWIC readers shall have a maximum contactless smart card read range of 10cm.

Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s, dependent on the contactless card communications speed capabilities.

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

TWIC readers shall require that a TWIC card, once read, shall be removed from the RF field for at least one second before attempting to read any new contactless card. This requirement is to minimize multiple reads of the same TWIC card for a single presentation.

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

Fixed TWIC 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 TWIC 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 TWIC reader shall output the following 75-bits:

Description	Position	Length (BITS)
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 TWIC readers may also support a 48-bit Wiegand output format when a TWIC reader includes a real time clock that may be used to verify the expiration date. In this case, it is presumed that the TWIC reader has the ability to process the expiration date. Some PACS control panels may not be able to

TWIC Reader Hardware and Card Application Specification

support both 48-bit and 75-bit Wiegand input at the same time. In such a case, a TWIC reader shall provide a method of setting the Wiegand output format as required by the local PACS.

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 (BITS)
Agency Code	1-14	14
System Code	15-28	14
Credential Code	29-48	20

Table 7.2 48-bit Wiegand Output Format

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

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

TWIC readers may contain additional user indications including lights, text messages, and audible indicators.

TWIC reader visual indicators shall be visible in daylight.

TWIC readers should have a finger guide to aid in proper finger placement on the sensor.

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

TWIC readers 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.

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

TWIC readers shall provide an automated alert or lockout after a configurable number of consecutive failed biometric matching attempts (i.e. the facility chooses the number of attempts).

TWIC readers may support a means of alerting the PACS/operator if the TWIC reader detects tampering.

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

8. Performance Requirements

TWIC readers should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to a TWIC reader and completion of the biometric match) of three seconds. This does not include the time required to acquire the TPK either using a magnetic stripe or through download from a PACS.

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

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

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

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

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

9. Operational Availability

Biometric enabled TWIC readers shall be able to handle 1 million touches without degradation.

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

10. Delivery

TWIC readers shall include technical manuals covering installation, operation and maintenance.

TWIC readers shall be packaged suitable for shipment to a designated installation point.

11. TWIC Card Application

The TWIC card application data model and card edge edition defined in this section is Version 1.1.

Annex E details the data model and card edge edition encoding convention within the Application Identifier (AID).

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 using a partial select 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, TWIC readers 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. The TPK is not used by the TWIC card application for any cryptographic function. The TPK is used by the client application to encipher (for storage in the card) or decipher (for use in a TWIC reader) 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 (BYTES)	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 Magnetic stripe also)	M
Card Holder Unique Identifier	0x5FC102 (0x3000)**	3377	Always Read	Contact and Contactless	M

TWIC Reader Hardware and Card Application Specification

Card Holder Fingerprints	0xDFC103 (0x2003)**	2500	Always Read	Contact and Contactless	M
Security Object	0xDFC10F (0x9000)**	1000	Always Read	Contact and Contactless	M

** The container IDs 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 includes 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 specific to an 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 the 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, to be used for the creation of the Security Object, shall be based on the contents of Data Objects as stored in the TWIC card application.

Table 11.1 Unsigned Card Holder Unique Identifier

Unsigned Card Holder 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 consists 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 TPK requires only 16 bytes of data storage. An additional 16 bytes have been added to the maximum size of the TPK element (Tag 0xC0) to support future algorithms.
2. The structural information consists of two additional bytes per element (simple TLV tag byte plus one byte for length). This requires a total of 40 bytes for this data object value.

TWIC Reader Hardware and Card Application Specification

Table 11.3 Signed Card Holder 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 consists of some additional bytes per element (simple TLV tag byte plus one or three bytes for length). This requires a minimum total of 12 bytes for this data object value.

Table 11.4 Card Holder Enciphered Fingerprint Templates

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

Notes:

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

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 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 signed CHUID. The 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 Magnetic Stripe Data Model

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

- The TPK is a 16 byte string used by an AES encipherment/decipherment algorithm.
- Track 1 of the TWIC magnetic stripe shall be reserved exclusively for the TPK character string. The TPK character string shall be encoded on the high-coercivity magnetic stripe track 1 of the card as defined in ISO/IEC 7811-6.
- Each nibble of the 16 bytes of the TPK shall 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 shall 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 in accordance with ISO/IEC 7811-2 shall 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 APDU command 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 readers, such APDU commands do not appear in this specification.
3. Beyond the tags described in this specification, some ISO/IEC 7816-6 tags may be available at the card interface in response to a GET DATA APDU command (e.g. Card Related Information). These tags are not required for interoperability in TWIC readers. Such additional tags are not described in this document as they are specific to either an applet implementation or the management features of an applet implementation.

TWIC Reader Hardware and Card Application Specification

11.5.1 SELECT*Command Syntax*

CLA	'00'
INS	'A4'
P1	'04' (Select by Name)
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	'00' or 'xx' -Length of TWIC card application property template if known

Note: In TWIC readers using the TWIC card, the SELECT "AID" APDU command shall always ask for a partial TWIC AID and analyze the information returned from a TWIC card when the SELECT APDU command 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 "AID" APDU command with a length of 11 bytes (c = 0x0B) shall, nevertheless, be supported by a TWIC card in order to be ISO/IEC 7816-4 compliant.

Card application Property Template

Upon successful 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. Refer to Appendix E.
Coexistent tag allocation authority	'79'	'07'	M	Coexistent tag allocation authority template. (Tag '4F')
Application RID coexistent with ISO/IEC 7816 name space for tags	'4F'	'05'	M	TSA RID

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

TWIC Reader Hardware and Card Application Specification

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	refer to Section 11.3 ICC Data Model
Le	'00' or 'xx' - 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' is explained in Appendix F of this document.
2. TWIC reader 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

TWIC Reader Hardware and Card Application Specification

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 APDU command (Tag list '5D' instead of '5C'). TWIC, in the same manner as PIV, does not support this alternate form of the GET DATA APDU command.

Appendix A Authentication Processing (NORMATIVE)

In order to determine the identity of a cardholder, an access control system shall 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 is difficult 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 may be strengthened through the use of a digital signature. A digitally signed identifier may be verified to determine that it is a genuine identifier for an individual, that said identifier was issued by the system authority, and the identifier has not been revoked or invented. However, an identifier by itself is generally public information and does not provide authentication that the individual using the identifier is the individual to whom the identifier was issued. An authentication factor, such as a password, should also exist. Further, the knowledge to satisfy a given authentication factor challenge should be limited to either the system authority (e.g. card authentication) or the individual (e.g. PIN or biometric) for whom the identifier was issued.

A TWIC card offers three different data 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 of an individual and determining that said 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 never revealed private key that exists only on the user’s smart card. The use of the card authentication certificate and associated private key provide strong proof that the smart card being presented to a TWIC reader is a genuine TWIC card that was issued to the individual by a trusted authority.

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

TWIC Reader Hardware and Card Application Specification

This appendix describes the process that may be used to authenticate one or more of these factors against a TWIC card. An access control system may choose to supplement or replace these authentication factors with off-card authentication information in a database. For example, a PACS PIN may be stored in the access control system and compared on entry, even though the TWIC card application does not support this capability. Such off-card authentication checks are beyond the scope of this specification.

TWIC employs the use of Public Key Infrastructure (PKI) to include signatures and certificates. TWIC issues five year certificates; the consequence of these longer life certificates is certain fields in the certificate have values that, by policy, vary from FIPS201. The following table provides the differences in the construction of TWIC Object Identifiers (OIDs) from their PIV equivalents. TWIC OIDs have the identical meaning to their PIV OID equivalents.

PIV OIDs are registered with the Computer Security Objects Registry for which NIST is the Registration Authority. The “PIV Root” is 2.16.840.1.101.3 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)}.

TWIC OIDs are registered with the Internet Assigned Numbers Authority (IANA). The “TWIC Root” is defined as 1.3.6.1.4.1.29138 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) twic-root (29138)}.

TWIC readers shall accept either OID value when parsing a signature or certificate from either the TWIC card application or the PIV card application.

PIV and TWIC Object Identifiers

ID	Object Identifier	Description
Certificate Policy		
id-TWIC-digital-signature	1.3.6.1.4.1.29138.2.1.3.5	May be asserted in the Certificate Policy field of an X.509 certificate
id-fpki-common-policy	2.16.840.1.101.3.2.1.3.6	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-TWIC-key-management	1.3.6.1.4.1.29138.2.1.3.6	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-fpki-common-devices	2.16.840.1.101.3.2.1.3.8	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.

TWIC Reader Hardware and Card Application Specification

ID	Object Identifier	Description
id-TWIC-devices	1.3.6.1.4.1.29138.2.1.3.8	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-fpki-common-authentication	2.16.840.1.101.3.2.1.3.13	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-TWIC-authentication	1.3.6.1.4.1.29138.2.1.3.13	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-fpki-common-cardAuth	2.16.840.1.101.3.2.1.3.17	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
id-TWIC-cardAuth	1.3.6.1.4.1.29138.2.1.3.17	May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.
Application Attributes		
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures.
twicFASC-N	1.3.6.1.4.1.29138.6.6	The twicFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures.
Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on PIV CHUIDS and PIV biometrics.

TWIC Reader Hardware and Card Application Specification

ID	Object Identifier	Description
id-TWIC-content-signing	1.3.6.1.4.1.29138.6.7	This specifies that the public key may be used to verify signatures on CHUIDS and biometrics that are present on either the TWIC or PIV card applications.
id-PIV-cardAuth	2.16.840.1.101.3.6.8	This specifies that the public key is used to authenticate the PIV card rather than the PIV cardholder.
id-TWIC-cardAuth	1.3.6.1.4.1.29138.6.8	This specifies that the public key is used to authenticate the TWIC card rather than the TWIC cardholder.
Certificate Extension		
id-PIV-NACI	2.16.840.1.101.3.6.9.1	The PIV NACI indicator extension indicates the status of the subject's background investigation at the time of credential issuance.
id-TWIC-interim	1.3.6.1.4.1.29138.6.9.1	The TWIC NACI indicator extension indicates the status of the subject's background investigation at the time of credential issuance.

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 a non-authorized party), but is neither enciphered 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 unsigned CHUID data object (tag = 0x5FC104).

Before using a CHUID (or the FASC-N it contains) the digital signature of the issuer should be verified in order to ensure 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 may be done when the CHUID of a new worker is registered 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 TWIC reader attached to the PACS.

The first time a CHUID is found in a PACS system (registration, 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:

- 1) TWIC reader selects the TWIC card application.
- 2) TWIC reader gets the complete contents of the CHUID data object.
- 3) TWIC 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.

TWIC Reader Hardware and Card Application Specification

- 4) TWIC reader searches the CHUID object to find the FASC-N tagged (0x30) value.
- 5) TWIC reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The TWIC reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or 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 should perform the following steps for authentication:

- 1) TWIC reader selects the TWIC card application.
- 2) TWIC reader gets the contents of the unsigned CHUID data object (which contains an unsigned FASC-n along with the expiration date).
- 3) TWIC reader searches the data object to find the FASC-N tagged (0x30) value.
- 4) TWIC reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The TWIC 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 present in the same card) contains a biometric template of fingerprint minutiae bound to the cardholder's FASC-N identifier via the digital signature of the card issuer. The signed fingerprint biometric template is stored in the TWIC card application in a format that is enciphered using a card-specific TWIC Privacy Key (TPK). The TPK is not available via the contactless interface, although the TPK may be retrieved via either the magnetic stripe or contact interface of a TWIC card. This retrieval of the TWIC Privacy Key from a TWIC card may occur at every TWIC reader during each access transaction, or obtained by a TWIC reader from the PACS where the corresponding TPK was stored as a one-time operation during card registration.

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

- 1) TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the magnetic stripe of a TWIC card, or the contact interface of a TWIC card.
- 2) TWIC reader selects a TWIC card's TWIC applet.
- 3) TWIC reader selects the fingerprint object.
- 4) TWIC reader gets the contents of the fingerprint data object.
- 5) The enciphered fingerprint template TLV (tag: 0xBC) is retrieved from the fingerprint data object.
- 6) The enciphered fingerprint template is deciphered 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) TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the TWIC reader have a verified copy of the document signer's X.509 digital certificate. The public key from this verified document signing certificate shall verify the signed biometric data. There are two options for the TWIC reader to obtain the document signing certificate for the card.

TWIC Reader Hardware and Card Application Specification

- a) The TWIC reader may retrieve the document signer's certificate from the CHUID signature field, since the CHUID shall be signed by the same entity as the biometric. The TWIC reader shall verify that the CHUID signing certificate from a TWIC card was signed by one of the trusted card issuing Certificate Authorities from TSA or another locally trusted issuer.
 - b) The TWIC reader may be locally configured with a copy of every trusted document signing certificate. This may improve performance, since this certificate does not need to be retrieved from each TWIC card, but may increase the local management burden as document signing certificates are added and removed.
- 9) A finger is sampled from the cardholder. This image shall be matched against one of the fingerprint minutiae 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 TWIC reader may prompt for subsequent attempts without requiring the TWIC card to be read again.
 - 10) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number. This value shall 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 is compatible with 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 may be used over the contactless interface for the purpose of authenticating that the card was issued by a trusted authority. This provides a mechanism 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 may be used in conjunction with the freely readable certificate to prove that the card has not been cloned or spoofed. Note that the card authentication key is defined as a local private key to the PIV application, only available after successful selection of the PIV application and is not accessible via the TWIC card application.

This mechanism requires that a credential presented to the system (or a TWIC reader it is connected to) shall be capable of performing an asymmetric Private Key operation such as an RSA signature generation. A TWIC card is issued with the optional Card Authentication Key and Certificate as specified in NIST SP 800-73, Revision 1. 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 the information prior to usage. This means that any contactless FIPS-201 card represents a strong single authentication factor (possession), and any additional authentication factors (PIN, biometric) need to be managed external to the card application itself (either in the PACS with a PACS PIN, or using another application such as the TWIC card application for biometric authentication of the user). To support local (on-card) second and third factor authentication with a FIPS-201 PKI credential, the PIV card application employing the contact interface of the card shall be used.

A TWIC reader (or panel, with bi-directional wiring) shall 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 may be limited to the issuing CAs for TSA, or may include external CAs from other agencies to authenticate federated identities. This may be the same set of trusted CAs that should be stored on each TWIC reader in order to

TWIC Reader Hardware and Card Application Specification

authenticate the CHUID signing certificate on a TWIC card, as required for biometric verification. The cryptographic operations performed by a TWIC reader (e.g., RSA signature verification) should be of the same type as those required by the biometric verification, and hence require an equivalent level of computing resources at a TWIC reader (e.g. a 32 bit embedded processor or cryptographic co-processor).

The public key information in a TWIC reader is not treated as secret or sensitive data, so extraction of this data from a TWIC reader does not create a security risk. However, incorrect configuration of a TWIC reader with illegitimate Authority Keys may result in that TWIC reader accepting the authenticity of illegitimate tokens.

A TWIC reader (or bi-directional panel) also needs to have access to a system clock capable of providing the current date and time. The current data and time is required to determine the expiration status of a TWIC card.

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

- 1) TWIC reader selects the PIV Applet.
- 2) TWIC reader gets the content of the Card Authentication data object (tag = 5FC101).
- 3) TWIC reader retrieves the binary contents of the Certificate value (tag: 0x70).
- 4) TWIC 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 a TWIC reader to produce the raw DER-encoded X.509 certificate. Otherwise, the contents of the Certificate value may 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 a TWIC 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 a TWIC 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-TWIC-cardAuth" keyPurposeID (1.3.6.1.4.1.29138.6.8), the Certificate is rejected.
- 10) If the Certificate's "subjectAltName" extension is present with the "twicFASC-N" (1.3.6.1.4.1.29138.6.6) 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) TWIC reader generates a random or pseudo-random challenge of at least 127 bytes of unique data and transmits this to the TWIC card using the GENERAL AUTHENTICATE APDU command.
- 13) The response (i.e. the card's signature) from the GENERAL AUTHENTICATE APDU command is verified using the Public Key from the Certificate. If verification fails, the TWIC card is rejected.

TWIC Reader Hardware and Card Application Specification

- 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 the FASC-N from the biometric shall be identical to the FASC-N contained within the Card Authentication Certificate. If they do not match, then the biometric and the TWIC card do not belong together, so one shall be rejected.

Appendix B TWIC Privacy Key Network Processing (INFORMATIVE)

This Appendix describes a method that may be used to perform the TWIC Privacy Key retrieval from a PACS system.

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

The Base64 conversion used in this Appendix was performed using a Web-based utility located at <http://www.motobit.com/util/base64-decoder-encoder.asp>.

The XML-RPC example uses the following data:

- 1) Request data using a FASC-N of 25 hexadecimal bytes with value of ->
D70339DAA1822C10842125A1685821084216C1B9870339A3EB

- 2) Return data of a TWIC Privacy Key of 16 hexadecimal bytes with value of ->
30313233343536373839303132333435

The Base64 encoding of the FASC-N yields ->

1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==

The Base64 encoding of the TWIC Privacy Key yields ->

MDEyMzQ1Njc4OTAxMjM0NQ==

An example input request using the FASC-N as a PACS record index is illustrated here:

```
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>1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==</base64></value>
```

```
    </param>
```

```
  </params>
```

```
</methodCall>
```

NOTE: The request Content-Length field value was not computed for this example.

Appendix C TWIC Reader Adaptability (NORMATIVE)**C.1 Change of operation mode**

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

C.2 Accepting new operating modes

TWIC readers should be capable of various modes whether currently defined by the Coast Guard or not. Also, it is anticipated that TWIC shall be expanded to all transportation modes in the future. Therefore, TWIC 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 (INFORMATIVE)

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 in addition to TWIC cards. In such an environment, a TWIC reader should be capable of selecting the application identifier (AID) associated with these different card types and, on successful selection of a specific card application, behave in accordance with the requirements of the specific card application. For a site that may use multiple card types, a TWIC reader should support the configuration of default AIDs.

As no standard mechanism exists to recognize the smart card type presented based only on the ATS (answer to select) or ATR (answer to reset), each TWIC reader is forced to use a sequence in which it shall apply one or more SELECT APDU commands to connect to a particular card application. For example, at an access point where most cards are CAC cards, a TWIC reader may be configured by default to first start by selecting the CAC card application, then the TWIC card application if no CAC card application is found in the card, then the PIV card application if no TWIC or CAC card applications are found. In most situations, the TWIC card is expected to be the prevalent card used and for this reason, the TWIC AID should be configured as the first application selected by the TWIC reader unless otherwise required by local operational policy.

Note: The PIV card application and the TWIC card application are using the same data object identifier (i.e. tag value) for the signed CHUID. It is also possible for a TWIC reader, which needs only the signed CHUID to make a decision, to first attempt to retrieve the signed CHUID by issuing a GET DATA “signed CHUID” APDU command without first sending a SELECT APDU command to a card. In this scenario, the default card application is implicitly selected when a TWIC card is presented. If the GET DATA APDU command is successful, and the signed CHUID is recognized by the PACS, this is the fastest way to recognize multiple card application types. Should the GET DATA APDU command be unsuccessful, one or more SELECT APDU commands are required before rejecting the card presented to a TWIC reader.

Appendix E TWIC AID Structure (NORMATIVE)

This section defines how the TWIC Application Identifier (AID) is defined and how it should be used in TWIC applications developed for TWIC readers.

The AID used for the TWIC application shall consist of a 5 byte Registered Identifier (RID) and a 6 byte Proprietary Identifier Extension (PIX).

E.1 Registered Identifier (RID)

TSA has obtained an international Registered Identifier (RID) in accordance with ISO/IEC 7816-5. The RID is represented here by the hexadecimal string "A0 00 00 03 67". This hexadecimal string is also called the TSA RID.

E.2 Proprietary Identifier Extension (PIX) Structure

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

The first two bytes of the PIX are used to define the group to which the card application belongs. The values '00 00' and 'FF FF' are currently not defined and these values are reserved for future use. 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 next two bytes of the PIX are used to identify the application within a group. The values '00 00' and 'FF FF' are currently not defined and these values are reserved for future use. The following applications are allocated:

Applications Group '20 00'

- TWIC application number '00 01'

The final two bytes of the PIX define the class of TWIC card and release edition. Release edition references the edition of the card application data model and card edge supported. Release editions are NOT linked to the Version number of this specification.

A major release value shall be changed if the card application data model is changed due to changes in mandatory data objects OR if the card edge (i.e. APDU commands) is modified or enhanced in a manner that would impact operational use of the TWIC card. Major releases start at "1".

A minor release value shall be changed if the card application data model is changed due to changes in optional data objects that may impact operational use of the TWIC card. Minor releases start at "1".

The next to last byte of the PIX is used to identify the major release of the data model and card edge edition as well as the class of TWIC card. If the most significant bit of this byte is set to one ('1') the card is a test TWIC card. In this case, a TWIC reader may configure itself in a diagnostic mode and execute one or more testing/diagnostic functions (presuming such a mode is allowed and enabled) when a test TWIC card is presented. The remaining 7 bits of this byte indicate the major release of the data model and card edge edition.

The major release of the data model and card edge edition is currently defined as release '1' (or '000 0001' in binary format).

TWIC Reader Hardware and Card Application Specification

The last byte of the PIX indicates the minor release of the data model and card edge edition. The minor release values '00' and 'FF' are currently not defined and these values are reserved for future use.

The minor release TWIC data model and card edge edition is currently defined as release '1' (or '0000 0001' in binary format).

A TWIC reader may use the least significant 7 bits of the major release and the all bits of the minor release to form a data model and card edge edition Version designation expressed as MAJOR.MINOR.

The TWIC application data model and card edge edition is currently defined as Version 1.1.

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	Major Release	00 & 7F	Reserved values
		1xxx xxxx	Bit 7 of value "1" indicates a test TWIC card
		01 or 81	TWIC specification major release 1
11	Minor Release	00 & FF	Reserved values
		01	TWIC application minor release 1

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 card applications.

The AIDs that shall be recognized for a TWIC card application are:

A0 00 00 03 67 20 00 00 01 01 01	Operational TWIC Card
A0 00 00 03 67 20 00 00 01 81 01	Test TWIC card

Only one TWIC AID release edition, using the PIX structure defined in this specification, shall exist on a given TWIC card.

Note: A TWIC reader looking for a TWIC card application should always use a partial SELECT APDU command and request only the first 9 bytes of the TWIC AID (i.e. "A0 00 00 03 67 20 00 00 01").

A TWIC card shall respond with the full AID of the TWIC card application that exists on this TWIC card (including the release edition as well as the test bit indicator). A TWIC reader shall verify if the TWIC reader supports the release edition (or test mode) returned by the TWIC card. Release editions of the data model and card edge should be upward compatible.

In the unlikely case a new TWIC card application release edition cannot be made upward compatible, (thus creating a potential problem for existing TWIC readers) a new application AID shall be defined using the TSA RID and a new PIX structure.

Appendix F Use of Get Response APDU at the application layer (INFORMATIVE)

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

When cards, drivers and readers are able to use the extended length format of APDUs, data blocks of up to 64K bytes of information may be exchanged without having to deal with low level data transport concerns. It is important to clearly explain this issue at the transport layer so the application layer is not adversely impacted when smart cards, in the near future, support large data block transfers.

Two different mechanisms are available in ISO/IEC 7816-4 to address this short length APDU issue:

1. Employ command chaining. This mechanism is commonly used for case 3 commands (e.g. PUT DATA with INS byte = 'DA') as used in PIV. Command chaining is not always supported by the same smart card for case 2 commands (e.g. GET DATA with INS byte = 'CA') or case 4 commands (e.g. odd INS byte GET DATA with INS = 'CB').
2. Use the GET RESPONSE APDU command at the application layer.

The recommended mechanism is to use the command chaining process but, as this mode is not mandated for commands retrieving information from a smart card by any ISO, PIV or TWIC specification, the smart card may not support such behavior. Unfortunately, other than trying the GET DATA APDU command with the command chaining bit set to "1", there is no simple way to know if the smart card accepts command chaining for retrieval of information (i.e. odd INS byte GET DATA with INS = 'CB').

Most PIV compliant smart cards (supporting transmission protocols T=0 or T=1) use the GET RESPONSE APDU command 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). This appendix details this GET RESPONSE mechanism with the motivation TWIC reader manufacturers may implement TWIC card interfaces in a consistent and coherent manner.

In most TWIC reader 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. It is highly recommended for TWIC reader manufacturers to keep these two layers separated. These layers exist to some extent "between" the specified behaviors detailed in ISO/IEC 7816-3 and ISO/IEC 7816-4. Separation of these layers should allow better interoperability and less dependency on a given TWIC card implementation.

This appendix describes a way TWIC readers should implement the use of the GET RESPONSE APDU command.

The described mechanism does not address (or use) the GET RESPONSE APDU command and length management defined in secure messaging modes (e.g. as defined in ISO/IEC 7816-4 or GlobalPlatform). The description herein should be compatible with secure messaging but may not cover all secure messaging behavior of smart cards.

In the description below, it shall be presumed that:

- The TWIC reader application layer has a maximum buffer size available of 64K bytes. The TWIC reader application layer makes all information requests using the extended length format. The TWIC reader application does not know the type of protocol the card is using.

TWIC Reader Hardware and Card Application Specification

- The interface layer (driver) has a maximum buffer size of 256 bytes. All interface layer (driver) requests to the smart card are made using a short length format.
- The smart 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 is always interpreted to mean "all you may get" up to the size of the requester's receiving buffer (i.e. '00' = 256 or 'FF 00 00' = 64K bytes).

For T=1 smart cards, the driver layer shall:

1. Issue a GET DATA APDU command to the smart card with a maximum length of Le = '00'.
2. If the data object length is smaller than 256 bytes, the smart card shall 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 bytes than expected.
3. If the data object is larger than 256, the smart card shall respond with the first 256 bytes of data and send a return code of SW1-SW2 = '61 xx'. Note that xx = '00' indicates at least 256 bytes of data is still available for transfer. The driver layer shall then re-issue a GET RESPONSE APDU command for a length of Le = 'xx' until it either receives the return code '90 00' (all data retrieved) or until it has reached the maximum data length supported by the application layer (i.e. 64K bytes).

For T=0 smart cards, the driver layer shall translate APDUs to TPDUs:

1. Issue the GET DATA APDU command (odd INS byte) to the smart card (without any Le).
2. The smart card returns no data (as this is not possible in T=0) in response to the GET DATA APDU command 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 APDU command with a length Le = 'xx'. If the return codes are again '61 xx', the driver loops on this function until it gets either a return code of '90 00' or it reaches the maximum data length supported by the application layer (i.e. 64K).

Appendix G Interpretation of the Biometric Template CBEFF Header (NORMATIVE)

The biometric template shall be encoded in a manner that communicates to a TWIC reader :

- 1) The presence of zero, one or two fingerprint minutiae patterns for use in 1:1 matching logic.
- 2) The quality level of said fingerprint minutiae for use in 1:1 matching logic.

The information in this Appendix is in accordance with SP 800-76-1.

TWIC readers shall first check the number of minutiae present to determine if a 1:1 match may proceed.

TWIC readers shall interpret the CBEFF header encoded information as follows:

Normal Case: At least One Usable Fingerprint Minutiae available for 1:1 matching

- 1) Use ANSI/INCITS 378-2004 Minutiae Template and ignore CBEFF Header Quality Field value³.

Exception 1: Unusable Fingerprint Minutiae to perform a 1:1 match

- 1) Examine ANSI/INCITS 378-2004 Minutiae Template for:
 - a) Number of Minutiae = 0
 - b) Fingerprint image Quality = 20 [lowest possible]
 - c) CBEFF Header Quality Field ≤ 0
 - i) Quality Value = -1 (Meaning -> Failed to compute a value by capture S/W)
 - ii) Quality Value = 0 (Meaning -> Quality too low for an effective 1:1 Match)

Exception 2: No Fingers Available at Enrollment Time. 1:1 matching not possible

- 1) Examine ANSI/INCITS 378-2004 Minutiae Template for:
 - a) Number of Minutiae = 0
 - b) Fingerprint image Quality = 20 [lowest possible]
 - c) CBEFF Header Quality Field < 0
 - i) Quality Value = -2 (Meaning -> Assignment not supported)

³ Note that, for some TWIC cards with usable fingerprint minutiae templates, the CBEFF Header Quality Field may contain the value "-2". The number of minutiae should always be checked prior to checking the CBEFF Header Quality Field.