Important note from TSA-TWIC regarding this TWIC NEXGEN documentation

The TWIC NEXGEN documentation consists of four parts:

1. Part 1 – General description of TWIC credential in use by the maritime industry,
2. Part 2 – TWIC card application data models (Legacy and NEXGEN), TWIC card application and card edge behavior during normal operation,
3. Part 3 – TWIC reader requirements to accept Legacy and/or NEXGEN TWIC cards,
4. Part 4 – TWIC registration and TWIC card use by a PACS.

Part 1 and Part 4 are documents created to help understand the use and principles attached to the use of the TWIC card. They are consistent with the other parts, but not used to test the cards or the readers. Part 2 and Part 3 are specifications, which are the requirements to comply with for the card (Part 2) and the readers using the cards (Part 3). The cards created by GPO are tested against Part 2 and the readers and systems in the field using the TWIC cards are tested using Part 3 as the reference documents.

The TWIC NEXGEN Part 2 specification contains the description of two TWIC card Data Models:

- TWIC Legacy (cards produced now)
- TWIC NEXGEN (cards to be produced soon).

IMPORTANT Notice: The planned TWIC card NEXGEN upgrade, described in these documents, has been designed to be backward compatible as much as possible with TWIC Legacy, but it is important to confirm that existing TWIC readers are compatible with TWIC Legacy as well as the new TWIC NEXGEN data model when it is used in backward compatibility mode.

In early 2024 some changes were implemented for Legacy TWIC Cards and these newly issued Legacy TWIC cards do not strictly comply with the 2012 documentation.

- In 2015 NIST indicated the use of the SHA-1 hash function was not secure enough and the TWIC cards issued now are using SHA-2. This is indicated in a TWIC technical advisory.
- In March 2024 the silicon chip used to build TWIC Legacy cards has been changed and the ATR of the chip is different. This is the only difference; all the application data are still compliant with the TWIC Legacy data model as described in the TWIC NEXGEN Part 2 Specification.

Regarding the NEXGEN version of the card, very minor changes are expected with the production model currently under development. A few details in the documentation details of the implementation (e.g. PDF 417) may still be slightly updated.

For technical information about these documents, the contact to use is: TWIC-Technology@tsa.dhs.gov

This page was last updated on March 14, 2024

Transportation Worker Identification Credential
TWIC® Specification

Part 2 – TWIC® Card Application
May 2024

Gilles Lisimaque

Gerald Smith

Lars Suneborn

Eric Berg

Department of Homeland Security
Transportation Security Administration
Enrollment Services and Vetting Programs
601 South 12th Street
Arlington, VA 20598-6025

VERSION CONTROL

January 2019	Version for Public comments
July 2019	Modifications incorporating industry comments
October 2019	Text revised for final publication
January 2020	Modifications incorporating Round 2 Industry Comments
February 2020	Correction of errors found in various places of the document.
May 2020	Technical corrections for coherence in the document
June 2021	Modification of the TAGS for coherence with PIV & ISO
September 2021	Added information about Algorithm identifier for Keys
January 2022	Added the four TSA E-Sticker Data Objects
February 2022	Error corrected in section 4.9 about the PDF417 example
March 2022	Typo corrected in section 4.7.2
April 2022	Removed the notion of a test bit in the TWIC AID
April 2022	Added header indicating this is not a final release
June 2022	Changes to allow the Visual Verification to be done without an agent present (Automatic Biometric verification)
July 2022	Added information about the TWIC PIN and the PIV PIN used by NEXGEN.. Made the Discovery Object in both Card applications (PIV & TWIC) mandatory.
August 2022	Some minor typos
August 2022	Update sections 4.3 & 4.5 with TWIC PIN information
November 2022	Correction in Section 4.9 of the PDF 417 example
March 2023	Minor corrections and spelling
June 2023	Added a PUK in the TWIC card application
July 2023	Correction of a typo in the section related to the TWIC PIN initial value. Appendix I about FASC-N added. Added reference to SP 800-73-4 too.
July 2023	Added a small section (3.3.5) about SHA-1 being phased out by NIST
July 24, 2023	Official release of the document
July 31, 2023	Minor typos and corrections in table of section 4.5 (color of cells)
August 8, 2023	Added in all four parts of the documentation a warning related to possible changes regarding the PUK (PIV & TWIC) as well as the format and content of the PDF 417
August 10, 2023	Changed in all four parts the documentation: The notion of TWIC PUK and TWIC PIN has been removed. This also makes the four TWIC protected e-stickers go away. The TWIC SDO will not be used but will be populated with Signed CHUID, Unsigned CHUID and Enciphered Fingerprints. In this version, only the PDF 417 still might be modified
August 29, 2023	Modified section 4.7.2 (Card Holder Enciphered Printed Card Information) to remove the signature of this Data Object.
September 21, 2023	The PDF 417 has been modified and is now using the AAMVA format. Corrections made from the version of September 15
December 18, 2023	PDF 417 modified to be aligned on AAMVA standard and CAT readers
January10, 2024	Correction in Appendix D about Decimal instead of BCD for the FASC-N Change in Printed Data Object data object length which. Not signed anymore

VERSION CONTROL Continued

January 30, 2024	Modification on Page 23, section 4.5 (last sentence) as well as on Page 59 Appendix F (last sentence of the page) regarding the Get Data command response when a Data Object in the TWIC Card application has never been Initialized (e.g. e-stickers)
February 20, 2024	Correction in Appendix D (UUID) of the constant value of the UUID Space Name. The Full value of the Hash was correct, but not the value of the first 60 bits listed after.
March 19, 2024	Correction in section 4.7.3 about the NIST standard SP 800-76-1 changed to SP 800-76 to make sure the latest version is always considered.
March 26, 2024	Correction about an incomplete reference in Page 50
May 6, 2024	Added information about un-initialized ISO data objects in the TWIC Card application where a Get Data returns the TAG followed by 0x00 (e.g. page 60)

List of acronyms and abbreviations used in this document.

AAMVA	American Association of Motor Vehicle Administrators
AES	Advanced Encryption Standard
AID	Application Identifier
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
CBEFF	Common Biometric Exchange Formats Framework
CCL	Canceled Card List of FASC-N (formerly known as the Hotlist)
CHUID	Card Holder Unique Identifier
CIN	Card Identification Number
CIV	Commercial Identity Verification
CRL	Certificate Revocation List
ECB	Electronic Codebook mode (used for block cipher)
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard (NIST)
GUID	Global Unique IDentifier
IBIA	International Biometric + Identity Association
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
INCITS	InterNational Committee for Information Technology Standards
ISO/IEC	International Standards Organization/ International Electrotechnical Commission
MARSEC	Maritime Security
NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
OID	Object IDentifier
PACS	Physical Access Control System
PDF417	Portable Data File 417 (barcode format)
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PIX	Proprietary Identifier Extension
RFC	Request for Comments (standards from IETF)
RID	Registered application provider Identifier
RSA	Rivest–Shamir–Adleman Algorithm
SHA	Secure Hash Algorithm
SIA	Security Industry Association
SP 8xx	Special Publication (NIST)
STA	Secure Technology Alliance
TIG-SCEPACS	Technical Implementation Guidance/ Smart Card Enabled Physical Access Control Systems

TLV	Tag-Length-Value
TPK	TWIC Privacy Key
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Credential
UUID	Universal Unique Identifier
VCCL	Visual Canceled Card List of CIN

Other abbreviations may be used in this document but are then defined (or spelled out) when first used.

List of web sites allowing to access most information and reference documents mentioned in this document

AAMVA	https://www.aamva.org/technology/technology-standards
ANSI/INCITS	http://www.incits.org/standards-information/
GlobalPlatform	https://globalplatform.org/
IBIA	https://www.ibia.org/
IETF – RFC	https://www.ietf.org/standards/rfcs/
ISO/IEC JTC1 SC27	https://www.iso.org/committee/45306.html
ISO/IEC JTC1	https://www.iso.org/standards-catalogue/browse-by-tc.html
NIST – FIPS	https://csrc.nist.gov/publications/fips
NIST – SP xxx	https://csrc.nist.gov/publications/sp
SIA	https://www.securityindustry.org/
STA	https://www.securetechalliance.org/
TSA – TWIC	https://www.tsa.gov/for-industry/twic

Note: In this document, some words appear written in all capital letters. This is not a typing error as such words are either acronyms, abbreviations, or elements to which is attached a specific meaning or behavior such as the various card commands available for a reader to communicate with the card.

Table of contents

1. Overview

1.1 Abstract

The Transportation Worker Identification Credential (TWIC®[1]) specification consists of five parts which are all linked.

This **second part** describes in detail the TWIC Card Specification, the application data model, the card behavior at the card edge as well as the various mode of operations allowed by such a card.

This document describes the card after it is personalized, activated and loaded with the cardholder information. The personalization and activation of the card is not covered by any document in this series as it may be done differently depending on the specific card manufacturer; this personalization process is under the direct control of the TWIC issuance-management system.

The TWIC card has always had two distinct card applications loaded in the same card: the Personal Identity verification (PIV) Data Model card application and the TWIC card application; each with their own unique Application Identifier.

This document describes two different types of TWIC cards: **Legacy TWIC**[2] cards which are deployed in the field now (these cards have a validity period of up to five years after they have been issued), as well as the new **NEXGEN TWIC** cards with an improved data model, including new features and enhanced modes of operations (which will also be issued for a validity period of up to five years). At this point in time, the date for issuing NEXGEN TWIC cards with this improved data model is not defined.

This part does not address any of the requirements for a NEXGEN TWIC card to be activated into a PIV Interoperable (PIV-I) compatible card. This technical possibility, available only in NEXGEN TWIC cards, will be presented in a future fifth part when the TWIC issuance/management system will be able to accommodate such an activation process. The NEXGEN TWIC card has been built to allow this possibility from a technical standpoint but does not plan to use this feature soon as this would break the NEXGEN backward compatibility when used in TWIC Legacy readers.

The TWIC specification was initially developed in 2007 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 (Now Secure Technology Alliance)[3]. The original specification developed by the NMSAC TWIC Working Group has been modified to accommodate TSA security and privacy requirements.

[1] TWIC® is registered in the U.S. Patent and Trademark Office by the U.S. Department of Homeland Security.

[2] The term “Legacy Cards” in this document applies to all cards which have been created before the NEXGEN card data model application specification, created either on the Legacy TWIC system (before July 2014) or the Technology Infrastructure Modernization (TIM) System (After July 2014). The printed security features of such cards have varied over the years (e.g. recently in 2018) but the application data model has not changed.

[3] Smart Card Alliance has changed its name into Secure Technology Alliance [STA] (https://www.securetechalliance.org/)

1.2 Scope and Purpose

This Part 2 is one of the parts of the series of documents related to the TWIC Specification:

- **Part 1** – General description of TWIC credential in use by the maritime industry
- **Part 2 – TWIC card application data model, TWIC card application and card edge behavior during normal operation**
- **Part 3** – TWIC reader requirements
- **Part 4** – TWIC registration and TWIC card use by a PACS
- **Part 5** – (future) TWIC activation as a PIV-I compatible credential[4].

The mission of the TWIC program is to provide a means of positively verifying the identity of those seeking access to secure areas, to conduct security threat assessments, enabling maritime vessel and facility operators to make informed access control decisions.[5]In its development, TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document. These specifications enable varying levels of control in support of threat level risk mitigation plans.

All comments, suggestions or additional change requests should be directed to the TWIC Specification Project Editor at, TWIC-Technology@tsa.dhs.gov

It is important to take into consideration the two different types of TWIC cards described in these specifications. As cards are issued for a period of up to five years, the new version of a TWIC card described in this specification (called NEXGEN TWIC), will gradually replace the millions of cards issued prior to this new TWIC card specification being adopted by TSA as the standard for issuance. In any case, because TWIC cards are issued for a validity period of five years, TWIC readers are required to work with the prior version of the TWIC card for at least five years after NEXGEN TWIC cards will begin to be issued to TWIC cardholders.

The two types of cards are called in this series of documents "**Legacy TWIC**" and "**NEXGEN TWIC**", respectively. In July 2018, TSA began issuing a new TWIC card with updated topographical features. In conjunction with this update, TSA did not change the TWIC data model. Within this document, the term NEXGEN references the proposed new TWIC data model as well as modified back topography of the NEXGEN TWIC card. The term **NEXGEN** used in this document should not be confused with the similarly titles **NexGen** used for the 2018 physical card design[6].

[4] This last part is to be created in the future as it requires some modification in the TWIC Issuance system as well as new PIV-I activation stations.

[5] https://www.dhs.gov/news/2012/06/27/uscg-and-plcy-written-testimony-house-committee-transportation-and-infrastructure

[6] See TWIC® NexGen card FAQ on the TSA web site: https://www.tsa.gov/for-industry/twic

Important terminology: In the four parts of this NEXGEN specification, in order to avoid any confusion with a PIV card and a "PIV-like" (PIV-I or CIV) application in TWIC cards, the following words will be used:

- **PIV Data Model** means the information in the card application is compliant with the various National Institute of Standards and Technology (NIST) documents describing the format of the data and structures to be stored in a "PIV-like" card. These documents are: NIST SP 800-73, SP 800-76, and SP 800-78[7]. The PIV card itself is in addition compliant with the NIST document SP 800-79 which defines the Federal trust model (Federal Bridge used by PIV and PIV-I) which the TWIC card does not use, as it complies with a simpler, more traditional trust model also adopted by e-Passports (described in the International Civil Aviation Organization - ICAO 9303 documentation).

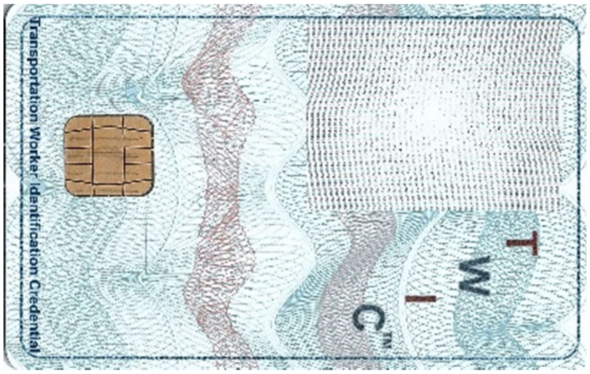
[7] See list of normative references in section 2.1 for details.

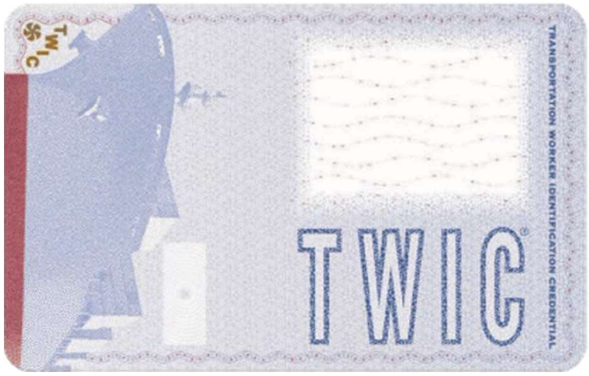
1.3 Summary of Changes from the previous Specification

The list of differences between Legacy TWIC cards and NEXGEN TWIC Cards can be found in Part 1 (General description of TWIC credential in use by the maritime industry) of this series of documents.

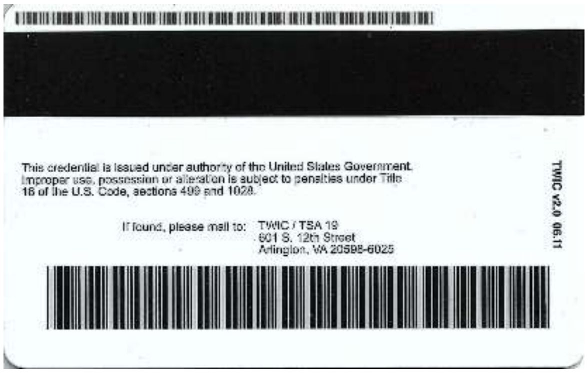
1.4 Visual Identification of TWIC Cards Versions

This section provides a brief description of the card aspect, allowing to determine which security features and which data model is in the card.





Front Before 2018 Legacy TWIC cards data model[8] – Front Since 2018

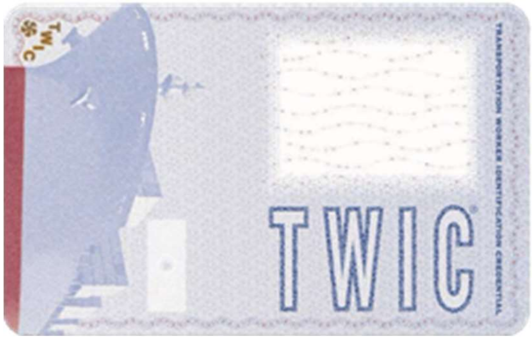


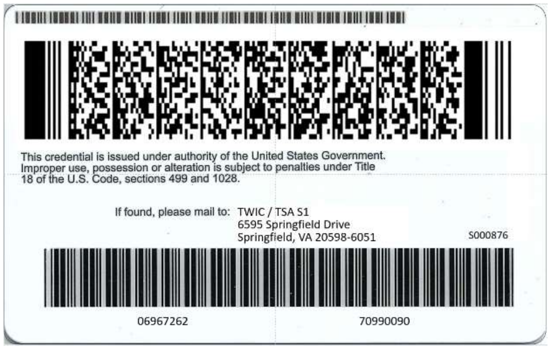
This credential is issued under authority of the United States Government.
Improper use, possession or alteration is subject to penalties under Title
18 of the U.S. Code, sections 499 and 1028.

If found, please mail to: TWIC / TSA 19
601 S. 12th Street
Arlington, VA 20598-6025

TWIC v2.0 06.11

Legacy TWIC Cards (Back)





This credential is issued under authority of the United States Government.
Improper use, possession or alteration is subject to penalties under Title
18 of the U.S. Code, sections 499 and 1028.

If found, please mail to: TWIC / TSA S1
6595 Springfield Drive
Springfield, VA 20598-6051

S000876

06967262 70990090

Front Back

NEXGEN TWIC Cards (New data Model and no Magnetic Stripe)

[8] Details of card printed security features are described elsewhere. Public information on security features can be requested by sending correspondence to the following e-mail address: TWIC-Technology@TSA.DHS.GOV

2. References

2.1 Normative References[9]

[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 800-76-2, Biometric Data Specification for Personal Identity Verification, July 2013

[R6] NIST Special Publication 800-73 Revision 4, Interfaces for Personal Identity Verification, April 2016

[R7] NIST Special Publication 800-78-4, Cryptographic Algorithms and Key Sizes for PIV, May 2015

[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 186-4, 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] AAMVA-2020-DLID-Card-Design-Standard

2.2 Informative References

[R16] FIPS Publication 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (August 2015)

[R17] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)

[R18] ICAO 9303 Machine Readable Travel Documents

[R19] 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)

[R20] TSA Guidance Package – Biometrics for Airport Access Control (30 September 2005)

[R21] OSDP v2.1.7 from SIA - Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.

[R22] Comparison between PIV, PIV-I and CIV from the Secure Technology Alliance. https://www.securetechalliance.org/resources/pdf/PIV_PIV-I_CIV_brief_022212.pdf

[9] The references of this section apply to the TWIC cards (Legacy and NEXGEN). For a complete list of references related to TWIC (cards and readers), please refer to Part 1 of this series of documents.

3. Definitions

3.1 Conformance Levels

- **expected:** A key word used to describe the behavior of the hardware or software in the design models *presumed* by this set of specification. Other hardware and software design models may also be implemented.
- **informative**: Portion of the document that explains the documentation or provides guidance on the use of the specification.
- **may:** A key word indicating flexibility of choice with *no implied preference*.
- **normative:** Portion of the document that details the requirements of the specification.
- **shall:** A key word indicating a mandatory requirement. Designers are *required* to implement all such mandatory requirements.
- **should:** A key word indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase *is recommended*.

Note: This document (Part 2) is not a document against which the TWIC card will be tested. It describes how the card **is working** and does not use always the term "shall" for the card in most instances. Nevertheless, the term "shall" is used when required for the TWIC reader and the Software client.

3.2 Glossary of terms

- **Canceled Card List (CCL**): Published daily by the Technology Infrastructure Modernization (TIM) System, this list contains all the TWIC card Federal Agency Smartcard Number (FASC-N) numbers which have been canceled. Cards which have expired are not on this list[10].
- **Card Application:** An application identified by its Application Identifier (AID) loaded (or present) into a smart card, as defined by ISO/IEC 7816-4[11]
- **Card Verification Device:** This term is used in this series of documents to indicate a device which does not interact with the chip of the TWIC card but may provide information[12] related to a given TWIC card. Such a device may use the Card Identification Number (CIN) of the card (printed on the back of the card), or verify some printed security features of the TWIC card (micro-printing, UV printing, etc.).
- **Cardholder:** The person presenting the TWIC card to an operator (or device) and claiming it is their own.
- **CIV -**Commercial Identity Verification – Card defined by the Secure Technology Alliance which uses the NIST SP 800-73 data Model but does not comply with the SP 800-79 trust model.
- **Federal Agency Smart Credential Number (FASC-N):** Static credential number used by many Physical Access Control System (PACS) to identify the credential registered to the cardholder.

[10] The TWIC CCL can be downloaded from https://universalenroll.dhs.gov/ccl/CCL.CSV

[11] A TWIC Card contains two independent applications (PIV & TWIC).

[12] The Card number found in the linear bar code on the back consists of the card IIN (most often 70990000) followed by the Card CIN (8 digits) printed on the left side under the linear bar code.

- **Key Algorithm Identifier:** Keys are identified by a one byte Tag, and is followed by a one byte Algorithm identifier. Example 9B0C is a TWIC Administrative Key used with an AES 256 bit algorithm. (See Appendix H – Key Identifiers and Key supported Algorithms)
- **Legacy TWIC:** TWIC Cards conforming to the 2012 TWIC Reader and Card Application Specification in terms of data model.
- **Legitimate Cardholder**: A person who was successfully vetted under a security threat assessment by the TSA, was issued a TWIC card and whose personal and biometric information are printed on (and loaded in) the TWIC card.
- **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.
- **NEXGEN TWIC:** TWIC cards conform to this new TWIC card data model specification.
- **Operator/Guard:** A person responsible for verifying the validity of a TWIC card, and/or the cardholder presenting the card.
- **PIV Data Model Card Application:** The card application present in a TWIC Card, conformant to the NIST SP 800-73, SP 800-76 and SP 800-78 specification.
- **TWIC Card Application:** The card application present in a TWIC Card, working as described in the TWIC Card specification.
- **TWIC Card:** A smart card that corresponds to the specifications laid out for the Transportation Workers Identity Credential (TWIC) Program.
- **TWIC Privacy Key:** A 128-bit AES symmetric key value used to encipher the personal user information, including the biometric templates, which are stored on the TWIC card.
- **TWIC Reader:** This term is used in this section to indicate a card reader, used alone, or as part of a more sophisticated system (e.g. a PACS) to interact with the chip of a TWIC card. This section does not make any difference between information processed in the reader itself, or in other parts of the system to which it is attached (e.g. a control panel, Certificate Validation System or a PACS back-end).
- **Visual CCL (VCCL):** Published daily by the Technology Infrastructure Modernization (TIM) System, this list contains all the Card Identification Numbers (CINs) which have been canceled. Cards which have expired are removed from this list on a daily basis.

3.3 Definitions of important words used in all four parts of the NEXGEN documents/specifications:

3.3.1 Identifiers vs Authenticators

Identifiers are unique numbers attributed by an authority to identify a specific person, object, or a case. An Identifier is not protected and is publicly visible to anybody. An identifier is not a secret. In the TWIC card, there are two identifiers of interest:

- One is the printed card identifier known as the **Card Identification Number (CIN)** located on the back of the TWIC card on the lower left side below the one-dimensional barcode.

- The second identifier is the **Federal Agency Smart Credential Number (FASC-N)** created by the TSA-TWIC issuance system and accessible electronically form the chip in the card which identifies the logical credential issued to a given user. FASC-N information is now also available in the NEXGEN UUID (value present in the GUID of the CHUID and the Card UUID). See Appendix D.

Identifiers may be digitally signed providing trust in that the identifier indeed is issued by a trusted authority and is not altered or forged.

Identifiers should be considered public information as they are displayed/exchanged in clear text and should never be used as authenticators. Identifiers can be quite easily copied and spoofed by attackers.

Authenticators always need to be protected and kept secret as much as possible. There are three types of authenticators in TWIC Cards:

- PIN (Password): Securely stored in, and verified by the card. The PIV PIN is known only by the TWIC card holder. This is considered a "Something you Know" Authentication Factor. Note: The TWIC card application does not have a PIN.
- Secret/Private Keys (using algorithms and allowing a system to execute a challenge response verifying the authenticity of the card). This is considered a "Something you Have" Factor of Authentication.
- Biometric reference information (e.g. fingerprints, face, etc.) that is securely stored in the TWIC card allows the system to verify that the person presenting the card is indeed the same person to whom the card was issued. This is a "Something you are" Authentication Factor.

Authenticators should be (very) hard to copy or modify. They are often uniquely attached to a specific identifier.

3.3.2 Verification vs. Authentication

Verification: Process by which a person, or a device is able to compare information providing a level of assurance. The verification process involves identifiers (public information available on the TWIC card or in the TWIC card) to identify the correct TWIC record and may eventually use authenticators (e.g. PIN or Biometrics). In such cases, the process needs to protect the secret authentication information used. The verification process may also consist of verifying an identifier is not backlisted (e.g. TWIC canceled card list). Most of the time, the term verification is used when a human process is involved.

Authentication: Process by which a level of assurance of a verification is enhanced by involving an authenticator, making sure the process cannot be compromised. An authenticator (secret) is always involved in such a process, even if the verification process uses only public information (e.g. Verification of Digital Signature). Authentication generally involves a secure electronic device such as a smart card to protect secret authentication information. This enables trust in the authentication result.

3.3.3 Credential vs. Card

Credential: An identifier attached to an individual to whom is assigned some authorization or privilege. In TWIC, the FASC-N as well as the Card Identification Number (CIN) are linked to an individual only after the background checks have been successfully completed. A credential is only an identifier but is often printed or loaded in a physical device such as a TWIC card which carries it. In TWIC cards, these identifiers are digitally signed, allowing to verify it was assigned by a trusted authority.

Card: Physical object on (and in) which can be found the information (identifiers) related to the credential it represents. In the case of the TWIC card, the CIN can be found printed on the card, and the FASC-N (another identifier) is found in the electronic chip of the card.

3.3.4 Summary of Changes to the previous specification

TWIC legacy cards use the SHA-1 hash algorithm as indicated in the TSA TWIC 2012 clarified specification. As of 2015, NIST phased out the SHA-1 algorithm for increased security reasons. TWIC Legacy cards may be issued in the future, prior to inception of issuance of TWIC NEXGEN cards, the hash function SHA-256 instead of the SHA-1dependent on TSA decisions. All TWIC NEXGEN cards use the SHA-256 for the hash algorithm.

3.3.5 Note from NIST about SHA-1

NIST's Policy on Hash Functions - August 5, 2015

SHA-1: Federal agencies **should** stop using SHA-1 for generating digital signatures, generating time stamps and for other applications that require collision resistance. Federal agencies may use SHA-1 for the following applications: verifying old digital signatures and time stamps, generating and verifying hash-based message authentication codes (HMACs), key derivation functions (KDFs), and random bit/number generation. Further guidance on the use of SHA-1 is provided in SP 800-131A.

3.3.6 Information about response to Get Data requests on Data Objects

In the TWIC NEXGEN card data model some Data Objects are present but may be not initialized or not populated. Depending on the type of behavior of the Data Object (either PIV or ISO), the results of the information returned by the Get Data command may be different:

- For empty or not initialized PIV data objects, a Get Data command would return a value of 0x53 00
- For not initialized ISO data objects, a Get Data command would return a value of 0xTAG 00.
- For empty ISO Data Objects with a constructed ASN.1 tag, a Get Data command would return a value of 0xTAG 02 80 00

3.3.7 Important Notice about this version of the document

The content and format of the PDF 417 on the back of the TWIC has been changed to comply with the AAMVA standard instead of the Simpler ASN.1 structure which was used in earlier versions of this specification. See Section 4.9.

4. TWIC Card Application

History of TWIC cards versions:

- The initial TWIC cards were identified as version 1.0. These cards have all expired and should no longer be in use. As such, they are mentioned in this document for historical reasons only.
- The TWIC Legacy cards conforming to the May 2012 TWIC card and reader specification are identified as version 2.0 (data model 01 01). This version of TWIC card remains in circulation at the time of publication of this document. All TWIC readers shall support such a card version.[13]
- The new NEXGEN TWIC card described in this document is identified as version 3.0 (data model 01 03) and identified visually by a two-dimensional bar code (PDF 417) on the back.

The card data model is provided as part of the card Application Identifier (AID) in the last two bytes. As only the last byte (minor version indicator) has changed over the years, it indicates all these versions are upward compatible with the previous version, thereby allowing a TWIC reader developed for the TWIC Legacy card Data Model (01 01) to work with cards using a newer data model (01 03) (See Appendix C for details).

Note: The card version printed on the back of the card does not represent the data model and may change when the physical aspects of the card change (e.g. security features of card topology). As such, the printed card version may be different from the card data model (see below its coding in the card AID). Accordingly, the card may change version but retain the same data model or change its data model but keep the same card topology.

4.1 TWIC Card Application IDentifiers (AIDs)

The TWIC card contains two different card applications**.** One is aligned with the PIV Data Model specification (NIST SP 800-73, SP 800-76 and SP 800-78 series) and is identified in this series of documents as "PIV Data Model Card Application". The other card application is the "TWIC Card Application" described in detail in this document. Both card applications are described in the following sections.

As all AIDs are defined by ISO/IEC[14] 7816-4, the TWIC card applications consists of an RID (Registered Identifier for a card issuer) and a PIX (Proprietary Identifier Extension specific to the application).

Application	RID	PIX (left four bytes to be used when selecting the AID)	
PIV	A0 00 00 03 08	00 00 10 00 01 00	
TWIC	A0 00 00 03 67 See Appendix C.1	20 00 00 01 yx xx yx xx is the card data model See Appendix C.2	y = 0 indicates live cards. Other values are reserved for future use x xx = 0 00 used in V 1.0 cards[15] x xx = 1 01 used in V 2.0 cards x xx = 1 03 used in NEXGEN

Note: TWIC readers shall explicitly select the PIV or the TWIC card application depending on which application it needs to use as neither of these may be the default selected card application in the card. See details about the AID structure and the Selection function in Appendix C .

[13] This card version is indicated as data model 01 01 in the card Application Identifier (AID).

[14] ISO/IEC - International Standards Organization/ International Electrotechnical Commission

[15] There are no more such cards in circulation today.

4.2 PIV Data Model Card Application in TWIC Cards (after card activation)

The information provided in this section is not detailed since the PIV Data Model card application loaded in a TWIC Card is based on the normative NIST SP 800-73 document. For information about the details of these data objects, refer to NIST SP 800-73, SP 800-76 and SP 800-78 series. Any difference with the SP 800-73 series of documents is indicated in this section.

Optional features of SP 800-73-4 that are not implemented in the PIV Data Model card application of TWIC cards are:

- The Virtual Card Interface (VCI)
  - No Secure Messaging Certificate Signer
  - No Pairing code or its container
- Key History objects and Retired certificates
- On Card Comparison (OCC)

Differences between Legacy TWIC and NEXGEN TWIC cards in the PIV Data Model Card Application include the following (Universal Unique Identifier [UUID] and Secure Hash Algorithm)**:**

- UUID: has a null value in the Global Unique Identifier (GUID) of Legacy TWIC Cards. The Card UUID is fully populated in NEXGEN TWIC cards (see Appendix D for details)
- SHA (Secure Hash Algorithm): SHA-1 predominantly is used in Legacy TWIC Cards
  SHA-256 is used in all NEXGEN TWIC cards

PIV Card Application in TWIC cards AID = A0 00 00 03 08 00 00 10 00 01 00 Data Object name	**Container ID**	**TLV DO Tag**	**Get Data ISO or PIV (2)**	**Access Rule for Contact**	**Access rule for Contactless**	**Legacy**	**NEXGEN**
X.509 Certificate for Card Authentication	0x0500	5FC101	PIV	Always	Never	Y	Y
Cardholder Unique Identifier (CHUID)	0x3000	5FC102	PIV	Always	Never	Y	Y
Cardholder non-enciphered minutia templates	0x6010	5FC103	PIV	PIN	Never	Y	Y
X.509 Certificate for PIV Authentication	0x0101	5FC105	PIV	Always	Never	Y	Y
Security Data Object	0x9000	5FC106	PIV	Always	Never	Y	Y
Card Capability Container	0xDB00	5FC107	PIV	Always	Never	Y	Y
Cardholder Facial Image (clear text)	0x6030	5FC108	PIV	PIN	Never	Y	Y
Printed Information (clear text not signed)	0x3001	5FC109	PIV	PIN	Never	Y	Y
X.509 Certificate for Digital Signature	0x0100	5FC10A	PIV	Always	Never	Y	N
X.509 Certificate for Key Management	0x0102	5FC10B	PIV	Always	Never	Y	N
Cardholder Iris Image Template (clear text)	0x1015	5FC121	PIV	PIN	Never	N	O
Discovery Object	0x6050	7E	ISO	Always	Always	N	Y
PIN (Personal Identification Number)	N/A (1)	80	N/A	Never	Never	Y	Y
PUK (PIN Unblocking Key) – For PIN reset	N/A (1)	81	N/A	Never	Never	Y	Y
PIV-Authentication Private Key (RSA 2048)	N/A (1)	9A07	N/A	Never	Never	Y	Y
PIV Administrative Management Key	N/A (1)	9B0C	N/A	Never	Never	Y	Y
Digital Signature Key (RSA 2048)	N/A (1)	9C07	N/A	Never	Never	Y	N
Key Management Key (RSA 2048)	N/A (1)	9D07	N/A	Never	Never	Y	N
Card Authentication Private Key (RSA 2048)	N/A (1)	9E07	N/A	Never	Never	Y	Y

(1) These data objects are mentioned for completeness, but as indicated in SP 800-73, they can be referenced (using the Tag-Length-Value [TLV] tag) in some commands (e.g. GENERAL AUTHENTICATE), but cannot be read (or updated) on any interface.

(2) The column “Get Data ISO or PIV” indicates if the Get Data issued on such a Data Object will return the tag 0x53 (PIV/SP 800-73 behavior) or the tag specified in the command of the Get Response (ISO behavior) to identify the TLV data object returned.

(3) The Cells colored in gray indicate a difference between the two data models.

(4) The letter O indicates an optional presence of the data object in NEXGEN TWIC cards. For such objects, when not populated, the tag is present with a data length of zero. A Get Data on such an empty Data Object would return 0x53 00 (PIV behavior).

(5) The Optional data field CardHolder UUID defined by NIST in SP 800-73-4 is not used in NEXGEN TWIC cards.

In the NEXGEN TWIC data model (V 1.3), two certificates are recommended to no longer be populated in the PIV Data Model card application. These certificates (Digital Signature and Key Management) are required under Federal Information Processing Standard (FIPS) 201 when the participant has a government e-mail address at the time of card issuance. As TWIC Cards are not for Federal Employees or contractors, TWIC participants do not have (by a large majority) such an e-mail address. Accordingly, the two private keys and their corresponding public key certificates are not required in the new data model.

Because of the many optional functions introduced in recent versions of SP 800-73 specifications, the discovery object (which determines the options used by the card) and the Card Holder Iris (on contact mode only) may become available in some TWIC cards (variable with the card manufacturer) but will not be populated by default in NEXGEN TWIC cards.

TSA TWIC being a Federal Issuer of TWIC, for Legacy TWIC cards as well as for the NEXGEN TWIC card, will continue to use the FASC-N as the Unique Card Identifier for TWIC card applications. As such, the FASC-N will be populated with the usual TWIC structure defined in 2007 by TSA TWIC and as described in the May 2012 TWIC Reader Hardware and Card Application Specification.

In NEXGEN TWIC cards, the Card Universally Unique Identifier (Card UUID) is now populated using the "mode 5" structure of RFC 4122[16] allowed by SP 800-73 specification, and this structure allows the value of the FASC-N to be extracted as part of the data structure (see "Appendix D - Structure of the Card UUID in TWIC cards for more information).

TWIC Legacy as well as NEXGEN TWIC card uses the PIV card application PIN to protect access to some cardholder data objects of the PIV Card application. The Discovery Object is now added in the NEXGEN TWIC card data structure to indicate this option (SP 800-73 Part 1 section 3.3.2):
Value of the PIV Card Application Discovery Object:

Discovery Data Object Tag:	0x7E	
Length of the data object:	0x12	
PIV Card AID Tag:	0x4F	{'4F 0B A0 00 00 03 08 00 00 10 00 01 00'}
PIN Usage Policy Tag:	0x5F2F	{'5F2F 02 40 00'[17]}

Note: Refer to NIST SP 800-73-4, SP 800-76 and SP 800-78 for the details of the content and the construction of the PIV data objects used in TWIC cards.

4.2.1 TWIC Cards and PIV-I Compatibility

It is possible that in the future NEXGEN TWIC cards could become PIV-I compatible. Beside important modifications in the issuance and activation support system, this would also require modifications to some of the data structures of the PIV Card Application data model (for example, the 14-digit FASC-N identifier shall be all nines: 9999-9999-999999 to be a PIV-I compliant Card). This will be addressed in a future Part 5 (PIV-I NEXEN TWIC card Activation) of this series of documents. At this point in time, in order to allow for backward compatibility with existing TWIC readers, all NEXGEN TWIC cards are issued as indicated in this document but could technically be PIV-I activated in the field if required.

This PIV-I activation of a NEXGEN TWIC card would impact only the PIV Data Model card application (and its data objects) of the TWIC card. It would not change anything in the TWIC card application of the same card.

[16] This Request for Comments (RFC) standard from IETF can be found at https://tools.ietf.org/html/rfc4122
[17] Important to notice: this value in the TWIC discovery object is different as the TWIC card application does not have an application PIN avauilable.

4.3 TWIC Card Application Data Model

Comparing Legacy TWIC and NEXGEN TWIC card application data models, the following changes are identified:

- Card UUID: has a null value of zeroes in Legacy TWIC Cards (called the GUID)
  Fully populated in NEXGEN TWIC cards (see Appendix D for details)
- SHA (Secure Hash Algorithm): SHA-1 predominantly is used in Legacy TWIC cards
  SHA-256 is used in NEXGEN TWIC cards
- New Objects are added and available in a NEXGEN TWIC card data model:

TWIC X.509 Certificate for Card Authentication	tag 0x5FC101
Discovery Object	tag 0x7E
Printed Card Information	tag 0xDFC109
Cardholder Facial Image	tag 0xDFC108
Cardholder Iris Image (optional)	tag 0xDFC121
Cardholder Personal Information	tag 0xDFC001
Cardholder Handwritten Signature (Optional)	tag 0xDFC002
Free Read/Write E-Stickers (Ten data objects)	tags 0xE1 to 0xEA
TSA Controlled E-Stickers (Four Data Objects)	tags 0xFA to 0xFD

4.4 Key Reference(s) in the TWIC Card Application[18]

TWIC uses two different types of cryptographic keys in its data model.

4.4.1 TWIC Privacy Key (TPK)

Available in both Legacy TWIC Cards and NEXGEN TWIC cards, the TWIC privacy Key (TPK) is an AES 128 symmetric static key, unique to each individual TWIC card. The TPK is used to protect the user's privacy when certain information is exchanged between the card and the TWIC reader; especially over the contactless interface. This TPK value is available from the card itself over the contact interface, or on the back of the card (magnetic stripe for Legacy TWIC cards or the PDF417[19] bar code for NEXGEN TWIC cards)[20].

The NIST document SP 800-78 defines the various algorithm identifiers used for keys. The TPK key has an algorithm identifier of 0x08 indicating this key is to be used with an AES algorithm in Electronic Codebook (ECB) mode.

Notes:

1. The TPK is not used by the TWIC card application for any internal cryptographic function. The TPK is used only by the client application to encipher (for storage in the card) or decipher (for use in a TWIC reader) the user's private information (e.g. reference biometric template).
2. The Algorithm Identifier is a field (tag 0xC1) found in the TWIC Privacy Key Container.

[18] For key reference in the PIV Card application, refer to NIST document SP 800-73

[19] PDF 417 - Portable Data File 417 (two dimensional [2D] barcode format)

[20] It must be noted the existing linear bar code (1D) containing the Card Identification Number is unchanged from the previous design (see image of the back of the card in Section 1.4 page 9, right bottom image).

4.4.2 TWIC Card Authentication Key (NEXGEN only)

A new asymmetric key (Private/Public key) has been added to the NEXGEN TWIC data model allowing the TWIC card application to perform active card authentication without requiring a reader to select and subsequently use the PIV data model card to perform card authentication.

It is similar in structure and in usage to the PIV card Authentication Key.

Notes:

- During the personalization process of the card, the Card Authentication Key is generated outside of the card for all Transportation Workers cards; and the key as well as the related certificate values of the PIV Card Authentication key are copied from the PIV card Application to the TWIC card Application. This means that they also share the same Certificate Revocation List (CRL). This is different for Trusted Agent Cards wherein the Card Authentication Keys are generated in the card at the time of activation, resulting in a different key (and a different certificate) for each the PIV Data Model and the TWIC Card Authentication values.
- NIST SP-800-78 allows the Card Authentication Key to be generated outside of the card. Trust in such a private key relies on the trust of the card personalization system, which in the case of TWIC is centralized (Government Printing Office – GPO) and involves digital signatures of all data objects on the TWIC card. It must be understood this off card key generation is not allowed by NIST for the PIV Authentication key (which requires the PIN presentation and exists only in the PIV Card application of the TWIC Card). This is why TWIC cards should not be used as an online token if the NIST level of trust is required (e.g. PIV-I/CIV).

Warning: Using the PIV Authentication Certificate private key (which requires a PIN presentation) in a TWIC card may technically work, but as the PIV User authentication private key is not generated in the TWIC card (it is loaded in the card during personalization), this mode would not be consistent with the security/trust requirements of NIST SP 800-78 and as such is not recommended except for use with Trusted Agent cards.

4.5 TWIC Card Application Data Models

TWIC Card Application Legacy = A0 00 00 03 67 20 00 00 01 01 01 NEXGEN = A0 00 00 03 67 20 00 00 01 01 03 Data Object Name	Container ID	TLV DO Tag	Get Data ISO or PIV (4)	Access Rule for Contact	Access rule for Contactless	Legacy	NEXGEN
X.509 Certificate for Card Authentication	0x0500	5FC101	PIV	Always	Always	N	Y
Cardholder Unique Identifier (CHUID)	0x3000	5FC102	PIV	Always	Always	Y	Y
Unsigned Cardholder Unique Identifier	0x3002	5FC104	PIV	Always	Always	Y	Y
Discovery Data Object	0x6050	7E	ISO	Always	Always	N	Y
TWIC Administrative Key (1)	N/A	9B0C	N/A	Never	Never	Y	Y
Card Authentication Private Key (RSA 2048)	N/A (1)	9E07	N/A	Never	Never	N	Y
Cardholder Personal Information (TPK encrypted)	0x6011	DFC001	PIV	Always	Always	N	O
Cardholder handwritten signature (TPK encrypted)	0x6012	DFC002	PIV	Always	Always	N	O
TWIC Privacy Key (TPK) container	0x2001	DFC101	PIV	Always	Never	Y	Y
Cardholder Fingerprints (TPK encrypted)	0x2003	DFC103	PIV	Always	Always	Y	Y
Cardholder Facial Image (TPK Encrypted)	0x6030	DFC108	PIV	Always	Always	N	Y
Printed Information (TPK encrypted)	0x3001	DFC109	PIV	Always	Always	N	Y
Security Data Object	0x9000	DFC10F	PIV	Always	Always	Y	Y
Cardholder Iris Image (TPK encrypted)	0x1015	DFC121	PIV	Always	Always	N	O
E-Stickers # 1 to 10 (free read & write) (3)	N/A	E1 to EA	ISO	Always	Always	N	O
TSA controlled E-Stickers (Issuer write controlled)	N/A	FA to FD	ISO	Always	Always	N	O

1) This Card Data Object can be referenced and used to manage the card application but cannot be read on any interface.
2) The cells colored in gray in the above table indicate the differences between Legacy TWIC and NEXGEN TWIC cards.
3) These data objects are free read (using a GET DATA Command) and write (using a PUT DATA command) and meant to be used as scratch pad (temporary memory) areas by relying party systems using the NEXGEN TWIC card. The NEXGEN TWIC card does not interpret, protect or manage these E-Stickers; the NEXGEN TWIC card simply allows reading and writing in these dedicated memory areas. They are unmanaged storage. See Appendix F (and Part 4) for more details.
4) The column “Get Data ISO or PIV” indicates if the Get Data issued on such a Data Object will return the tag 0x53 (PIV/SP 800-73 behavior) or the tag specified (ISO/IEC 7816-4 behavior) in the GET RESPONSE.

Note: Optional data objects (indicated in the last column of the table by the letter “O”) are always present in NEXGEN cards, and as such can be selected/read, but when the Data Object has never been initialized, the Get Data Command could respond with:

- no tag and no length (just a return code of 0x9000) ,
- or the tag followed by 00 (length) for ISO data objects, or 0x53 00 for PIV data Objects.

4.6 Description of the TWIC Data Model Objects (Legacy & NEXGEN)

All data objects used in the TWIC cards use a TLV (Tag-Length-Value) construction. The Tag may be a simple tag or indicate a constructed tag (containing other tags). The tag may be on one or three bytes; and the length is on one, two or three bytes.

The length bytes are not shown in the following sections but should be taken into account when the whole data object maximum size is considered for data storage.

4.6.1 Data Object - Unsigned Card Holder Unique Identifier

Unsigned Card Holder Unique Identifier		0x5FC104 (constructed data object-PIV Get Data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
FASC-N	0x30	M	Fixed Text	25
GUID (Card UUID value)	0x34	M	Fixed Numeric	16
Expiration Date	0x35	M	Date (YYYYMMDD)	8
Error Detection Code	0xFE	M	LRC	0

Note: This constructed data object value has a fixed length of 57 bytes, not counting the tag itself (0x5FC104) and its length (0x39)

4.6.2 Data Object – TWIC Privacy Key Container

TWIC Privacy Key Container		0xDFC101 (constructed data object-PIV Get data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
TWIC Privacy Key (TPK)	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. This data object being constructed, the structural information consists of two additional bytes per sub-element (simple TLV tag byte plus one byte for length). This requires a maximum total of 40 bytes for this data object value without counting the Tag itself (0xDFC101) and its attached length (0x28).

4.6.3 Data Object - Signed Card Holder Unique Identifier

Card Holder Unique Identifier		0x5FC102 (constructed data object- PIV Get Data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
FASC-N	0x30	M	Fixed Text	25
GUID (Card UUID Value)	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 data object value maximum size requires an additional 20 bytes for primitive tags and their lengths.

4.6.4 Data Object - Card Holder Enciphered Fingerprint Templates

Card Holder Fingerprints		0xDFC103 (constructed data object-PIV Get data)		
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[21] 378 standard.
2. Tag 0xBC contains the enciphered biometric template. The Common Biometric Exchange Framework Format (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 (TPK). Deciphering of the biometric template should be performed using the "no padding" option of the AES algorithm.
3. Four additional bytes of structural information are required for this data object.

4.6.5 Data Object - Security Object

Security Object		0xDFC10F (constructed data object-PIV Get data)		
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

Warning: The use of this data object may be deprecated in a future release.

Notes:

1. The security object exists in TWIC for PIV compatibility. The security object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents (MTRD) Offering ICC Read-Only Access Version 1.1. [8]. Tag "0xBA" is used to map the Data Objects in the TWIC data model to one the 16 Data Groups specified in the Machine Readable Travel Document. For **Legacy TWIC cards**, the objects hashed in the TWIC card Application are: the Unsigned CHUID (0x3002), the Signed CHUID (0x3000), and the signed fingerprint templates (0x2003). For **NEXGEN TWIC Cards**, the objects hashed are the Unsigned CHUID (0x3002), the Signed CHUID (0x3000), the signed fingerprint templates (0x2003), the signed Printed Information (0x3001), the cardholder signed facial image (0x6030), the cardholder encrypted IRIS image (0x1015), the encrypted cardholder personal information (0x6011), and the cardholder encrypted handwritten signature (0x6012). This enables the TWIC security object to be fully compliant for future activities with identity documents.
2. The card issuer's content signing key used to sign the CHUID and other objects is the same as used to sign the security object, as an attached signature in this one case, and shall be verified in the same manner. The signature field of the security object does not include the issuer's certificate since it is included in the signed CHUID. The Card Issuer's signature is in accordance with FIPS 201-1 using the SP-800-78 document as reference with the key sizes in accordance with the TWIC card life.
3. Eight additional bytes of structural information are required for this data object.

[21] INCITS - InterNational Committee for Information Technology Standards

4.7 New Data Objects added in the NEXGEN TWIC data model

4.7.1 Data Object – X509 Certificate for Card Authentication

X509 Certificate for Card Authentication		0x5FC101 (Constructed Object-PIV Get data)		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
Certificate	0x70	M	Variable	1856
Certificate Information	0x71	M	Fixed	1

This structure is similar to the PIV Certificate for Card Authentication but does not use the MSCUID.

4.7.2 Data Object – Enciphered Printed Card Information

Enciphered Printed Card Information			0xDFC109 (Constructed Object-PIV Get data)		
Data Element (TLV)	**Tag**		**M/O**	**Type**	**Max Bytes**
Information ciphered using TPK	0xBC		M	Variable	200

TLV representation of this Data Object:

```
53 LL
  BC ZZ              Data Enciphered with TPK
      01 L1 [data] - Name
      02 L2 [data] – Employee Affiliation (Empty Value)
      04 L3 [data] – Expiration Date (DDMMMYYYY)
      05 L4 [data] – Agency Card Serial Number (8 digits of the CIN)
      06 L5 [data] – Issuer & System Identifier (7099xxxx)
      07 L6 [data] – Organization Affiliation Line 1 (Empty Value)
      08 L7 [data] – Organization Affiliation Line 2 (Empty Value)
```

Notes:

- Data Element 06 concatenated with Data Element 05 is the value of the linear bar code printed on the back of the card (complete CIN)
- The signature block is not present in this data object. In the TWIC NEXGEN card, this data object is a copy of the PIV Data Object 0x5FC109 which is not signed.

4.7.3 Data Object - Card Holder Enciphered Facial Image

Card Holder Enciphered Facial Image		0xDFC108 (constructed data object-PIV Get data)		
Data Element (TLV)	**Tag**	**M/O**	**Type**	**Max Bytes**
Facial Image (TPK ciphered)	0xBC	M	Variable	16710

Notes:

1. The facial image is encoded in accordance with the NIST SP 800-76 standard.
2. Tag 0xBC contains the enciphered facial image information. The CBEFF integrity option is required per SP 800-76, 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 (TPK). Deciphering of the facial image information should be performed using the “no padding” option of the AES algorithm.
3. Four additional bytes of structural information are required for this data object.

TLV representation of this Data Object:

```
53 82 L1L2

  BC 82 L1L2    Data Enciphered with TPK

      CBEFF Header
      BDB - ANSI/INCITS 385
      CBEFF Signature Block
```

4.7.4 Data Object – Card Holder Enciphered Iris Image

Card Holder Enciphered Iris Image		0xDFC121 (constructed data object-PIV Get Data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Iris Image (TPK ciphered)	0xBC	O	Variable	7100

Notes:

1. The iris image is encoded in accordance with the NIST SP 800-76 standard.
2. Tag 0xBC contains the enciphered iris image information. The CBEFF integrity option is required per SP 800-76, 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 (TPK). Deciphering of the iris image information should be performed using the “no padding” option of the AES algorithm.
3. Four additional bytes of structural information are required for this data object.

TLV representation of this Data Object:

```
53 82 L1L2

  BC 82 L1L2    Data Enciphered with TPK

      CBEFF Header
      BDB – ISO 19794-6
      CBEFF Signature Block
```

4.7.5 Data Object – Discovery Object

Present in both card applications (PIV & TWIC), the value of this data object is different between the PIV card application (which has a PIN) and the TWIC card application (which has no PIN).

Discovery Data Object		0x7E (Constructed Data Object-ISO Get data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Discovery Data Object as described in SP 800-74	0x7E	M	Constructed data object	18

Tag 0x7E length 0x12

- Tag 0x4F (AID) length 0x0B Value 0x A0 00 00 03 67 20 00 00 01 01 03
- Tag 0x5F2F length 0x02 - see below for the value of this Data Object

In the PIV card application, the Tag 5F2F has a value of 0x04 00 indicating the use of a local PIN.
In the TWIC card application, the Tag 5F2F has a value of 0x00 00 indicating no PIN is available.

4.7.6 Data Object – Card Holder Enciphered Personal Information

Card Holder Enciphered Personal Information		0xDFC001 (Constructed Data Object-PIV Get data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Card Holder Personal Information (TPK ciphered)	0xBC	O	Variable	4096

Requirements for an Identity Document to be Real ID compliant:

- To be added in this data object:
  - Person's full legal name Tag 0x81 – up to 40 bytes
  - Person's date of birth Tag 0x82 – YYYY-MM-DD
  - Person's gender Tag 0x83 – One Byte
  - Person's address of principal residence Tag 0x84 – up to 100 bytes
- Information already available in the TWIC card data model in other data objects:
  - Person's identification card number (FASC-N is in the digital signature of data objects)
  - Person's facial image (printed on and digitally stored in the NEXGEN TWIC card)
  - Person's signature (added to some NEXGEN TWIC cards – Data object 0xDFC002)
- Elements already part of the TWIC card design:
  - Physical Security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes (all data objects are digitally signed)
  - A common machine-readable technology, with defined minimum data elements
- The Identity document must be issued with a maximum validity date not higher than the authorized legal residency period of the cardholder (in case the cardholder is not a permanent resident or a US citizen). This clause could technically be met if the card was canceled at the end of the legal residency period, but this is not done by the TWIC management system as of today.

TLV representation of this Data Object (this is an example and may not reflect the real content):

```
53 82 L1L2
  BC 82 L1L2    Data Enciphered with TPK
      81 L1 [data] – Legal Name
      82 L2 [data] – Date of Birth
      83 L3 [data] - Gender
      84 L4 [data] - Address
      3E L5 [data] – PKCS7 Signature Block
```

.

4.7.7 Data Object – Card Holder Enciphered Handwritten Signature

Card Holder Enciphered handwritten signature		0xDFC002 (constructed Data Object-PIV Get data)		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Handwritten signature (TPK ciphered)	0xBC	O	Variable	8128

Notes:

1. The handwritten signature is encoded in accordance with the NIST SP 800-76 standard.
2. Tag 0xBC contains the enciphered handwritten signature. 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 (TPK). Deciphering of the handwritten signature should be performed using the "no padding" option of the AES algorithm.
3. Four additional bytes of structural information are required for this data object.

TLV representation of this Data Object:

```
53 82 L1L2
  BC 82 L1L2    Data Enciphered with TPK
      CBEFF Header
      BDB - ISO 19794-7
      CBEFF Signature Block
```

4.7.8 Data Objects - E-Stickers (free read & write)

Free read/Write E-Stickers	0xE1 to 0xEA (Read & Write access-ISO Get data)	
	Type	Max Bytes
Objects under the control of the client application using context specific tags[22]	Private Constructed data objects – Size and content variable	Up to 3K bytes each

See Appendix F about the suggested use of such data objects.

4.7.9 Data Objects – TSA E-Stickers (free read & TSA only update)

TSA protected E-Stickers	0xFA to 0xFD (Read & Write access-ISO Get data)	
	Type	Max Bytes
Objects under the control of the card issuer using context specific tags[23]	Private Constructed data objects – Size and content variable	Up to 3K bytes each

[22] ANS.1 TLV Context Specific tags have a meaning which depends on the context defined by the main tag and/or the context within the data object itself. The Tag values are from 0x80 to 0x8E and from 0x90 to 0x9E for non-constructed tags, and values from 0xA0 to 0xAE or 0xB0 to 0xBE for constructed tags. See T-REC-X.680-200811.pdf and related publication for details. ISO 7816-6 could also be used as guidance on TLV tags used in smart cards.

[23] ANS.1 TLV Context Specific tags have a meaning which depends on the context defined by the main tag and/or the context within the data object itself. The Tag values are from 0x80 to 0x8E and from 0x90 to 0x9E for non-constructed tags, and values from 0xA0 to 0xAE or 0xB0 to 0xBE for constructed tags. See T-REC-X.680-200811.pdf and related publication for details. ISO 7816-6 could also be used as guidance on TLV tags used in smart cards.

4.8 Magnetic Stripe Data Model (Legacy TWIC Cards Only)

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 Legacy card. The TPK is encoded on the magnetic stripe as follows:

- The TPK is a 16 bytes string to be used with an AES encipherment/decipherment algorithm.
- Track 1 of the TWIC magnetic stripe is reserved exclusively for the TPK character string. The TPK character string is 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 is encoded as ASCII alphanumeric characters (0 to 9 and A to F) giving a total of 32 characters representing the 32 hexadecimal digits of the TPK.
- The TPK is 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 is coded after the end sentinel.

4.9 Two-dimensional Bar Code Data Model - PDF417 (NEXGEN cards)

The PDF417 bar code information is coded using the format defined by the AAMVA standard for Identification Documents. The TPK itself can be found in the AAMVA subfile ZTA and is identical to the same Data Object which can be read from the TWIC card contact side.

The full encoding of the PDF 417 according to the AAMVA standard is as follow:

Offset in Bytes	Data Element Name	Format of Value	Length in Bytes	AAMVA Field ID	Value/example/ format	End of Field	Comment	*
				←	Elements concatenated	→		
0	Separators	Hex	4	-	0x400A1E0D	-	Coding of: space (0x40), LF (0x0A), record separator (0x1E), CR (0x0D)	C
4	File Type	ASCII	5	-	ANSI + space	-		C
9	Issuer Identifier	ASCII	6	-	709900	-	TSA issuance of the ID	C
15	AAMVA version	ASCII	2	-	10	-		C
17	Jurisdiction number	ASCII	2	-	01	-	AAMVA uses 00 for DL	C
19	Number of subfiles	ASCII	2	-	02	-	Two Subfiles: ID and ZT	C
21	Subfile 1 designator	ASCII	2	-	ID	-	AAMVA data elements	C
23	Offset of the ID subfile	ASCII	4	-	0041	-		C
27	Length of ID subfile	ASCII	4	-	0168	-		C
31	Subfile 2 designator	ASCII	2	-	ZT	-	ZT Contains the TWIC Privacy Key - TPK	C
33	Offset of ZT subfile	ASCII	4	-	0210	-		C
37	Length of ZT subfile	ASCII	4	-	0063	-		C
41	ID Subfile identifier	ASCII	2		ID	-	Beginning of Subfile ID	C
43	Card expiration date	ASCII	8 +4	DBA	MMDDYYYY	0x0A	Information to update	V
55	Last name	ASCII	20+4	DCS	Last Name	0x0A	Information padded with space on 20 bytes	V
79	First Name	ASCII	20+4	DAC	First Name	0x0A	Information padded with space on 20 bytes	V
107	Card Issuance Date	ASCII	8+4	DBD	MMDDYYYY	0x0A	Information to update	V
119	Customer's Birth Date	ASCII	8+4	DBB	MMDDYYYY	0x0A	Information to update	V
131	Customer Gender	ASCII	1+4	DBC	X (1,2 or 9)	0x0A	Information to update (1=male, 2=female)	V
136	Eye Color	ASCII	+4	DAY		0x0A	Field Value empty	C
140	Height	ASCII	+4	DAU		0x0A	Field value Empty	C
144	Street Address	ASCII	+4	DAG		0x0A	Field value Empty	C
148	City	ASCII	+4	DAI		0x0A	Field Value Empty	C
152	State	ASCII	+4	DAJ		0x0A	Field Value Empty	C
156	Postal Code	ASCII	10+4	DAK	00000-0000	0x0A	Value 0 = Unknown -Padded with 2 spaces	C
171	Customer ID value (PI)	ASCII	8+4	DAQ	00000000	0x0A	TWIC Card Information Number (CIN)	V
183	Document Discriminator	ASCII	+4	DCF		0x0A	Field Value Empty	C
187	Country of issuance	ASCII	3+4	DCG	USA	0x0A	Indicates the units of height and weight	C
194	Last Name Truncated	ASCII	1+4	DDE	N	0x0A	Family name not truncated	C
199	First name truncated	ASCII	1+4	DDF	N	0x0A	First name not truncated	C
204	Middle name truncated	ASCII	1+4	DDG	U	0x0A	Truncation of middle name unknown	C
209	End of Subfile 1 (ID)	Hex	1			0x0D	CR in Hexadecimal (end of subfile 1)	C
210	Subfile 2 (TWIC file)	Hex	56+5	ZTZTA	TPK data object	0x0A	Contains 0xDCF101 TWIC data object	V
272	End of Subfile 2 (ZT)	Hex	1			0x0D	CR in Hexadecimal (end of subfile 2)	C

- Note: This column indicates if the field is a constant (C), or a variable (V) updated for each card

The TPK data object which in the subfile ZTA has the same format than the same data object found on the TWIC card contact side but it is listed in ASCII and needs to be converted to hexadecimal:

1) :0xDFC101 Constructed TPK Data Object Tag (same as in Card Data Model)
   a) 0xC0 0xll xx...xx (Hexadecimal representation of the key – up to 256 bytes)
   b) 0xC1 01 08 Algorithm Identifier (0x08 = AES ECB)
   c) 0XC2 01 00 TPK Key reference (unused = 0x00)

Example of a PDF 417 with such a structure: List of the values of the variable data objects:

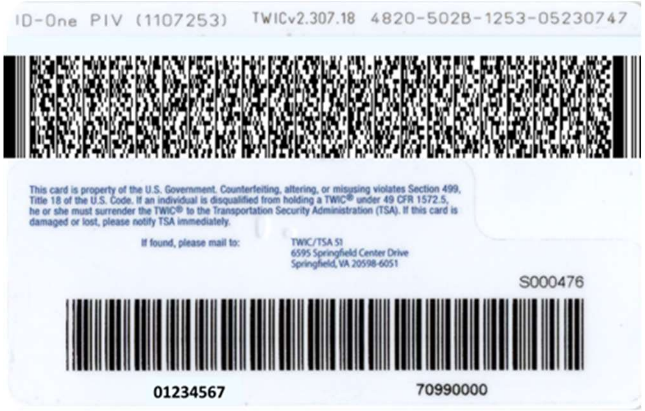
Card expiration date:	08182026	
Cardholder Last Name:	Cardholder	length of field is constant (20 characters) padded with spaces.
Cardholder first name:	TWIC G.	length of field is constant (20 characters) padded with spaces.
Cardholder birth date:	15061944	
Cardholder gender:	1	
Card Issuance Date:	08182021	
Personal Identifier:	01234567	This is the TWIC CIN which can be used to check the VCCL
TPK data object:	DCF101 28 C0 10 1234567890ABCDEF1234567890ABCDEF C1 01 08 C2 01 00	

PDF 417 encoded Data:

Note: The PDF 417 bar code was generated using tools from the company TokenWorks

```
@LF
RSCR
ANSI·709900100102ID00410168ZT02100063IDDBA08182026LF
DCSCardholder··········LF
DACTWIC·G.·············LF
DADLF
DBD08182021LF
DBB15061944LF
DBC1LF
DAYLF
DAULF
DAGLF
DAILF
DAJLF
DAK000000000··LF
DAQ01234567LF
DCFLF
DCGUSALF
DDENLF
DDFNLF
DDGULF
CR
ZTZTADCF10118C0101234567890ABCDEF1234567890ABCDEFC10108C20100LF
CR
```

Example of the back of the card with such a bar code:’



ID-One PIV (1107253) TWICv2.307.18 4820-502B-1253-05230747

This card is property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code. If an individual is disqualified from holding a TWIC® under 49 CFR 1572.5, he or she must surrender the TWIC® to the Transportation Security Administration (TSA). If this card is damaged or lost, please notify TSA immediately.

If found, please mail to:

TWIC/TSA 51
6595 Springfield Center Drive
Springfield, VA 20598-6051

S000476

01234567 70990000

5. TWIC Card Application Command Set

The TWIC card application does support the following ISO/IEC Application Protocol Data Units (APDU) commands for operation (the command name is written in capital letters):

- SELECT Card Command
- GET DATA Card Command
- GENERAL AUTHENTICATE Card Command
- PUT DATA (Card command in NEXGEN cards only)

Notes:

1. As for PIV (NIST SP 800-73), the GET RESPONSE APDU command does not appear at the application command layer (it is a transport layer command) 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 E of this document.
2. Other APDU commands may be required to handle application management features but, as they are not required for interoperability once the TWIC card has been activated and are not used by TWIC readers, such APDU commands do not appear in this specification.
3. Beyond the tags described in this specification, other ISO/IEC 7816-6 (or Global Platform) 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. Additional tags are not described in this document as they are specific to either an applet implementation, a given card manufacturer, or the management features of an applet implementation.

5.1 SELECT Card Command

Command Syntax

CLA	‘00’
INS	‘A4’
P1	‘04’ (Select by Name)
P2	‘00’
Lc	‘09’ (Select on a partial TWIC AID or a Full PIV AID length)
Data Field	TWIC AID (= TSA RID || TWIC first four bytes of the PIX)
Le	‘00’ or ‘xx’ -Length of the response including the TWIC card application property template expected when the application is found

- **Note:** In TWIC readers using TWIC cards, the SELECT “AID” APDU command shall always ask for a partial TWIC AID and analyze the information returned from the 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[24] or a live TWIC card. A full SELECT “AID” APDU command with a length of 11 bytes (Lc = 0x0B) is, nevertheless, supported by a TWIC card in order to be ISO/IEC 7816-4 compliant.

5.1.1 Application Property Template

Upon successful selection, the application selected returns the **application property template**, a constructed data object (Tag 61) as well as other data objects described below.

Tags embedded in the Application Property Template[25]:

Tag 4F When embedded in Tag 61, its value contains the full AID of the application selected by the command. (See Appendix C - TWIC AID Structure – Page 52)

Tag 50 Its value is a text (ASCII) string related to the Application Selected (e.g. Name).

Tag 79 Coexistent Tag Allocation Scheme. Contains another Tag 4F which represents the RID of the application selected. (See Appendix C – TWIC AID Structure - Page 52)

Other possible Tags part of the response

Tag 7F66 provides information to the reader about the size of data exchanges (See ISO/IEC 7816-4 about “ADPU Management - extended length information”)

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

[24] Test Cards are not used anymore with NEXGEN TWIC cards

[25] For other tags which could be returned in the Response, see ISO/IEC 7816-4 “section about “Application Template and related Data Elements”

5.2 GET DATA Card Command

Command Syntax

CLA	‘00’
INS	‘CB’
P1	‘3F’
P2	‘FF’
Lc	‘ 03’, ‘04’ or ‘05’ depending on the data object tag length
Data Field	refer to section 4.5, 4.6 and 4.7 related to the TWIC data model refer to section 4.2 and SP 800-73-4 for the PIV 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	TLV tag of the data object to be retrieved (one or three bytes)

Response Syntax for PIV/SP 800-73 compliant Data Objects

Data Field	TLV with the tag ‘53’ containing in its value field the requested data object[26]
SW1-SW2	Status Word

Response Syntax for ISO compliant Data Objects

Data Field	TLV with the tag of the data object requested in the command Data Field
SW1-SW2	Status Word

Return codes for both data objects modes

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 E 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.

[26] This response is not ISO/IEC 7816-4 compliant, but is the format imposed by the NIST SP 800-73 specification.

Some cards, depending on the transport protocol used, may not accept truncation in the response of the amount of data constituting a data object. In such cases, 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 formally 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/SP 800-73, does not support this alternate form of the GET DATA APDU command. In any case, it should be understood that reading all fields of a data object is required for security, allowing to verify its integrity and trustworthiness by checking its digital signatures.

3. Some TWIC cards (e.g. Legacy) did allow a Get Response which was not fully ISO compliant regarding the use of the length Le. TWIC NEXGEN cards do behave with the following ISO compliant rules:
    a. Le = 0x00 - It will only return 0x9000 and NO data
    b. Le Absent - It will only return 0x9000 and NO data
    c. Le < size of container - It will only send back Le bytes

5.3 GENERAL AUTHENTICATE Card Command

This command is available in NEXGEN TWIC as part of the TWIC card Application.

The GENERAL AUTHENTICATE card command performs a cryptographic operation, such as an authentication protocol, using the data provided in the data field of the command and returns the result of the cryptographic operation in the response data field[27]. The GENERAL AUTHENTICATE command shall be used with the TWIC authentication key ('9A') to authenticate the card or a card application to the client application.

The GENERAL AUTHENTICATE command supports command chaining to permit the uninterrupted transmission of long command data fields to the TWIC Card Application. If a card command other than the GENERAL AUTHENTICATE command is received by the TWIC Card Application before the termination of a GENERAL AUTHENTICATE chain, the TWIC Card Application does rollback to the state it was in immediately prior to the reception of the first command in the interrupted chain. In other words, an interrupted GENERAL AUTHENTICATE chain has no effect on the TWIC Card Application.

Command Syntax

CLA	'00' or '10' indicating command chaining
INS	'87'
P1	Algorithm reference. 0x07 for RSA 2048. See Table 6-2, SP 800-78 [6]
P2	Key reference: 0x9E (Card Authentication) - See Table 6-1, of SP 800-78
L$_c$	Length of data field
Data Field	PKCS #1 v1.5 or PSS padded message hash value See details below for template 0c7C
L$_e$	Absent or 0x00 depending on the place in the chain of commands

See detailed description of this command in document from NIST related to PIV cards - SP 800-73 Part 2 (PIV Card Application Command Interface) section A.4.1 related to RSA keys 2048 used with the General Authenticate Command on page 42.

[27] For cryptographic operations with large keys, e.g., RSA 2048, the GET RESPONSE command is used to return the complete result of the cryptographic operation. The GET RESPONSE command is illustrated in Appendix E

Data Objects in the Dynamic Authentication Table Template (0x7C)

Name	Tag	M/O	Description
Witness	'80'	C	Demonstration of knowledge of a fact without revealing the fact. An empty witness is a request for a witness.
Challenge	'81'	C	One or more random numbers or byte sequences to be used in the authentication protocol.
Response	'82'	C	A sequence of bytes encoding a response step in an authentication protocol.
Exponentiation	'85'	C	A parameter used in ECDH key agreement protocol

Response Syntax

Data Field	Absent, authentication-related data, signed data, shared secret, or transported key
SW1-SW2	Status word

SW1	SW2	Meaning
'61'	'xx'	Successful execution where SW2 encodes the number of response data bytes still available
'69'	'82'	Security status not satisfied
'6A'	'80'	Incorrect parameter in command data field
'6A'	'86'	Incorrect parameter in P1 or P2
'90'	'00'	Successful execution

5.4 PUT DATA Command (Card command available only in NEXGEN TWIC cards)

Command Syntax

CLA	‘00’
INS	‘DB’ - Command available on NEXGEN for E-Stickers (Free, or TSA Protected) Data Objects
P1	‘3F’
P2	‘FF’
Lc	Two or more bytes depending on the size of the command data field containing the E-Sticker information to be written in the card.
Command Data Field	See next table
Le	absent

Command Data Field

Name	information	M/O	Comment
Tag	0xE1 to 0xEA And 0xFA to 0xFD	M	TLV tag (One Byte) of the data object to be written in the card followed by the length of the value field on one or more bytes depending on the length on the value.
Length	One, two or Three bytes (see Appendix B)	M	Length of the value field (information to be stored) or 0x00 indicating an absent value field (equivalent to an erase)
Value	Data to write	O	This data field is not present when the length is zero (0x00)

Notes: **-** If a Put Data command is executed referencing any other data object in the card, it will be rejected with an error code of ’69 82’ or ’69 85’

Response Syntax

SW1-SW2		Meaning
SW1	SW2	Status word Description
‘65’	‘81’	Memory Failure – Indicates the card was not able to write in its memory
'67'	'00'	Length related error – Either the Lc field is not consistent with the length of data provided, or the length of data provided cannot be stored in the data object selected.
‘69’	‘82’	Security status not satisfied (data object selected is not updatable)
‘69’	‘85’	Condition of use not satisfied (data object selected is not updatable)
‘6A’	‘80’	Incorrect parameter(s) in the command data field
‘6A’	‘81’	Function not supported (might be a Legacy TWIC card)
‘6A’	‘84’	Not enough space in data object allocated in the card
‘6A’	‘88’	Data Object not found
‘90’	‘00’	Successful execution

6. PIV and TWIC Object Identifiers

TWIC employs Public Key Infrastructure (PKI) to include signatures and certificates. TWIC issues five-year certificates. The consequence of these longer life certificates is that 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 identical meanings 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 be able to recognize any OID value from the table below when parsing a signature or certificate from either the TWIC card application or the PIV card application[28].

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.
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.

[28] This considers the situation in which a NEXEGEN TWIC card had its PIV card application activated as PIV-I. In such card, the TWIC card application would still use the TWIC OIDs.

ID	Object Identifier	Description
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.
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	Object Identifier	Description
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 Threat Assessment indicator extension indicates the status of the subject's background investigation at the time of credential issuance.

6.1 How to use OIDs to find out the type of card presented

6.1.1 Using the ROOT of the OID:

The following Object Identifiers (OIDs) can be used to determine the issuer class of card being presented; namely TWIC, PIV, PIV-I, or CIV[29]. The use of the card authentication OID is preferred as it is accessible over either the contact or contactless interface AND support for a card authentication certificate is now available in both card applications of the card.

Card Authentication OID by class of card issuer:

OID NAME	Object Identifier	Description
id-TWIC-cardAuth	1.3.6.1.4.1.29138.2.1.3.17	**TWIC** - 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-PIV-cardAuth OR id-fpki-common-cardAuth	2.16.840.1.101.3.2.1.3.17	**PIV** - This specifies that the public key is used to authenticate the PIV card rather than the PIV cardholder.

[29] As of this writing the name Commercial identification Verification (CIV) is under revision by the Secure Technology Alliance (STA).

OID NAME	Object Identifier	Description
id-fpki-certpcypivi-cardAuth	2.16.840.1.101.3.2.1.3.19	**PIV-I** - This specifies that the public key is used to authenticate the PIV-I card rather than the PIV-I cardholder.
id-civCardAuthentication	1.3.6.1.4.1.24019.1.1.2.3	**CIV** (CertiPath) - This specifies that the public key is used to authenticate the CIV card rather than the CIV cardholder.

see https://en.wikipedia.org/wiki/Object_identifier for explanation of Object Identifier and “dot notation”.

Also refer to Annex A of X.660:2004 detailing “dot notation”.

- **“Root”.6.8** indicates that the card authentication key is linked to the physical card and not to the cardholder (no PIN required).
- **“Root”.6.9.1** indicates the background checks have been done successfully according to the rules established by the “Root” (issuer) for the cardholder.

7. TWIC Modes of Operation (Verification and/or Authentication)

7.1 General

This section describes what happens from the card standpoint when used in a given mode of operation by a TWIC reader. This section does not describe in detail what functions take place in the back-end system or reader and only describes direct card interactions.

TWIC cards are based upon a PIV compatible smart card (compliant with NIST SP 800-73, SP 800-76 and SP 800-78) and carry both a PIV Data Model card application and a TWIC card application that may be independently selected. This allows a TWIC card to operate either in “PIV-like” mode in PIV compatible readers[30] or in TWIC mode in TWIC readers.

TWIC contactless CHUID verification and TWIC contactless biometric user authentication are supported directly by the TWIC card application by all Legacy or NEXGEN TWIC cards.

Active Card authentication is supported by the NEXGEN TWIC card application, but not by Legacy TWIC cards. That said, for Legacy TWIC, Active card authentication over the contact or contactless interface is supported through the selection of the PIV Data Model card application.

Note: All data shall be retrieved from the TWIC card application for NEXGEN TWIC cards. Legacy TWIC cards require the use of the PIV card application and data model card for operations involving Active Card Authentication as well as obtaining the Facial Image from the card.

This section lists all the possible modes of operation of the TWIC card, independently of the type of device using it, but does not cover PACS registration (see Part 4 of the NEXGEN TWIC set of documents for card registration). Part 3 of the NEXGEN TWIC specification describes how these modes are implemented in the various types of TWIC readers.

The TWIC Card(s) can be used for various types of access control operations, each having a specific level of identity assurance[31].

Legacy TWIC cards have 6 Modes of operations:

- ❖ Manual Mode - Flash Pass/Visual Inspection (no device involved)
- ❖ Mode 0 - Supplement To Visual Inspection (STVI)[32]

1. Mode 1 - CHUID Verification
2. Mode 2 - Active Card Authentication
3. Mode 3 - CHUID Verification and Biometric Verification
4. Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric Verification

NEXGEN TWIC cards have 8 Modes of operations:

- ❖ Manual Mode - Flash Pass/Visual Inspection (no device involved)
- ❖ Mode 0 - Supplement To Visual Inspection (STVI)[33]

1. Mode 1 - CHUID Verification
2. Mode 2 - Active Card Authentication
3. Mode 3 - CHUID Verification and Biometric Verification
4. Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric Verification

[30] This mode is called CIV by the Security Technology Alliance. See documents available at https://www.securetechalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/

[31] PIV modes requiring either contact interface use or PIN presentation are not considered for access control in this document.

[32] This mode is available on iOS and Android Smart phones and is called TWIC ADVISR.

[33] This mode is available on iOS and Android Smart phones and is called TWIC ADVISR..

5. Mode 5 - CHUID Verification and Reference Picture Verification (RPV)
6. Mode 6 - CHUID Verification and RPV and Active Card Authentication

Notes:

- Only Mode 1 to Mode 4 were described in the previous TWIC documentation. These four modes do not require an operator.
- Mode 5 and 6 require an operator (local or remote) and are not available on Legacy TWIC cards.
- For all TWIC cards, this set of specifications presumes that Personal Identity Numbers (PINs) are not a requirement for authentication at any Maritime Security (MARSEC) level[34].
- The sequence in which the various verifications are shown in the mode of operations (described in the next section) are not mandatory, unless specified otherwise. For example, verifying if the FASC-N is on the CCL can technically be done before or after the Card Validity date is checked.
- For the detail operations performed by the Card Verification Device (CVD) or the TWIC readers for these modes, refer to Part 3 of this series of documents. In the following sections, the main principles of these modes are described from the TWIC card standpoint, but not the details of the actions performed by the readers.

7.2 Manual Mode - Flash Pass/Visual Inspection

The card is presented to an operator for access by the cardholder to access a facility. No device is used in this process. **The operator must verify that**:

1. the card looks legitimate (printed security features, card aspect, etc.),
2. the facial image printed on the card is the same as the cardholder, and
3. that the validity date printed on the card has not passed (card has not expired)

In this mode, a canceled (revoked) card will not be detected[35].

This mode is considered as providing a very low authentication level.

7.3 Mode 0 -Basic Mode or Supplement to Visual Inspection (STVI)

In addition to a Flash Pass verification, a Card Verification Device (CVD) is used to check if the card presented to the operator is not canceled. This mode is available on both Legacy TWIC and NEXGEN TWIC cards. **The operator using a Card Verification Device must verify that:**

1. the card looks legitimate,
2. the facial image printed on the card is the same as the cardholder,
3. the validity date printed on the card has not passed,
4. the card is not on a canceled list card (Visual CCL list).

The Card Identifier Number, or CIN, (found on the back of the TWIC card, bottom left) may be entered manually by the operator on the card verification device or read using the linear bar code of the TWIC card. The card verification device verifies the CIN against the Visual CCL[36] which has been downloaded in the card verification device recently.

This mode is considered as providing a low assurance level.

[34] See Part 4 – PACS registration section, where the PIV card PIN allows Legacy Cards to access the cardholder facial image.

[35] There is an average of more than 150,000 cards on the canceled card list which makes the manual detection of a card on the CCL nearly impossible.

[36] The Visual CCL contains the Card Identification Numbers (CINs) of the canceled TWIC cards and is updated daily.

7.4 Mode 1 - CHUID Verification

The TWIC reader (operating automatically, or under the control of an operator) executes the following steps:

1. Select the TWIC Card Application,
2. Read data from the TWIC card (using contact or contactless communication) the Card Holder Unique Identification Number (CHUID, Tag 0x5FC102)
3. Using the CHUID digital signature, verify the Integrity and the Validity of the CHUID,
4. Verify that the Card Expiration Date (from the CHUID) has not past,
5. Verify that the Credential Number from the CHUID (FASC-N) is not on the CCL[37]

The verifications steps 3 to 5 of this mode shall always be done, but may also be executed in the back-end system to which the TWIC Reader is connected.

This mode is considered as a low assurance level.

7.5 Mode 2 - Active Card Authentication (ACA)[38]

Note: For this specific mode, Legacy TWIC Readers that have not been updated to work with NEXGEN TWIC cards select the PIV Card Application in Step 1 and skip the test of step 2 and start at step 2.a of the following sequence of operation, as defined in the previous TWIC documentation. Both execute the same verifications.

The TWIC Reader (operating automatically, or under the control of an operator) executes the following steps:

1. Select the TWIC Card Application (AID = 0xA00000036720000001 selection on first 9 bytes)[39],
2. If the card is a Legacy Card (AID = 0xA000000367200000010101 returned), then
    a. Select the PIV Data Model Card Application (AID = 0xA00000030800001000)
3. Read from the TWIC card the Card Authentication Certificate (Tag 0x5FC101)
4. Verify the Integrity and the Validity of the digitally signed Card Authentication Certificate,
5. Extract from the Card Authentication Certificate the card identification number (FASC-N), and the certificate expiration date.
6. Verify the card certificate is not expired,
7. Verify the card identification number (FASC-N) is not on the CCL.
8. Execute an Active Card Authentication challenge using the Card Authentication Key and verify it is successful.

The verifications steps 4 to 8 of this mode must always be performed but may be executed in the back-end system (or the Certificate Validation System) to which the TWIC Reader is connected.

Note: This mode is similar to the PIV CAK mode but uses the CCL instead of the CRL for PIV CAK mode.

This mode provides a good level of assurance of the authenticity of the physical card (one factor - What you have).

[37] The CCL (Canceled Card List) contains the FASC-N (electronic credential identifier) of canceled TWIC Cards.

[38] This function is called CAK in PIV related documents as it uses the Card Authentication Key of the PIV Card Application. Because NEXGEN has its own Card Authentication Key in the TWIC Card Application and uses the CCL this document calls it ACA indicating the Key to use is the Card Authentication key of the TWIC card Application.

[39] This Select command uses only the first 9 bytes of the Card full AID as defined by ISO/IEC 7816-4 allowing to have the same select for all TWIC cards (Legacy or NEXGEN). The full AID value is returned by the card in the command response allowing the client application to test the version of the TWIC card presented.

7.6 Mode 3 - CHUID Verification and Biometric Verification

The TWIC reader (operating automatically, or under the control of an operator) must execute the following steps (Steps 1 to 5 are identical to Mode 1):

1. Select the TWIC Card Application,
2. Read from the TWIC card (using contact or contactless communication) the Card Holder Unique Identification Number (CHUID, Tag 0x5FC102)
3. Using the CHUID digital signature, verify the Integrity and the Validity of the CHUID,
4. Verify the Card Expiration Date (from the CHUID) is not past,
5. Verify the Card Identification Number from the CHUID (FASC-N) is not on the CCL
6. Obtain the Card TPK (either from the back-end system, or the back of the card [magnetic stripe for legacy TWIC cards/PDF417 for NEXGEN TWIC cards])
7. Read from the card the Cardholder Fingerprint template (Tag 0xDFC103). The TWIC Reader shall verify the biometric signature using the signing certificate.
8. Decipher the Cardholder fingerprint template using the TPK.
9. Verify the Card Fingerprint signature information has the same FASC-N as the FASC-N in the CHUID (see recommendation in FIPS 201-2, section 6.2.1.1)
10. Using the CBEFF information attached to the template, verify which finger(s) to be presented and that the template is not empty (no finger registered).
11. If there is no finger registered in the data object, indicate this mode cannot be used.
12. Capture the user presented fingerprint, create a template and verify it against the reference template obtained from the card.
13. If there is a match, indicate success. If not, retry step 12 up to a certain number of times (e.g. 3). After the maximum unsuccessful attempts, indicate no match was found

As for Mode 1, steps 3 to 5 may be executed in the back-end system and not in the device reading the card directly. Most of the verifications related to certificates and digital signatures are taken care of by the Certificate Validation System (CVS) which is a function described in more detail in Part 3 of this series of specification.

Steps 8 to 12 may be executed in a different device than the device interfacing with the card.

In this mode, in addition to the CHUID verification described in Mode 1, the cardholder's live biometric sample is compared to a biometric stored in the card as a reference. The biometric reference template may be read from a TWIC card at each use or may be stored in a database part of the TWIC Reader system (e.g. the PACS system which registered the user).

This mode provides a good level of authentication of the cardholder (one factor - who you are).

7.7 Mode 4 - CHUID Signing Certificate and ACA and Biometric Verification

Combining Mode 2 and Mode 3 provides a very good level of authentication with two authentication factors (Who you are & What you have).

7.8 Mode 5 - CHUID Verification and Reference Picture Verification (RPV)

In this mode, in addition to verifying the CHUID information and its signature, the user reference digital facial image is extracted from the card (TWIC NEXGEN cards only), deciphered and its digital signature verified. The reference cardholder facial image from the card is then displayed on the TWIC Reader (or on a remote device at the operator's location) for the operator to compare with the cardholder presenting the card. A remote operator must have a live video showing the TWIC card holder to determine if the displayed image is indeed the same as the person presenting the card to the reader and then manually make a determination to grant or deny access. The face verification may as well be done using an automated biometric back-end verification system instead of an operator.

With Legacy TWIC cards, this mode could be achieved by storing the cardholder facial image in the back-end system (The Cardholder facial image in Legacy TWIC cards is in the PIV Data Model Card Application and is protected by the PIV card PIN) at the time of card registration.

This mode, which requires an operator, or a biometric face recognition system, provides a good level of user authentication (One Factor - Who you are).

7.9 Mode 6 - CHUID Verification and RPV and ACA

This mode provides two factors authentication. In addition to the CHUID (mode 1) and Card Authentication (mode 2), this mode verifies (as in mode 5) the digital signature of the reference cardholder picture and displays it for an operator to authenticate the cardholder presenting the card.

This mode, available only on NEXGEN TWIC cards, provides a very good level of authentication (two factors: Who you are & What you have).

Appendix A TWIC Privacy Key Card Retrieval Processing

This Appendix describes how to extract the TWIC Privacy Key for TWIC cards. Three different methods can be used:

On TWIC Legacy Cards:

1. Reading the Data Object 0xDFC101 using the contact interface of the card, or
2. Reading the magnetic stripe on the back of the card.

On TWIC NEXGEN Cards:

1. Reading the Data Object 0xDFC101 using the contact interface of the card, or
2. Reading the two-dimensional bar code (PFD417) on the back of the card.

A.1 Reading Data Object 0xDFC101 using the contact interface of the card (all TWIC cards)

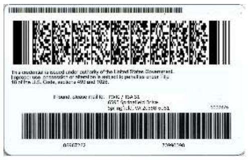
1. Select TWIC card Application
2. Read (GET DATA Card Command) data object 0xDFC101
3. Extract the information related to the TPK (value and Algorithm Identifier)

See detailed structure of the data object in section 25 - Data Object – TWIC Privacy Key Container.

A.2 Reading the magnetic stripe on the back of the card (Legacy TWIC Cards only)

1. Insert the TWIC card in a magnetic stripe reader
2. Decode the information form the magnetic stripe reader and extract the TWIC Privacy Key (TPK)

A.3 Reading the PDF417 on the back of the card (NEXGEN TWIC cards only)



1 Read the two-dimensional bar code (PDF417) from the back of the card.
2 Extract the information related to the TPK (Subfile ZTA, tag 0xDFC101)

See detailed structure of the PDF417 data string in section 4.9-

Appendix B Length management and structure of TLV data objects

All the data objects in the TWIC card (in both card applications) are using a TLV (Tag-Length-Value) structure.

The tags used in the TWIC card are on one, (eventually two) or three bytes. They are defined in different documents depending on the card application they are used in. PIV data object tags are described in the NIST document SP 800-73-4. Since some of these tags are ISO smart card generic tags, they may also be described in the ISO/IEC 7816-4 standard (e.g. 0x7F61 - biometric template). All of the TWIC data object tags are described in this document in sections 4.3, 4.5, 4.6 and 4.7   The tags are all on one, (sometimes two) or three bytes.

For historical reasons, these tags are not fully compliant with the Basic Encoding Rules (BER) defined in the ASN.1 standard ITU-T X.690[40]. The difference relates to the bit indicating if the data object is constructed (when it contains more TLV data objects) or primitive (contains just a length and one data value) or is not used consistently[41]. As such, the information about the construction of a given data object (constructed or primitive) has to be known by the client application using TWIC cards and cannot always be deducted by analyzing the structure of the tag itself[42].

The length of all data objects in the TWIC cards are on one, (sometimes two) or three bytes. All of the length used are compliant with the TLV BER encoding rules (ASN.1 standard ITU-T X.690).

The table below (which represents the first octet of the length: the byte which follows the last byte of a tag), explains how lengths of TLV data objects are constructed:

Form	Bits							
	8	7	6	5	4	3	2	1
Definite, Short	0	Length (0 to 127 bytes in bit 7 to 1 of this byte)						
Indefinite	1	0 (this form is not used in TWIC or PIV)						
Definite, Long	1	Length (0 to 127 bytes) to multiply by the position of the byte in the length.						
Reserved	1	127 (never used, value reserved by the standard)						

This table shows that any data object with data of a length bigger than 127 bytes will have two or more bytes for its length.

As such, the client application shall always test for (or built) the number of bytes used in a given TLV data object according to this structure.

It is possible (but not recommended) to have more bytes than required to indicate the real length of a data object. For example, a typical data object with usually 128 bytes of data, may have a length of two bytes even when the data object is completely empty (see examples below).

[40] Abstract Syntax Notation One (ASN.1) - INTERNATIONAL TELECOMMUNICATION UNION (ITU) - https://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf

[41] For a simple explanation of this standard a good reference can be found at: https://en.wikipedia.org/kiki/X.690#BER_encoding

[42] For example, the Tag 0x5FC102 (CHUID) used by the PIV as well as the TWIC card application does not have the bit 6 of the first byte turned on. As such it looks like a primitive data object when it is in fact a constructed data object. If the tag was compliant with the BER ASN.1 notation it would be referenced as 0x7FC102.

Example of the length of a data object with 435 bytes in the value field:

Byte 1								Byte 2								Byte 3							
1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	1	1
Long Form	Length is on following two bytes							435 bytes of data in the value field															

Examples of the length of a data object with 0 bytes in the value field (empty object):
Example with a length of zero on one byte (no value field follows):

Byte 1							
0	0	0	0	0	0	0	0
Short Form	Length is zero on one byte						

Example with a length of zero on two bytes (no value field follows):

Byte 1								Byte 2							
1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Long Form	Length is in the following one byte							Zero byte of data in the value field							

Appendix C TWIC AID Structure

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 consists of a 5-byte Registered Identifier (RID) and a 6 byte Proprietary Identifier Extension (PIX).

C.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.

C.2 Proprietary Identifier Extension (PIX) Structure

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

The PIX of TSA cards consist of 6 bytes:

- 2 bytes for the Application group
- 2 bytes for the TSA Application (0x0001 for TWIC)
- 2 bytes for the major and minor application release (with one bit for test cards)

Application Group:

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' (all TWIC Cards)

Application:

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 value ’00 01’ identifies the TWIC application.

Releases and class:

The final two bytes of the PIX define the class of TWIC cards and the 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.

The two last bytes of the PIX are used to identify the major and minor releases of the data model and card edge edition and also to indicate the class of the TWIC card (test or not). If the most significant bit of the first 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[43]. The remaining 7 bits of this byte always indicate the major release of the data model and card edge edition. The next and last byte indicates the major release of the data model.

[43] The test mode is not used anymore and will not be used in NEXGEN TWIC cards. As such this bit will always be zero (0).

A major release value is changed when 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. A change in major release indicates that backward interoperability may not be guaranteed for all modes of operation. Major releases start at “1”.

A minor release value changes if the card application data model is modified (or enhanced) due to changes or additions in optional data objects that improve the operational use of the TWIC card. Changes in minor releases are managed to provide backward compatibility in all modes of operations with the previous release. Minor releases start at “1”. (‘0000 0001’ in binary or 0x01)

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.

For Legacy cards, the minor release TWIC data model and card edge edition is defined as release ‘1’ (or ‘0000 0001’ in binary format).

The NEXGEN cards described in this series of documents are using minor release ‘3’ (0r ‘0000 0011’ in binary format).

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

Bytes of the AID	Symbol	Value	Comment
1 to 5	RID	A0 00 00 03 67	TSA RID
6 & 7	Group	00 00 & FF FF	Reserved values
		10 00	TSA employees & contractor group
		20 00	non-TSA employees or contractors group
8 & 9	Application	00 00 & FF FF	Reserved values
		00 01	TWIC application in group 20 00
10	Major Release	00 & FF	Reserved values
		0xxx xxxx	Bit 7 is reserved for future use and is set to “0” in all TWIC cards
		01	TWIC specification major release #1
11	Minor Release	00 & FF	Reserved values
		01	TWIC application first release
		03	TWIC application NEXGEN release

Note: As defined by ISO//IEC 7816-4, the AID technically 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 by a client application using a TWIC card data model are:

A0 00 00 03 67 20 00 00 01 01 01	Operational Legacy TWIC Card
A0 00 00 03 67 20 00 00 01 01 03	Operational NEXGEN TWIC card

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

Note: A TWIC reader looking for a TWIC card application shall 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 answers with the full AID of the TWIC card application that exists on the 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 could not be made upward compatible (thus creating a potential problem for existing TWIC readers), a new application AID will have to be defined using the TSA RID and a new PIX structure.

It is also possible, in NEXGEN Cards, to access the discovery data object to verify the application AID value.

Appendix D Structure of the Card UUID in TWIC cards

In all Legacy TWIC Cards, the Card UUID (present in the GUID of the FASC-N), is using the null value allowed by the RFC 4122 (all 16 bytes are zeros).

In NEXGEN TWIC cards, the Card UUID is present in the GUID of the FASC-N as well as in all digitally signed data objects of the card. Its structure is using the named-based version (version 5 of RFC 4122) with a name preventing collisions. The detail of this structure is described below. It must be noted that the value of the card FASC-N can be extracted from the Card UUID structure used in NEXGEN TWIC cards.

The latest revision of NIST SP800-73 document requires the use of a RFC 4122 populated compliant format to construct the Card UUID in all PIV and PIV-I cards. TWIC NEXGEN is aligned with this requirement which ensures that a common identifier (the Card UUID) will be shared between all card applications in the TWIC card (PIV/CIV, TWIC and eventually PIV-I in TWIC cards if such activation was to be done).

There are three acceptable structures providing quasi-unique numbers in addition to the null structure used by TWIC Legacy cards. For NEXGEN TWIC cards, this document describes the use the UUID name version of RFC 4122 (so called "version 5" form) which allows a backwards compatible method for TWIC readers needing to use the FASC-N value, even if the PIV Data Model card application has been activated into PIV-I in the card[44].

A FASC-N includes three important data fields used by many PACS as a unique identifier. These fields (in order of appearance in the FASC-N) are the Agency Code (four decimal digits), a System Code (four decimal digits), and a Credential Number issued under a given System Code (6 decimal digits). It means the maximum number of credentials such a structure can work with is 99,999,999,999,999 cards. Such a (large) number requires only 47 bits to code the binary value[45] of all of the fields of a FASC-N. It means that using a 48 bit structure will guarantee that any existing numeric value for these fields allows any FASC-N to be stored in a UUID structure without losing any information.

As such, NEXGEN TWIC Cards are using the Name Version of RFC 4122 (code M = 5) to create the Card UUID according to the following mapping:

Space Name =	DHS-TSA-TWIC	constant for all NEXGEN TWIC cards
Sub Name =	FASC-N (value)	using a trivial hash function (direct mapping)
p values =	all zeros	Will be used in the future to manage versions

Using the canonical representation of the UUID structure as defined in RFC 4122 for version 5:
hhhhhhhh-hhhh-5hhh-Nppp-nnnnnnnnnnnn

- h = hash value of the space name on 60 bits
- N can be 8, 9, A or B depending on the two high bits of the next field
- p = Zeros, or Random or Pseudo random on 14 bits
- n = hash value on the sub-name on 48 bits

The following example is using SHA-1 to hash the Space Name (resulting in a message digest of 20 bytes [160 bits] or in this case 0x91be2094f6dc34931f98f3c111765355926432f5) and truncated to the most significant 60 bits, the "h" value of the name space for TWIC cards is constant: 0x91be2094f6dc349.

All p values are zeros, so N will have a value of 8.

[44] PIV-I cards require the FASC-N value to be all "9"s, losing backward compatibility with previous TWIC structures.

[45] 48 bits allows counting to up to 281,474,976,710,656.

The “n” values will be representing the FASC-N on a direct trivial Decimal mapping to a binary value on 48 bits (or Hexadecimal on 12 digits).

Such a structure allows any TWIC reader to reconstruct the first three fields of a TWIC FASC-N (i.e., Agency Code = 7099, System Code and Credential Number) from the Card UUID (or conversely) if needed, allowing a very simple migration path for the readers and the PACS they interface with.

```
Agency Code–System Code–Credential Number
          \     |          /
           \    |         /
            \   |        /
             V  V       V
```

Example for a FASC-N of **7099-1055-048796** (Decimal) -> in Hexadecimal = 0x**4090E49E505C**

Corresponding Card UUID in canonical form: **91be2094-f6dc-5349-8000-4090E49E505C**

Notes:

1 -The FASC-N Value is sometimes said to be Binary Coded Decimal (BCD) but here it is represented with decimal numbers, so it is a decimal representation.

2- To do these conversions, you may use the following web sites

https://miniwebtool.com/hex-to-bcd-converter

https://miniwebtool.com/decimal-to-hex-converter/

Appendix E Use of Get Response APDU at the application layer

Note: As explained in this section, the length management of data blocks transmitted between the card and the TWIC reader have a different structure than TLV data object length.

Many cards in use today, as well as interface drivers and card TWIC 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 that the application layer is not adversely impacted when future smart cards support large data block transfers[46].

The following mechanisms are available in ISO/IEC 7816-4 to address this short length APDU issue when Extended Length transmission is not used:

1. Employ command chaining. The command chaining bit in the CLASS byte of the APDU indicates command chaining used to TRANSMIT to the card (like PUT DATA or GENERAL AUTHENTCIATE) when a command data field payload is larger than 256 byte. This mechanism is commonly used for case 3 commands (e.g. PUT DATA with INS byte = 'DA') as used in PIV/SP 800-73.
2. Use the GET RESPONSE APDU command at the application layer to RECIEVE information.

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/SP 800-73 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 to enable TWIC reader manufacturers to implement TWIC card interfaces in a consistent and coherent manner.

In most TWIC reader implementations, the limit between the Transport Protocol Data Unit (TPDU) layer (transport layer dependent on the transport protocol) and the APDU (application layer interface) may be difficult to establish. It is highly recommended that TWIC reader manufacturers 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 and card Operating System version.

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

[46] It must be noted that in an electrically noisy environment, using large blocks may slow down the communication speed as for any error, the whole block has to be retransmitted.

The described mechanism does not address (or use) the GET RESPONSE APDU command and length management defined in secure messaging modes[47] (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 is assumed 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.
- 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 = ‘00 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 ‘00 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 does respond with the data object. If the length “Le” of the Get Data was different than 00 (01 to 1F), some card may return the information, but issue a return code of ‘62 82’ in the response indicating there are less data bytes than expected.
3. If the data object is larger than 256, the smart card does 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 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).

[47] Not used in TWIC standard modes of operation.

Appendix F Use of E-Stickers Data Objects in NEXGEN cards

More detailed information about the use of E-Stickers is provided in Part 4 (about PACS using NEXGEN cards). This section is only a brief summary of what these data objects can be used for, and how they are accessed in NEXGEN cards.

There are Ten E-Stickers (tags 0xE1 to 0xEA) which behave as ISO data objects with Get data (read) and Put data (write) commands. These ten data objects can be Updated (using a PUT DATA) or Read (Using a GET DATA) without any access control restriction from the card. They are available for client systems (PACS, Worker's management systems, etc.) to store or retrieve information related to the given user of that card.

There are four TSA controlled Data Objects (0xFA to 0xFD). These data objects, also behaving as ISO data objects, are, as all E-Stickers, free read, but they require the Card issuer to be authenticated by the card in order to be updated.

Any of these Data Objects can be used to store addition information related to the cardholder (e.g., if the cardholder is also a HAZMAT[48] qualified person) and for other purposes.

The following structure is suggested (but not mandated or controlled as e-Stickers are TSA unmanaged storage) in order to allow such data objects to be used by multiple unrelated entities in NEXGEN TWIC cards.

- All E-Sticker Tags (Free update Tags 0xE1 to 0xEA as well as TSA Controlled Data Objects 0xFA to 0xFD) are using only byte and indicate they are constructed Data Objects.
- Data Object tag and its Length (One to up to three bytes)
    - Header (has its own Tag and Length[49]):
        - Code (one byte - indicates what the DO is used for)
        - Sub-Code (one byte - Sub-indication of the DO use)
        - System ID (8 bytes - owner/creator of the Data Object)
        - Creation date & time (6 bytes - when the Data Object was written in the card)
    - Information (has its own Tag and Length)
        - Information specific to the owner (identified by the data object System-ID)

Note: to indicate an E-Sticker is empty, it should be written with a zero-length header according to constructed ASN.1 tags. This is how they should be initialized (or erased) in a NEXGEN TWIC card.

Example of an empty E-Sticker: 0xE1 02 80 00

Nevertheless, sometimes, these Data Objects (as some other ISO optional Data Objects in TWIC NEXGEN) may have never been initialized even during the card production; in such case, either the response to the Get Data will be the requested tag followed by 0x00 (which is not a good ISO response) or there will be no information about the tag or length returned, just a return code of 0x9000. Example for a never initialized e-Sticker with Tag 0xE2: response might be: 0xE2 00.

[48] HAZMAT = Hazardous Material(s)

[49] length of zero in a Put Data is equivalent to an erase

Example for an E-Sticker (values below are examples):

Tag (one bytes):	0xE1	
Length (one up to three bytes)	0x1D	
1) Header Tag	0x80	
2) Header Length	0x10	
a) Code	0x53	
b) Sub-Code	0x00	
c) System-ID/Owner	0x2542500010000000	
d) Creation Date	0x201707281300	(YYYYMMDDHHMM)
3) Information tag	0x81 (or 0xE1 if the information is a constructed data object as well)	
4) Information length	0x09	
a) Update Date	0x20180323	(YYMMDD)
b) Update Time	0x130203	(HHMMSS)
c) Number of people	0X0025	

In this imaginary example, the information is for a local use case (Code byte 0x53): The sub-code is set to 0x00, the System ID is the ZIP code of Harper's Ferry (ZIP = 25425) which created the E-Sticker on 2017-07-28 at 13:00 hours, and updated the information on March 23, 2018 at 13:02:03 hours, indicating there was a load of 25 passengers on the Ferry that day.

The suggested codes, sub codes and system ID structures proposed are detailed in a separate document (not a specification) related to E-Stickers: NEXGEN TWIC E-Stickers Vx.pdf [50]which may be obtained by sending an e-mail to TWIC-Technology@TSA.DHS.Gov

[50] This document is only a recommendation/suggestion and not a specification.

Appendix G Interpretation of the Biometric Template CBEFF Header

The biometric template is encoded in a manner that communicates to a TWIC reader including:

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 value[51].

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 during capture)
      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)

[51] 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.

Appendix H – Key Identifiers and Key supported Algorithms

The following tables are extracted from the NIST document SP 800-78-4 Section 6.2

Algorithm Identifier	**Algorithm – Mode**
'00'	3 Key Triple DES – ECB
'03'	3 Key Triple DES – ECB
'06'	RSA 1024 bit modulus, 65 537 ≤ exponent ≤ 2^{256} - 1
'07'	RSA 2048 bit modulus, 65 537 ≤ exponent ≤ 2^{256} - 1
'08'	AES-128 – ECB
'0A'	AES-192 – ECB
'0C'	AES-256 – ECB
'11'	ECC: Curve P-256
'14'	ECC: Curve P-384
'27'	Cipher Suite 2
'2E'	Cipher Suite 7

Card Keys used in PIV cards:

Key Type	**Key Reference Value**	**Permitted Algorithm Identifiers**
PIV Secure Messaging key	'04'	'27', '2E'
retired key management key	'82', '83', '84', '85', '86', '87', '88', '89', '8A', '8B', '8C', '8D', '8E', '8F', '90', '91', '92', '93', '94', '95'	'06', '07', '11', '14'
PIV Authentication key	'9A'	'07', '11'
PIV Card Application Administration Key	'9B'	'00', '03', '08', '0A', '0C'
digital signature key	'9C'	'07', '11', '14'
key management key	'9D'	'07', '11', '14'
asymmetric Card Authentication key	'9E'	'07', '11'
symmetric Card Authentication key	'9E'	'00', '03', '08', '0A', '0C'

Appendix I - Federal Agency Smart Credential – Number (FASC-N)

The following is for information only and information was copied from the document:

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems - V 2.3 published on December 20, 2005 by the Physical Access Interagency Interoperability Working Group.

Field name	Length (BCD digits)	Field description
AGENCY CODE	4	Identifies the government agency issuing the credential
SYSTEM CODE	4	Identifies the system the card is enrolled in and is unique for each site
CREDENTIAL NUMBER	6	Encoded by the issuing agency. For a given system no duplicate numbers are active
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Initially encoded as “1”, will be incremented if a card is replaced due to loss or damage
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier. (e.g. DoD EDI PN ID)
OC	1	ORGANIZATIONAL CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government

OI	4	ORGANIZATIONAL IDENTIFIE
		OC=1 – FIPS 95-2 Agency Code
		OC=2 – State Code
		OC=3 – Company Code
		OC=4 – Numeric Country Code

POA	1	PERSON/ORGANIZATION ASSOCIATION CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary

According to SP 800-73-4 section 3.1.2, the credential series, individual credential issue, person identifier, organizational category, organizational identifier, and person/organization association category may be populated with all zeros.