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.

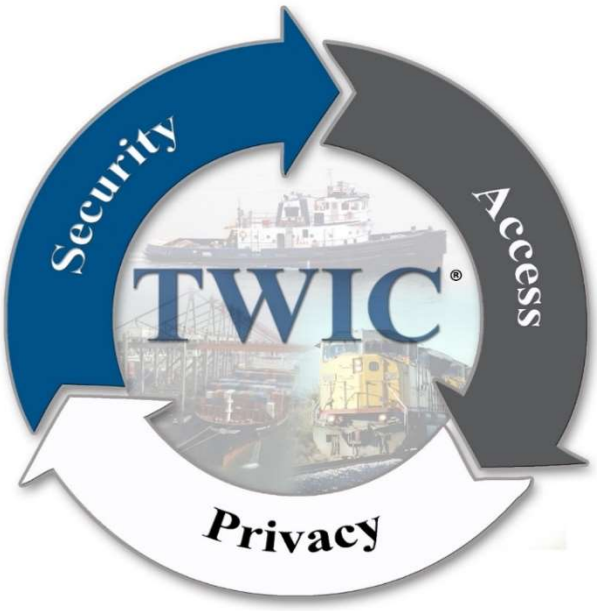
In early 2024 some changes were implemented for Legacy TWIC Cards and these newly issued Legacy TWIC cards do not strictly comply with the 2012 documentation.

- 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 3 – TWIC® Reader Requirements
April 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 the comments from Industry
October 2019	Text revised for final publication
January 2020	Modifications incorporating comments from the Industry Round 2
May 2020	Modification incorporating Round 3 changes
April 2022	Added header indicating this may not be the final release
July 2022	Added information about the TWIC application PIN (now used by NEXGEN) and the PIV Application PIN used by the NEXGEN & TWIC Legacy cards
February 2023	Updates of the document to be used in the new NEXGEN SC-QTL process. Editorial changes only, no information updates.
March 2023	Minor editorial changes and typo corrections
April 2023	Editorial corrections
June 2023	Very minor editorial corrections
July 24th, 2023	First Official release of the documentation
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 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. In this version, only the PDF 417 still might be modified
August 22, 2023	Notion of Safe Operation in an explosive atmosphere is expanded to all TWIC readers as an option (was only Fixed outdoor readers before)
September, 19 2023	The format of the PDF 417 on the back of the card has changed from ASN.1 to the AAMVA standard. The details are in Part 2.

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.

List of acronyms and abbreviations frequently used in this specification.

AAMVA	American Association of Motor Vehicle Administrators
AES	Advanced Encryption Standard
AID	Application Identifier
ANSI	American National Standards Institute
CA	Certification Authority
CBEFF	Common Biometric Exchange Formats Framework
CCL	Canceled Card List of FASC-N (formerly known as the Hotlist)
CFR	Code of Federal Regulations
CHUID	Card Holder Unique Identifier
CIN	Card Identification Number
CISPR	International Special Committee on Radio Interference
CIV	Commercial Identity Verification
CRL	Certificate Revocation List
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard (NIST)
IBIA	International Biometric + Identity Association
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCITS	InterNational Committee for Information Technology Standards
ISO/IEC	International Standards Organization/ International Electrotechnical Commission
MARSEC	Maritime Security
NFC	Near Field Communication
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
RSA	Rivest–Shamir–Adleman Algorithm
SIA	Security Industry Association
STA	Secure Technology Alliance
SP 8xx	Special Publication (NIST)
TLV	Tag-Length-Value
TPK	TWIC Privacy Key
TSA	Transportation Security Administration
TWIC	Transportation Workers Identification Credential
UUID	Universal Unique Identifier
VCCL	Visual Cancelled Card List of CIN

Table of Contents

List of Figures & Tables

1. Overview

1.1 Abstract

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

This third part describes in detail TWIC reader requirements, the type of mechanical and electrical specifications a TWIC reader must comply with, as well as the various functional options a TWIC reader implementation can claim to be supported. Both portable as well as fixed readers are described in this part. The functions specified in this third part are requirements, indicated by a "shall"; a TWIC reader must comply with them in order to be qualified for the Transportation Worker Identification Credential (TWIC) use. Some features are optional, and the term "may" (or "should") is used in such optional cases.

Important terminology:

- A new terminology is introduced in this series of documentation in relation to readers. The term "***Card Verification Device***" is used for devices which are not interacting electronically with the TWIC card. In addition to the two types of readers (Fixed or Portable), the term "***TWIC Reader***" is used for any type of device which interacts electronically with the TWIC Card. A TWIC reader may be an instance of a physical TWIC reader of the standard types (fixed or portable), or a device such as a computer, or even an enabled NFC[2] smart phone in which has been loaded a specific application dealing with TWIC cards and using the TWIC card according to one of the modes described in this series of documents. As a consequence, this part has been completely redesigned from the previous specification, with the functional requirements (dealing with the TWIC cards in various modes) being first described for all types of readers, even if they are not described in the following sections, followed by specific sections for the two types of instantiated TWIC physical readers: Fixed and Portable.
- To avoid any confusion with a Personal Identity Verification (PIV) card and a "PIV-like" 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 NIST documents describing the format of the data and structures to be stored in a PIV-like card. These documents are: SP 800-73, SP 800-76, and SP 800-78[3]. In addition, the PIV card itself is compliant with the NIST document SP 800-79 which defines the Federal trust model (Federal Bridge used by PIV and PIV-I[4]) 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).The TWIC card always has two distinct card applications loaded in it: the PIV Data Model card application and the TWIC card application. Each card application in a TWIC card has a unique Application Identifier (AID) used to select the application by a reader.
- As a new version of the TWIC card is being introduced (called NEXGEN TWIC card), this specification considers two types of TWIC cards (Legacy TWIC and NEXGEN TWIC), and all readers shall be able to recognize them and work with both[5].

A reader is often a component of a larger system such as a Physical Access Control System (PACS). This third part of the documentation deals mainly with reader behavior, but may also impose some

[1]TWIC® is registered in the U.S. Patent and Trademark Office by the U.S. Department of Homeland Security.
[2] NFC stands for Near Field Communication and is defined in ISO/IEC 18092
[3] NIST Special Publications can be found in the list of normative references in Section 2.1
[4] PIV-I stands for Personal Identity Verification Interoperable. See Reference [R38]
[5] The NEXGEN TWIC card has been designed to be backward compatible with Legacy TWIC cards and as such, a TWIC reader only compliant with the previous TWIC specification should be able to work with NEXGEN TWIC cards but will not be able to take advantage of the new features available in NEXGEN TWIC.

requirements on the PACS controller/panel or the back-end system the reader is connected to, making sure all security verifications (e.g. verification of digital signatures, or card does not appear on the canceled card list) have been fulfilled for the reader to be considered as compliant with requirements described in this series of documents.

The TWIC specification was initially developed by the National Maritime Security Advisory Committee (NMSAC) in response to a request from the Transportation Security Administration (TSA) and the U.S. Coast Guard. The NMSAC TWIC Working Group included members of the maritime industry with support from representatives from the security technology industry who are affiliated with such organizations as the International Biometric Industry Association (IBIA[6]), the Security Industry Association (SIA) and the Smart Card Alliance[7]. The original specification developed by the NMSAC TWIC Working Group has been modified to accommodate TSA security and privacy requirements.

1.2 Scope and purpose

The scope of the TWIC specification documentation is to provide:

- Part 1 – General Description of TWIC credential in use by the maritime industry
- Part 2 – TWIC card application data model, TWIC card application card edge behavior during normal operation
- **Part 3 – TWIC reader requirements (**this document**)**
- Part 4 – TWIC registration and TWIC card use by a PACS
- Part 5 – (Future) TWIC activation into a PIV-I compatible credential[8].

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

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

It is important to consider 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. 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 begin to be issued to TWIC cardholders.

The two types of cards are called "**Legacy TWIC**" and "**NEXGEN TWIC**" respectively in this series of documents. 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

[6] IBIA changed its name from International Biometric Industry Association to International Biometric + Identity Association
[7] Smart Card Alliance has changed its name into Secure Technology Alliance (https://www.securetechalliance.org/)
[8] This last part is to be created in the future as it requires some modification in PIV-I activation stations.

NEXGEN TWIC card. The term **NEXGEN** used in this document should not be confused with the similarly title **NexGen** used in some communications for the 2018 physical card design[9].

1.3 Summary of Changes to 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) section 1.3 of this series of documents.

The requirements for Safe operation of TWIC readers in an explosive Atmosphere were initially limited to Fixed Outdoor Readers. This version of the specification expands the notion of Safe operation requirements to all types of readers as an option.

It is also important to note that some TWIC Legacy cards may be issued with the hash function SHA-256 instead of the SHA-1 initially used when Legacy Cards were first defined in 2012.

1.3.1 Warning about possible changes of this revision of the specification

> The content and format of the PDF 417 on the back of the TWIC card has been changed to comply with the AAMVA standard instead of the basic ASN.1 structure as it was before. Some information (such as the date of birth of the card holder) has also been added to the bar code data elements. See TWIC NEXGEN Specification Part 2 for details.

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

2. References

2.1 Normative References[10]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[R28] OSHA Regulation 1910.147 De-energizing Equipment

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

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

[R31] NIST Special Publication 800-96 PIV Card to Reader Interoperability Guidelines (September 2006)

[R32] AAMVA DL/ID Card Design Standard (2020) -

2.2 Informative References

[R33] FIPS Publication 201-2 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (August 2015)

[R34] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)

[R35] ICAO 9303 Machine Readable Travel Documents

[R36] 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).

[R37] OSPD 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.

[R38] Comparison between PIV, PIV-I and CIV[11] from the Secure Technology Alliance. https://www.securetechalliance.org/resources/pdf/PIV_PIV-I_CIV_brief_022212.pdf

[11] Commercial Identity Verification

3. Definitions

3.1 Conformance levels

- **may:** A key word indicating flexibility of choice with *no implied preference*.
- **must:** A key word indicating a mandatory requirement which may not be testable and would have to be asserted by the manufacturer of the product. Designers of systems including TWIC readers shall implement the functionality described for a correct security implementation, even if it is outside of the testable physical product.
- **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*.

3.2 Glossary of terms

- **Canceled Card List (CCL**): Updated each day by the TWIC system, this list contains all the TWIC credential numbers (FACS-Ns) which have been canceled. Cards which have expired are not in this list.
- **Card Application:** an application identified by its Application Identifier (AID) loaded (or present) in a smart card as indicated in ISO/IEC 7816-4.
- **Card Verification Device (CVD):** This term is used in this series of documents to indicate a device which does not interact electronically with a TWIC card but may provide information 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 a Device) and claiming to be the legitimate cardholder.
- **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.
- **Legitimate Cardholder**: The vetted person who was given the TWIC card by the TSA TWIC system and whose personal and biometric information is 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.
- **Operator/Guard:** A person in charge of verifying the validity of a TWIC card, and/or the cardholder presenting the card.

- **PIV application PIN:** Personal Identification Number which has to be presented when the PIV card application is selected in order to access (in read mode) to the data objects which are PIN protected.
- **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 specifications.
- **TWIC Card Application:** The card application present in a TWIC Card, conformant to the TWIC Card Specification (Part 2 of this series of documents)
- **TWIC Card:** A smart card that corresponds to the specifications laid out for the Transportation Workers Identity Credential Program.
- **TWIC Legacy:** TWIC Cards conforming to the 2012 clarified TWIC Reader and Card specification.
- **TWIC NEXGEN:** TWIC cards conforming to this new TWIC card specification.
- **TWIC Privacy Key:** A 128-bit AES[12] symmetric key value used to encipher the biometric templates that are stored on the TWIC card.
- **Visual Canceled Card List (VCCL)** - Updated each day by the TWIC system, this list contains all the Card Identification Numbers (CINs) of TWIC cards which have been canceled. Cards which have expired are not kept in this list.

[12] AES - Advanced Encryption Standard – See NIST documents at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

4. General considerations for the use of TWIC Cards

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

The TWIC is designed to be used in various systems at different levels of security depending on the requirements of each site and under specific threat levels. This document does not make any recommendation on the specific levels which need to be used by the sites but indicates the different modes of operations available allowing each site to create its own authentication security policy (level of identity assurance about the credential presented) in accordance with the TWIC Rule and Coast Guard requirements.

TWIC cards are based upon a PIV compatible smart card and carries both a PIV Data Model card application and a TWIC card application that may be independently selected. This allows a TWIC card to operate both in PIV/CIV mode (in PIV/CIV[13] compatible readers) as well as TWIC mode (in TWIC compatible readers). TWIC contactless CHUID[14] verification and TWIC contactless biometric user authentication are supported directly by the TWIC card application. Card authentication is not supported in the TWIC card application by Legacy TWIC cards but is available in a NEXGEN TWIC card application. For Legacy TWIC cards, card authentication over the contactless interface is supported through the selection of the PIV Data Model card application. See Section 4.4.4 for Details).

Note: All TWIC-related data shall be retrieved from the TWIC card application except for operations involving Legacy TWIC cards for the Active Card Authentication (ACA) function.

4.1 Type of readers using TWIC cards

This part considers different types of readers interacting with TWIC cards (Legacy or NEXGEN). Two main categories are defined:

1. **Card Verification Device (CVD):** This term is generic and used when a device deals with a TWIC card without interacting electronically with the chip of the TWIC card. For example, reading the linear bar code (1D) on the back of the card[15], or verifying one or more security features. The device could be of any kind and is not specifically defined in this document.
2. **TWIC Readers:** This generic term is used in this series of documents for electronic readers interacting with the chip of the TWIC card, either using the contact or contactless interface. This includes Fixed TWIC reader, Portable TWIC readers, but also any other TWIC readers claiming functionality described in this series of documents. The detail categorization of TWIC readers defined in this document is provided in section 4.1(Card reader types).

All TWIC Readers shall support configuration of one or more verification or authentication modes listed in the next section (4.4 Modes of Operation)

[13] See document form the Secure Technology Alliance comparing PIV, PIV-I and CIV type of cards: https://www.securetechalliance.org/publications-a-comparison-of-piv-piv-i-and-civ-credentials/
[14] Card Holder Unique Identifier
[15] The linear bar code exists unchanged in its content on Legacy TWIC and NEXGEN TWIC cards. See Part 2 section 1.4, page 9 for the image of the back of the two types of TWIC cards.

4.2 Overview of the TWIC Eco-System

Figure 1 below indicates the limit between the responsibilities of TSA over the TWIC card and where a given Maritime site must make decisions on how to use the TWIC card for access. This Part provides guidance for maritime sites on the various possible uses of the TWIC card as well as indications on how to select/install/use a reader connected to an access control system able to use the TWIC card as the access token.

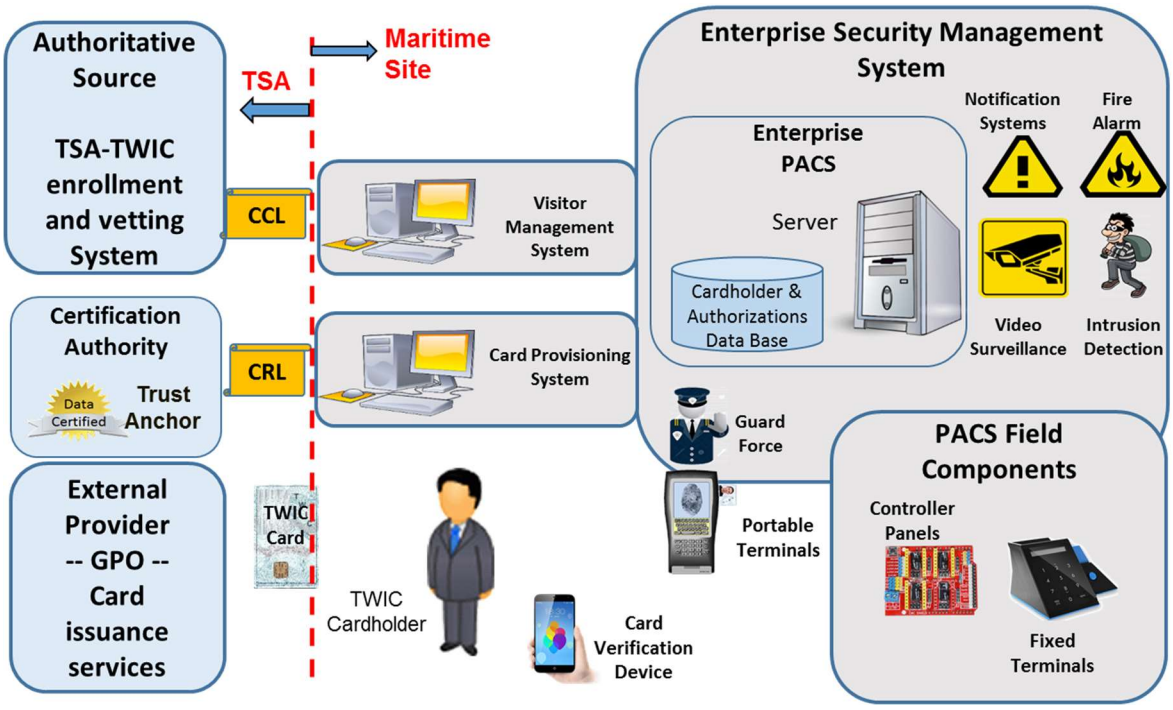


Figure 1- The TWIC Eco System

First, this document will present the functional use of the TWIC card for access, without direct physical consideration of the access control system (or reader) implementation and in a second part, present the various readers (or sub-systems) which could be used in a TWIC Access Control System from their hardware standpoint.
Note: CCL, CRL as well as the VCCL are updated by the TSA system once a day, every morning.

4.3 Certificate Validation System

All cards using the NIST SP 800-73 data model must be verified using cryptographic mechanisms to ensure that the card issuer is trusted, that the card has not been altered or invented, and that all data objects in the card belong to the same cardholder.

These cryptographic operations (certificate verifications, digital signatures checks, CRL checks, Card active challenges, etc.) must be executed as fast as possible (to minimize the delay perceived by the user when using the card). This specific processing may be done in every reader, but for cost and efficiency reasons, some PACS configurations do have one (or more) Certificate Validation System(s) shared by all readers. Figure 2 - Generic TWIC Access Control System in Page 36 of this document shows the generic functions requires in a TWIC PACS, including the Certificate Validation System.

At the functional level (first sections of this document), no hypothesis is made about where or by which physical element of the system is executing the required function.

4.4 Modes of Operation of the TWIC Card

This section describes the various modes of operations of a TWIC card used in a TWIC reader at a functional level. TWIC readers may claim one or more mode of operation(s) listed in this section.

Notes:

- For completeness, the "Flash Pass/Visual Inspection" mode is described in this section even though it does not require a TWIC reader, but only an operator. As such this mode cannot be claimed by a reader.
- A new mode (called Mode 0) is introduced in this specification for both Legacy and NEXGEN TWIC cards. It does not verify the card per say but provides verification that an unexpired TWIC card has not been canceled. This mode uses the Card Identification Number (CIN) and is an application available on iOS and Android Smartphones (the application name is ADVISR©) and could also be easily implemented in a computer using EXCEL for example.
- Only four modes (Mode 1 to Mode 4) were described in the previous TWIC documentation. These four electronic modes do not require an operator. These modes are available with both Legacy TWIC and NEXGEN TWIC cards.
- Two new modes (Mode 5 and 6) are available with NEXGEN TWIC cards and are not available when using Legacy TWIC cards[16]. These two modes most likely require an operator (local or remote) to verify the cardholder picture displayed by the TWIC Reader or on the screen of a device to which it is connected. The verification could also be done by an automated biometric verification system.
- For all TWIC cards, this set of specifications presumes that Personal Identification Numbers (PINs) are not a requirement for verification or authentication at any MARSEC level. However, the PIV Card Application PIN may be asked for presentation when TWIC Legacy cards are registered in the PACS system, and the cardholder picture is to be used (see Part 4).
- Some modes of operation may require that the TWIC card be pre-registered in the PACS. Guidance about TWIC card registration is provided in Part 4 of this series of documentation (TWIC registration and TWIC card use by a PACS)
- For some modes of operation, the TWIC reader (or the back end it is connected to) will need to have the knowledge of the TWIC Privacy Key (TPK) to decipher the personal information related to the cardholder obtained from the card. There are four different ways to obtain the TPK in the TWIC reader itself:
    - For Legacy TWIC Cards, by reading the magnetic stripe on the back of the card (not available with NEXGEN TWIC cards)
    - For NEXGEN TWIC cards, by reading the two-dimensional (2D) bar code (PDF[17] 417) on the back of the card (not available with Legacy TWIC cards). It must be noted that the linear one-dimensional (1D) bar code containing the Card Identification Number (CIN) exists unchanged on both types of cards (Legacy & NEXGEN).
    - For both types of cards, the TPK can be obtained by using the card contact interface and accessing data object tag 0xDFC101 which also contains the TPK information.
    - For TWIC Readers connected to a PACS (or a back-end in which the card is registered), where the TPK has been previously stored in the PACS database during registration and indexed by the card FASC-N. In this case, the reader can retrieve the TPK from the

[16] Unless the cardholder picture has been stored in the back end system at registration.
[17] Portable Data File format 417 for two-dimensional bar codes

PACS for a given card (e.g. using the card FASC-N as an index for the PACS) when the card is presented. This works for both type of cards (Legacy TWIC and NEXGEN TWIC).

Warning: *The description of modes of operation of readers using TWIC cards in the next sections has nothing to do with a "right for access". The legitimacy of the access request to a given location by the cardholder is completely under the authority of the maritime facility or vessel operator where the cardholder is attempting to access.*

Legacy TWIC cards have 6 Modes of operations:

- Manual Mode - Flash Pass/Visual Inspection (no device involved)
- Mode 0 - Supplement to Visual Inspection (STVI)
- Mode 1 - CHUID Verification
- Mode 2 - Active Card Authentication
- Mode 3 - CHUID Verification and Biometric Verification
- 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)[18]
- Mode 1 - CHUID Verification
- Mode 2 - Active Card Authentication
- Mode 3 - CHUID Verification and Biometric Verification
- Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric Verification
- Mode 5 - CHUID Verification and Reference Picture Verification (RPV)
- Mode 6 - CHUID Verification and Reference Picture Verification and Active Card Authentication

Note: Modes 5 and 6 are available only on NEXGEN TWIC cards. These modes could technically be achieved with Legacy TWIC cards by storing the cardholder picture extracted from the PIV Data Model card application (protected by the PIV card Application PIN) during back-end system registration and displayed upon card presentation using the FASC-N as an index into the back end system database.

4.4.1 Manual Mode - Flash Pass/Visual Inspection

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

1. the card looks legitimate (printed security features, card aspect, etc.),
2. the cardholder picture printed on the card is the same as the cardholder live image, and
3. 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[19].

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

[18] An Application called TWIC ADVISR is available on IOS and Android smartphones for this mode.
[19] There are an average of 150,000 cards on the canceled card list which makes the manual detection of a card on the CCL nearly impossible.

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

In addition to a Flash Pass/Visual Inspection verification, a Card Verification Device 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 using the CIN printed (in clear text and in a bar code) on the back of TWIC cards.

The operator using a Card Verification Device Must:

1. verify that the card looks legitimate (printed security features, card aspect, etc.),
2. verify that the picture printed on the card is the same as the cardholder live image,
3. verify that the validity date printed on the card has not passed,
4. The Card Identification Number (CIN) found on the back of a TWIC card shall be entered in the Card Verification Device, either manually by the operator on the Card Verification Device or read by the Card Verification Device using the one-dimensional bar code on the back of a TWIC card (same for Legacy TWIC and NEXGEN TWIC cards).
5. The Card Verification Device shall then verify the CIN is not canceled by using the Visual CCL list[20] which has been downloaded/updated recently.
6. As a result of the verification, the CVD will tell the operator if the card has been canceled.

This mode is considered as providing a very low-level user authentication.[21]

4.4.3 Mode 1 - CHUID Verification

The TWIC Reader uses the TWIC Card Holder Unique Identification Number (CHUID) to verify authenticity and that the card is not expired or canceled. This mode is available on both Legacy TWIC and NEXGEN TWIC cards.

Mode 1 provides a verifiable identification factor, but no biometric link to the person presenting the card and no assurance of the authenticity of the card and/or its issuer. As such, CHUID verification is considered as a very low-level of assurance as it does not involve any authentication. If the CHUID digital signature is verified and registered in the PACS, then subsequent verification of the CHUID digital signature during access is not required; otherwise, the CHUID digital signature shall be completely verified each time it is accessed from a TWIC card.

The CHUID is a freely readable data object that is digitally signed (to prevent such a number from being modified or invented by a non-authorized party) but is neither enciphered nor strongly bound to the physical card or the cardholder (it can be copied easily). The signed object contains a unique Federal Agency Smart Credential Number (FASC-N) identifier, which should be used as the primary identification number for the card. The FASC-N may be found in the signed CHUID data object (tag 0x5FC102) or the unsigned CHUID data object (tag 0x5FC104) as well as in all digitally signed data objects in the card.

Before using a CHUID (or the FASC-N it contains) for the first time, the digital signature of the issuer shall be verified to ensure that the credential number is not altered or invented and that the card was issued by TSA. This verification may take place when the CHUID is downloaded from a trusted source to the PACS for insertion in the authorized CHUID access control list (a whitelist in the PACS) or may be

[20] The Visual CCL application contains the Card Identification Numbers (CINs) of active but canceled TWIC cards. The CIN is printed on the back of every TWIC card and encoded in the linear bar code. This Visual CCL list is different from the CCL which uses the FASC-N, number which can only be read electronically as the FASC-N is not printed on a TWIC card.
[21] This mode, called TWIC® ADVISR is available as a free application for iOS and Android smartphones.

done when the CHUID of a new worker is registered in the PACS, or at the first time a CHUID is used by a PACS. Under no condition should a CHUID be used if its digital signature has never been verified by the PACS or a TWIC reader attached to the PACS.

The first time a CHUID is used (or stored) in a PACS system (registration, download, or first use), the digital signature shall be verified.

The following steps apply to a TWIC reader operating in signed CHUID Mode.

1. TWIC reader shall select the TWIC card application[22].
2. TWIC reader shall retrieve the entire contents of the digitally signed CHUID data object.
3. TWIC reader shall decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the card issuer's digital signature certificate for the document signer (guaranteeing the CHUID was created by an accredited issuer) that is used to verify the signed objects on the card.
4. If a TWIC reader is configured for expiration checking using the signed CHUID, the date encoded in the signed CHUID data object shall be compared to the current date/time. If the expiration date encoded in the signed CHUID data object is before the current date/time, the reader shall reject the card. If the TWIC reader is not equipped to check the expiration date of the TWIC card, this verification shall be done by the back-end system to which the reader is connected.
5. The TWIC reader verifies that the *id-TWIC-content-signing* object identifier is present in the card issuer's digital signature certificate for the document signer. If the *id-TWIC-content-signing* object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC reader shall reject the card. If the TWIC reader does not do this verification, it shall be done by the back-end system to which the reader is connected.
6. The TWIC reader shall verify the CHUID signature and origin up to and including the trust anchor (i.e. the TWIC Root). If this verification has been performed by the back-end system when the card was registered, the TWIC reader may not be required to do so[23].
7. The TWIC reader shall search the CHUID object to find the FASC-N tagged (0x30) value.
8. The TWIC reader shall decode the FASC-N Tag-Length-Value (TLV) record and extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue. If connected to a back-end system, the TWIC reader may transmit data in a method prescribed by the security system controller/panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N allowing the card to be uniquely identified.
9. If the TWIC reader is configured to use the TWIC Canceled Card List to check for card revocation using the signed CHUID, the TWIC reader checks if the FASC-N from the signed CHUID data object is listed on the latest version of the CCL accessed by the reader. If the FASC-N from the signed CHUID data object is listed on the latest version of the CCL accessed by the reader, the TWIC reader shall reject the presented card. If the TWIC reader does not verify if the card is on the CCL, the back-end system to which it is connected shall do so.

[22] Instead of selecting the TWIC card application, the same level of verification can be achieved by selecting the PIV card application in the TWIC card as long as the FASC-N and the root of trust (digital signatures) do indicate the card application was indeed issued by TSA. In this case, this mode is called "alternate Mode 1" and is allowed.

[23] Part of this verification should also include make sure the content signing certificate has not been revoked.

10. Alternatively, A TWIC reader may perform Unsigned CHUID signature verification using the Security Data Object. When configured for unsigned CHUID signature verification using the Security Data Object, the TWIC reader shall verify the signature and origin of the unsigned CHUID, up to and including the trust anchor using the Security Data Object.
11. When configured for unsigned CHUID signature verification using the Security Data Object, if the *id-TWIC-content-signing* object identifier is not present in the card issuer's digital signature certificate for the document signer of the Security Data Object, the TWIC reader shall reject the card.

    The TWIC reader may support use of the unsigned CHUID without signature verification for use in cases where the CHUID signature has been previously verified by and registered in the PACS.

    The following steps apply to a TWIC reader using the unsigned CHUID, with or without signature verification (this option may be deprecated in a next Release).

    1. TWIC reader shall select the TWIC card application.
    2. TWIC reader shall retrieve the contents of the unsigned CHUID data object (which contains an unsigned FASC-N along with the card expiration date).
    3. If a TWIC reader is configured for expiration checking using the unsigned CHUID, the date encoded in the unsigned CHUID data object is compared to the current date/time. If the date encoded in the unsigned CHUID data object is before the current date/time, the reader shall reject the card. If this date verification is not performed by the TWIC reader, the back-end system to which it is connected shall do so.
    4. TWIC reader searches the data object to find the FASC-N tagged (0x30) value.
    5. TWIC reader decodes the FASC-N TLV record and may retrieve the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue. The TWIC reader may transmit data in a method prescribed by the security system controller/panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N.
    6. If the TWIC reader is configured to use the TWIC Canceled Card List to check for card revocation using the unsigned CHUID, the TWIC reader checks to see if the FASC-N from the unsigned CHUID data object is listed on the latest version of the CCL accessed by the reader. If the FASC-N from the unsigned CHUID data object is listed on the latest version of the CCL accessed by the reader, the TWIC reader shall reject the presented card. If the TWIC reader is not configured to check the CCL, the back-end system to which it is connected shall perform this verification.

This mode is considered as providing a very low level of identity assurance[24].

4.4.4 Mode 2 - Active Card Authentication (ACA)[25]

This mode has a different implementation for Legacy TWIC cards and NEXGEN TWIC cards.

This mode provides a single factor authentication at the same level of security as for a PIV Data Model Card Authentication Key operation (called CAK). The FASC-N and expiration date are present in the

[24] The assurance level is low as the information verified (CHUID) is just an identifier which can be copied form one card to a cloned card and is not physically linked to the legitimate cardholder or a physical card.
[25] This mode is very similar to the PIV Card Authentication Key challenge (CAK) but requires the reader to check if the card is not on the TWIC CCL, the verification on the CRL being optional.

Card Authentication certificate which obviates the need to read the CHUID as long as the TWIC reader has the correct signing key to verify the digital signature.

In NEXGEN TWIC and Legacy TWIC Cards, in addition to the TWIC card application, every TWIC card also contains a separate application with its own application identifier (AID) that is compatible at the Data Model level with the Personal Identity Verification (PIV) specification as referenced in the NIST FIPS 201-2 standard and its associated special publications (SP 800-73, SP 800-76 and SP 800-78). The PIV Data Model card application includes a Card Authentication Key and Certificate that may be used over either the contact or the contactless interface for the purpose of authenticating that the TWIC card was issued by a trusted authority.

In NEXGEN TWIC cards, the TWIC card application contains a Card Authentication Key and its certificate that may be used over the contactless or contact interface for the purpose of authenticating that the NEXGEN TWIC card was issued by a trusted authority. As such, the use of the PIV Data Model Card application for this purpose is not required, but a similar active type of Key verification shall be done in NEXGEN TWIC cards with the TWIC card application.

Using a Key Authentication mechanism provides a strong binding between the legitimate cardholder's identity (via the FASC-N) to the physical card token by embedding a TWIC Private key in the chip (that is certified FIPS 140-2) and cannot be read/guessed/copied via any interface. This key data may be used in conjunction with the freely readable certificate to prove that the card has not been cloned or spoofed. Note that the card authentication key is defined as a local private key to the PIV Data Model application (for Legacy TWIC cards and NEXGEN TWIC cards) or the TWIC card application (for NEXGEN TWIC cards only). This key is only available after successful selection of the correct card application AID (PIV Data Model for Legacy TWIC and TWIC [or eventually the PIV Data Model] for NEXGEN TWIC).

A TWIC reader, or the system to which the TWIC reader is connected, shall support asymmetric cryptographic operations. A TWIC card is issued with the optional Card Authentication Key and Certificate as specified in NIST SP 800-73, Revision 4. The certificate profile standardizing the contents of the Card Authentication Certificate is documented by the Federal Identity Credentialing Committee's (FICC) Shared Service Provider (SSP) subcommittee[26].

A TWIC reader shall use bi-directional communication to communicate with the controller/panel or the system to which the TWIC reader is connected to. The system shall be locally configured with X.509 certificates containing the public key for all currently active Certificate Authorities (CAs) that are trusted for issuance of TWIC Card Authentication certificates. This may be limited to the issuing CAs for TSA or may include external CAs from other agencies to authenticate federated identities. This may be the same set of trusted CAs that should be stored on each TWIC reader in order to authenticate the CHUID signing certificate on a TWIC card, as required for biometric verification. The cryptographic operations performed by a TWIC reader (e.g., RSA signature verification) should be of the same type as those required by the biometric verification, and hence require an equivalent level of computing resources in a TWIC reader (e.g. a 32/64 bit embedded processor or a cryptographic co-processor).

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

A TWIC reader (or the controller/panel or system to which the TWIC reader is connected) should have access to a system clock capable of providing the current date and time. The current date and time is

[26] See the Federal Identity Management Handbook
https://www.doi.gov/sites/doi.gov/files/migrated/hspd12/upload/FederalIdentityManagementHandbook.pdf

required to determine the expiration status of a TWIC card. The verification of the credential expiration date shall be performed either by the reader, the controller/panel it is connected to or the back-end system supporting the TWIC reader.

The output of a TWIC reader, upon successful authentication, depends on the infrastructure capabilities and requirements. When card authentication is performed, the TWIC reader shall obtain the encoded FASC-N and expiration date from the Card Authentication Certificate.

The entire verified Card Authentication Certificate may be passed to the access control system for more advanced processing.

The following steps apply to a TWIC reader operating in Active Card Authentication Mode.

1) TWIC reader shall select the TWIC card application[27]
    a) If the card is a Legacy TWIC card (check of the returned AID in the Select response), then the TWIC reader shall select the PIV Data Model card application[28].
2) TWIC reader shall retrieve the content of the Card Authentication data object (tag = 0x5FC101).
3) TWIC reader shall retrieve the binary contents of the Certificate value (tag: 0x70).
4) TWIC reader shall retrieve the content of the CertInfo value (tag: 0x71).
5) If the least significant bit of the CertInfo value is '1', then the contents of the Certificate value are compressed using the "gzip" algorithm and are to be decompressed by a TWIC reader to produce the raw DER-encoded X.509 certificate. Otherwise, the contents of the Certificate value may be used without decompression. TWIC card certificates are not gzip compressed.
6) The TWIC reader shall compare the "issuer" name in the Certificate against the "subject" name in each trusted issuing CA Certificate stored on a TWIC reader. For each CA with a matching name, the Public Key is used to attempt to verify the signature on the token's Certificate. If no matching CA Certificate is found on a TWIC reader with the same name and with a Public Key that verifies the signature on the Certificate, then the reader shall reject the card containing the Certificate.
7) If a TWIC reader is configured for expiration checking using card authentication, and the date encoded in the Card Authentication Certificate's "notAfter" validity date is before the current date/time, the reader shall reject the card containing the Certificate. If the TWIC reader is not configured to check the expiration date, the controller/panel or the back end to which it is connected shall perform expiration checking.
8) If the Certificate's "keyUsage" extension does not contain the "digitalSignature" flag, the Certificate is rejected.
9) If the Certificate's "extendedKeyUsage" extension does not contain the "id-TWIC-cardAuth" keyPurposeID (1.3.6.1.4.1.29138.6.8), the Certificate is rejected.
10) The Certificate's "subjectAltName" extension identified as "twicFASC-N" (1.3.6.1.4.1.29138.6.6) name entry shall be retrieved from the certificate and used as the unique credential number (e.g. for optional transmission to a controller/panel or back-end system).

[27] Instead of selecting the TWIC card application, the same level of verification can be achieved by selecting the PIV card application in the TWIC card if the FASC-N and the root of trust (digital signatures) do indicate the card application was indeed issued by TSA. In this case, this mode is called "alternate Mode 1" and is allowed

[28] For existing qualified TWIC readers that have not been updated to recognize a NEXGEN TWIC card, they must select the PIV card application instead and, thereby, use the NEXGEN TWIC Card in backward compatibility mode.

11) If the Certificate contains any unknown extensions with the Criticality Flag set to TRUE, the Certificate is rejected.

12) The TWIC reader shall generate a random or pseudo-random challenge of at least 127 bytes of unique data and transmit this to the TWIC card using the GENERAL AUTHENTICATE Card command.

13) The response (i.e. the card's signature) from the GENERAL AUTHENTICATE Card command shall be verified using the Public Key from the Certificate. If verification of the response (i.e. the card's signature) from the GENERAL AUTHENTICATE Card command fails, the TWIC reader shall reject the card.

14) If verification has succeeded, the Certificate is accepted as an authentication factor. Identifying information (e.g. the Certificate, the FASC-N, or other unique identifying components) may be immediately used locally or at a controller/panel or backend system as input for the access control rules. Supplemental second and third factors (e.g. PIN, biometric) may be independently evaluated.

15) If the TWIC reader is configured to use the TWIC Canceled Card List to check for card revocation using card authentication, the TWIC reader checks to see if the FASC-N from the Card Authentication Certificate is listed on the latest version of the CCL accessible by the reader. If the FASC-N from the Card Authentication Certificate is listed on the latest version of the CCL accessible by the reader, the TWIC reader shall reject the presented card. If the TWIC reader is not configured to check the card identifier against the CCL, the controller/panel or the back-end system it is connected to shall do so[29].

16) If the TWIC reader is configured to use the TWIC Certificate Revocation List (CRL) to check for certificate revocation, the TWIC reader checks to see if the Card Authentication Certificate is listed on the latest version of the CRL accessible by the reader. If the Card Authentication Certificate is listed on the latest version of the CRL accessible by the reader, the TWIC reader shall reject the presented card[30].

This mode provides a good level of authentication of the authenticity of the physical card presented (one factor - what you have).

4.4.5 Mode 3 - CHUID Verification and Biometric Verification

In this mode, in addition to the CHUID verification described in Mode 1 (section 4.4.3), the cardholder's live biometric sample (fingerprint) is compared to a stored biometric reference template.

The biometric reference template may be read from a TWIC card at each use or stored in the PACS system during PACS registration of the user and indexed, for example, using the card FASC-N.

The TWIC card application (as well as the PIV Data Model card application present in the same card) contains a biometric template of fingerprint minutiae bound to the cardholder's FASC-N identifier via the digital signature of the card issuer. In addition to be digitally signed, a 128-bit symmetric AES TWIC Privacy Key, TPK, is used to encipher the biometric templates that are stored on the TWIC card. This TPK is accessible using the contact interface, or by decoding the information on the back of the card (Magnetic stripe for Legacy TWIC cards, or PDF 417 bar code for NEXGEN TWIC cards). The TPK is not available via the contactless interface, although the TPK may be retrieved via either of the following:

[29] It is recommended, but not required, to perform the CCL verification AFTER the card digital signatures has been fully verified. This enables detection of fraudulent cards presented, even if their identifier has also been placed on the CCL.

[30] Same comment for the CRL verification as for the CCL verification. By performing this verification after the integrity and authenticity of the card has been verified, it allows detection of false cards, even if they have been revoked.

The magnetic stripe (for Legacy TWIC cards), the two-dimensional PDF417 bar code on the back of NEXGEN TWIC cards, the contact interface of a TWIC card, or the back-end system that the reader is connected to if the card TPK was previously registered. This retrieval of the TWIC Privacy Key from a TWIC card may occur at every TWIC reader access transaction, or it may be obtained by a TWIC reader from the PACS where the corresponding TPK was stored as a one-time operation during card registration.

In order to confirm that the cardholder matches the stored reference biometric templates, the data shall be retrieved, deciphered, verified, and matched against the live finger presented by the cardholder.

The following steps apply to a TWIC reader operating in CHUID Verification and Biometric User Authentication Mode.

1) The TWIC reader shall perform a signed CHUID Verification (Mode 1) as defined in section 4.4.3. This step provides the Card FASC-N.
2) If the fingerprint reference template is provided by the back-end system to which the reader is connected, the next step is Step 3. Nevertheless, the following steps (a through g) shall have been executed at least once, when the fingerprint reference was initially registered in the back-end system.
    a) The TWIC reader shall select the TWIC card application.
    b) The TWIC reader shall load/retrieve the TWIC Privacy Key of the TWIC card, from local memory, a server, the magnetic stripe of a legacy TWIC card, the two-dimensional bar code of a NEXGEN TWIC card, or the contact interface of a TWIC card.
    c) The TWIC reader shall select and retrieve the contents of the fingerprint data object (tag 0xDFC103) from the card.
    d) The enciphered fingerprint template TLV (tag: 0xBC) is extracted from the fingerprint data object read in the previous step (Tag 0xDFC103).
    e) The enciphered fingerprint template is deciphered using the TWIC Privacy Key.
    f) The CBEFF[31] record is parsed into the CBEFF Header, the ANSI[32]/INCITS[33] 378 Biometric Data Block, and CBEFF Signature Block containing the FASC-N in the signature attributes[34].
    g) TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the TWIC reader have a verified copy of the document signer's X.509 digital certificate. If signature verification of the CBEFF record using the public key from this verified document signing certificate fails, the TWIC reader shall reject the card.
    h) TWIC reader compares the FASC-N from the signed CHUID with the FASC-N from the Signed Attributes of the CBEFF Signature Block. If the FASC-N from the signed CHUID and the FASC-N from the CBEFF Signature Block do not match, the TWIC reader shall reject the card.
3) TWIC reader acquires a live sample fingerprint image from the cardholder's presented finger. The TWIC reader shall convert the sampled image to a minutiae template and compare the template against the fingerprint minutiae templates stored in finger view records in the reference

[31] Common Biometric Exchange Formats Framework
[32] American National Standards Institute
[33] InterNational Committee for Information Technology Standards
[34] The structure of the header and signature blocks are defined in ANSI INCITS 398 Common Biometric Exchange Formats Framework (CBEFF) with the exact values for PIV/TWIC defined in SP 800-76.

biometric object at an appropriate level of confidence (see Appendix F). If the fingerprint does not match one of the templates on the first attempt, the TWIC reader shall prompt the cardholder for subsequent attempts without requiring the TWIC card to be read again. If the number of subsequent matching failures exceeds the readers configurable retry counter, the TWIC reader shall reject the card.

4) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number required for the access authorization process.

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

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

This mode combines Mode 2 (Active Card Authentication as described in section 4.4.4) and Mode 3 (Biometric User Authentication similar to section 4.4.5) and provides two-factor authentication. This mode requires the CHUID embedded content signing certificate to be used for the chain of trust to be validated.

When performing two-factor authentication, the biometric user authentication process described in this section varies from Section 4.4.4 in that only the document signing certificate is required to be read from the signed CHUID. The FASC-N and expiration shall be obtained during Active Card Authentication. The FASC-N obtained from Active Card Authentication shall be used to match the FASC-N found in the biometric data.

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

1) The TWIC reader shall perform an Active Card Authentication (see section 4.4.4). This step also provides the Card FASC-N.
2) If the fingerprint reference biometric template has been recorded during the card enrollment by the back-end system and is provided using the FASC-N as an index, the next step is step 3. Nevertheless, the following steps (a through g) shall have been executed at least once, when the fingerprint reference was initially registered in the back end system.
    a. TWIC reader shall load the TWIC Privacy Key of the TWIC card, from local memory, a server, the magnetic stripe of a Legacy TWIC card, the two-dimensional bar code of a NEXGEN TWIC card, or the contact interface of a TWIC card.
    b. TWIC reader shall select the TWIC card application in a TWIC card.
    c. TWIC reader shall select and get the contents of the fingerprint data object (Tag 0xDFC103).
    d. The enciphered fingerprint template TLV (tag: 0xBC) shall be retrieved from the fingerprint data object.
    e. The enciphered fingerprint template shall be deciphered using the TWIC Privacy Key.
    f. The CBEFF record shall be parsed into the CBEFF Header, the ANSI[35]/INCITS[36] 378 Biometric Data Block, and CBEFF Signature Block containing the FASC-N in the signature attributes

[35] American National Standards Institute
[36] InterNational Committee for Information Technology Standards

g. TWIC reader shall retrieve the document signer's certificate from the CHUID signature field, since the CHUID is signed by the same entity as the biometric.

h. TWIC reader shall verify that the *id-TWIC-content-signing* object identifier is present in the card issuer's digital signature certificate for the document signer. If the *id-TWIC-content-signing* object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC reader shall reject the card.

i. TWIC reader shall verify the CBEFF signature and origin up to and including the trust anchor. If signature verification of the CBEFF record using the public key from the verified document signing certificate fails, the TWIC reader shall reject the card.

j. TWIC reader compares the FASC-N from Card Authentication Certificate with the FASC-N from the Signed Attributes of the CBEFF Signature Block. If the FASC-N from the Card Authentication Certificate and the FASC-N from the CBEFF Signature Block do not match, the TWIC reader shall reject the card.

3) TWIC reader acquires a fingerprint image from the cardholder's presented finger. The TWIC reader shall convert the sampled image to a minutiae template and match the template against the fingerprint minutiae templates stored in finger view records in the signed biometric object at an appropriate level of confidence (see Appendix F). If the fingerprint does not match one of the templates on the first attempt, the TWIC reader shall prompt the cardholder for subsequent attempts without requiring the TWIC card to be read again. If the number of subsequent matching failures exceeds the readers configurable retry counter, the TWIC reader shall reject the card.

4) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number required for access authorization. This value shall match the FASC-N from any other authentication factors that are matched to know that they are bound together by the card issuer

This mode provides a very good level of authentication with two authentication factors (Who you are and what you have).

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

This mode combines a verification of the CHUID information and its signature (Mode 1), and a verification of the legitimate cardholder digital picture. It requires an operator. This mode also requires the CHUID embedded content signing certificate to be used for the chain of trust to be validated.

The procedure described here extracts the reference picture form the card (NEXGEN TWIC cards only), but could also be used with a Legacy TWIC card given that the reference cardholder picture could be stored in the PACS during registration and retrieved using the card FASC-N as an index.

To confirm that the cardholder's face matches the previously stored legitimate cardholder picture, the data shall be retrieved, deciphered, verified, and displayed on a screen for an operator to verify against the person's face presenting the card (i.e. live biometric).

1) The TWIC reader performs signed CHUID Verification as defined in section 4.4.3. This step provides the FASC-N of the card presented.

2) If the cardholder picture has been stored when the card was registered in the system's back end, the reference cardholder picture is to be retrieved from the system's data base using the FASC-N as an index, and the next step is then Step 3.[37]

    a. The TWIC reader shall load the TWIC Privacy Key from a TWIC card from local memory, a server, the two-dimensional bar code of a NEXGEN TWIC card, or the contact interface of a TWIC card.

    b. The TWIC reader shall select the Cardholder Facial Image data object (tag 0xDFC108).

    c. The TWIC reader shall retrieve the contents of the Cardholder Facial Image data object (Tag 0xDFC108).

    d. The enciphered Facial Image TLV (tag: 0xBC) shall be retrieved from the Cardholder Facial data object.

    e. The enciphered Facial Image shall be deciphered using the TWIC Privacy Key.

    f. The CBEFF record shall be parsed into the CBEFF Header, the ANSI/INCITS 385 Facial Image Record, and CBEFF Signature Block containing the FASC-N in the signature attributes.

    g. The TWIC reader shall retrieve the document signer's certificate from the CHUID signature field, since the CHUID is signed by the same entity as the Facial Image Data object.

    h. The TWIC reader shall verify that the *id-TWIC-content-signing* object identifier is present in the card issuer's digital signature certificate for the document signer. If the *id-TWIC-content-signing* object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC reader shall reject the card.

    i. The TWIC reader shall verify the CBEFF signature and origin up to and including the trust anchor. If signature verification of the CBEFF record using the public key from the verified document signing certificate fails, the TWIC reader shall reject the card.

    j. The TWIC reader shall compare the FASC-N from the CHUID with the FASC-N from the Signed Attributes of the CBEFF Signature Block. If the FASC-N from the CHUID and the FASC-N from the CBEFF Signature Block do not match, the TWIC reader shall reject the card.

3) TWIC reader displays on a screen (local or remote) the reference picture from the card (or from the back end) for an operator (or an automated biometric verification system) to compare with the live image of the cardholder presenting the card. If the reference picture displayed does not match the cardholder, the operator/system shall deny access to the cardholder.

The reference cardholder picture may be extracted from the card itself (TWIC NEXGEN cards only), or provided by the PACS if the information was stored in the PACS data base when the card was registered (Legacy TWIC as well as NEXGEN TWIC cards).

This mode, which requires an operator (or an automated biometric verification system), provides a good level of user authentication (One Factor – who you are).

[37] It is important to note that this mode may also be used with a Legacy TWIC card if the cardholder picture has been extracted from the PIV Data Model card application during registration. Otherwise, this would require entry of the PIV Application PIN in Legacy TWIC cards and the use of the contact interface only.

4.4.8 Mode 6 – CHUID Verification and RPV and ACA

This mode involves an operator (or an automated biometric verification system) and provides two factors of authentication. It combines the CHUID verification (Mode 1), the Card Authentication (Mode 2), and as explained in Mode 5, it displays the reference picture of the legitimate cardholder, allowing an operator to authenticate the person presenting the card. This mode also requires the CHUID embedded content signing certificate to be used for the chain of trust to be validated.

When performing two factor authentication, the Facial Image Verification process described in this section varies from Section 4.4.3 in that only the document signing certificate is required to be read from the signed CHUID. The FASC-N and expiration shall be obtained during Active Card Authentication. The FASC-N obtained from Active Card Authentication shall be used to match the FASC-N found in the Cardholder Facial Image data.

In order to confirm that the cardholder face matches the stored legitimate cardholder picture, the data shall be retrieved, deciphered, verified, and displayed on a screen for an operator to verify the cardholder's face.

1) TWIC reader performs an Active Card Authentication (see section 4.4.4).
2) TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the two-dimensional bar code of a NEXGEN TWIC card, or the contact interface of a TWIC card.
3) TWIC reader selects the TWIC card application in a TWIC card.
4) TWIC reader selects and retrieves the contents of the Cardholder Facial Image data object (Tag 0xDFC108).
5) The enciphered Facial Image TLV (tag: 0xBC) is retrieved from the Cardholder Facial data object.
6) The enciphered Facial Image is deciphered using the TWIC Privacy Key.
7) The CBEFF record is parsed into the CBEFF Header, the ANSI/INCITS 385 Facial Image Record, and CBEFF Signature Block containing the FASC-N in the signature attributes.
8) TWIC reader retrieves the document signer's certificate from the CHUID signature field, since the CHUID is signed by the same entity as the facial image data object.
9) TWIC reader verifies that the *id-TWIC-content-signing* object identifier is present in the card issuer's digital signature certificate for the document signer. If the *id-TWIC-content-signing* object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC reader shall reject the card.
10) TWIC reader shall verify the CBEFF signature and origin up to and including the trust anchor. If signature verification of the CBEFF record using the public key from the verified document signing certificate fails, the TWIC reader shall reject the card.
11) TWIC reader compares the FASC-N from Card Authentication Certificate with the FASC-N from the Signed Attributes of the CBEFF Signature Block. If the FASC-N from the Card Authentication Certificate and the FASC-N from the Signature Block do not match, the TWIC reader shall reject the card.
12) TWIC reader displays on a screen (local or remote) the reference picture from the card for an operator to compare with the cardholder presenting the card. If the reference picture

displayed does not match the live image of the cardholder, the operator shall deny access to the cardholder.

As mentioned in Mode 5 (section 4.4.7), the cardholder reference picture could also have been stored in the PACS when the card was registered for a similar mode. In such case, steps 2 to 11 could be bypassed.

This mode, which requires an operator (or an automated biometric verification system), provides a very good level of authentication (two factors: Who you are and what you have).

4.5 Card Reader Types

This documentation considers different types of readers that may be used to verify the user's TWIC card. They are:

- **Card Verification Device:** This device may be a computer, a tablet, or a smart phone, and does not interface electronically with the TWIC card. This type of "reader" is mentioned in this documentation only for completeness, but as it does not interact with the chip of the TWIC card, it is not described/used outside of Mode 0 (the only mode, beside the flash pass mode, which supports a non-electronically functioning TWIC card).
- **TWIC readers** – These are readers able to communicate with a TWIC card electronically, using either the contact or contactless interfaces. This generic term is used when a functionality of the reader is described which does not depend on a specific instance of the physical reader. The specific instances of TWIC readers described in this document are:
    - **Fixed Physical Access Control Reader** – a TWIC reader installed in a wall, turnstile or similar type installation. It typically communicates with an external access control system to control a door, gate, turnstile, etc. Fixed TWIC readers may operate in indoor environments or in outdoor environments exposed to the weather. There are two types of fixed readers:
        - **Network Attached** (see section 5.2) or
        - **Standalone** (see section 5.3)
    - **Portable Verification Reader** – is a handheld TWIC reader that may be used for portable, spot-check identity verification. A portable TWIC reader may be attached to a network (see section 5.4) or be a portable TWIC reader with no permanent network connectivity as described in section 5.4.

Summary of reader types described in this document:

TWIC Readers	Bi-directional communication	Limited communication
Fixed Reader	Network attached (section 5.2)	Standalone (section 5.3)
Portable Reader	Network connected (section 5.4)	No connectivity (section 5.4)

- **Example of other type of readers able to work (in some modes) with TWIC cards but not described in this document:**
    - NFC Enabled Smart Phones
    - PIV APL approved readers

4.6 Optional TWIC Reader Features

TWIC readers may have specific features required for one mode of operation or another. They are listed hereafter as features a TWIC reader manufacturer needs to (or may) claim depending on its type.

Bar Code reader - Linear: In all TWIC cards, a linear bar code on the back of the card provides the Issuer Identification Number and Card Identification Number (IIN and CIN).

Bar Code reader – PDF 417: In this next generation of cards (NEXGEN TWIC), an additional two-dimensional bar code provides more information which could be used by the reader to access/decipher some personal information stored in the card, as well as retrieve the card TPK).

Biometric Sensor - Fingerprint: When the reader is used in a biometric mode (fingerprint verification), the reader shall have a biometric sensor attached to it in order to capture an image of the user's presented fingerprint. TWIC readers with a fingerprint capture device should have a finger guide to aid in proper finger placement on the sensor. For biometrically enabled TWIC readers, the fingerprint sensor should be embedded in the same chassis as the TWIC reader. If a separate fingerprint sensor module is used, the wiring between the TWIC reader and the biometric unit shall not be exposed.

Camera: In some PACS, the access control system uses the cardholder facial image to verify the user's identity. When the TWIC reader is used to provide the user's identifier (e.g. the card FASC-N), the PACS is able to verify the captured video image matches the legitimate cardholder picture, either extracted from the card, or previously stored during enrollment. The camera may be separated from the reader and not connected at all to the reader itself.

Contact Interface: For TWIC readers interacting with a TWIC card using the contact interface, the reader shall have an interface accepting cards compliant with the contact requirements defined in ISO/IEC 7816 (parts 2, 3 and 4). It is highly recommended that the reader support negotiable communication protocol speeds allowing the reader and the card to communicate at the highest possible communication speed.

Contactless Interface: For TWIC readers interacting with a TWIC card using the contactless interface, the reader shall have an interface accepting cards compliant with the contactless requirements defined in ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-2. The maximum card read range shall not be more than 10 centimeters. Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s, dependent on the contactless card communications speed capabilities. If two or more contactless smart cards are presented at the same time in a TWIC reader's contactless field, the TWIC reader shall reject all the cards presented. These readers also shall comply with ISO/IEC 7816-4 for the application layer.

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

Display: The display allows the reader to interact with (or inform) the operator or the cardholder.

Pin-Pad/Keyboard: Some TWIC readers may be required to have a PIN-Pad (or a keyboard) allowing an operator or a cardholder to interact with the reader software.

Secure bi-directional communication interface: A TWIC reader may be connected to a back-end system, allowing to download information (e.g. CCL); it may also have a bi-directional communication interface allowing it to query information from the controller/panel/back-end system about the specific card presented. For example, the reader could send the card FASC-N to the back-end system requesting information such as: "has the card structure been already verified?" or "Is this card canceled?", or "What is the cardholder picture associated with this card?", and so on.

Visible indicators: All TWIC readers shall have visible indicators providing information about the reader status and its interactions with the card presented. At a minimum, indications such as "power on", "card detected" and/or "communicating with card", shall be present. Optionally in

the absence of a display, more information with more indicators (or blinking indicators) could be useful to indicate malfunctions such as “communication with back end lost”, “Power too low”, etc.

Wireless interface: readers may be connected to a back end (PACS or even a server) using a wireless interface. This interface may be a standard Wi-Fi RF communication, or a non-standard type of RF communication, but in any case, the exchange of information shall be encrypted and protected against cyber-attacks.

4.7 Operational Requirements for All TWIC Readers:

1. TWIC readers shall identify TWIC cards using at least the 3 data elements of the FASC-N [38] (Agency code – System code – Credential Number).
2. TWIC Readers shall verify the expiration date of a TWIC card by extracting the information from the CHUID, and after verifying its digital signature.
3. TWIC readers should have visible indicators showing clearly and continuously display power status (on, ready or out of service).
4. TWIC readers may contain additional user visible (or audible) indicators such as lights, text messages, and audible indicators.
5. TWIC reader visual indicators shall be visible in daylight.
6. TWIC readers shall allow for future functional enhancements to be added in the field. A mechanism should be provided that assures that only authorized/authenticated firmware/software updates are permitted.
7. TWIC readers may support a means of alerting the PACS/operator (or owner of the device) if the TWIC reader detects tampering.

[38] The FASC-N identifies the unique **user credential identifier** loaded in each card which is physically identified by its CIN (Card Identifier Number).

5. Physical Access Control

The following sections cover only Physical Access Control Systems and the readers which are connected to them (either fixed, or portable).

The term "Physical Access Control System" (PACS) is used in these sections when a functional requirement encompasses not only the reader itself, but some of the back-end devices the reader is connected to (Controller/Panel, Certificate Validation System, etc.).

TWIC cards have been designed for physical access control in which the cardholder is biometrically authenticated. No PIN ("what you know" factor) is considered in any of the access modes or the use of TWIC cards in this document[39].

The following sections consider automated access control without any operator being involved in the authentication or access **decision process** (even if it is a portable device controlled by an operator). As such these sections do not address Manual Mode, Mode 0, Mode 5 or Mode 6 which all require an operator (or a biometric verification automated system) decision.

Nevertheless, if one of the TWIC readers described hereafter (fixed or portable) is able to be used in Mode 5 (CHUID verification and Electronic Visual Verification) or Mode 6 (CHUID Verification and Electronic Visual Verification and Active Card Authentication), the manufacturer may claim such a mode in which an operator/system verifies the result provided by the reader such as "reference picture displayed (on the card or on the device) is valid". Such a reader shall also verify the content signing expiration date included in the CHUID.

5.1 Access Control System Overview

Figure 2 below, Generic TWIC Access Control System, provides a graphical view of the relationship between a physical access control system (as a whole), a biometric sub-system boundary, a biometric TWIC reader, the Certificate Validation sub-system as well as the cancellation verification sub-system. This is a generic diagram and specific implementations may vary from this particular depiction. Key elements of Figure 2 are described in Table 4.2 below.
Generally, a TWIC card is used at a door or gate that may or may not be attended. Either the ISO/IEC 14443 contactless interface (or ISO/IEC 7816-2 & ISO/IEC 7816-3 contact interface) shall be used to transfer the Card unique ID number assigned to the cardholder (FASC-N) as well as the reference biometric data between a TWIC card and a TWIC reader. The cardholder biometric template stored on a TWIC card is enciphered with a key unique to each TWIC card and remains enciphered during transmission to a TWIC reader over the contactless or contact interface. The key required to decipher the reference biometric template of the user, called the TWIC Privacy Key (TPK), shall be obtained from one of several sources. These sources include the magnetic stripe encoded on each Legacy TWIC card, the two-dimensional bar code (PDF417) printed on the back of TWIC NEXGEN cards, the TWIC card memory (but only accessible through the contact interface) or from the physical access control system where the TPK has been previously registered during enrollment.

[39] The PIV Application PIN may be required for PACS registration of Legacy TWIC cards. See Part 4 of this series of documents for guidance.

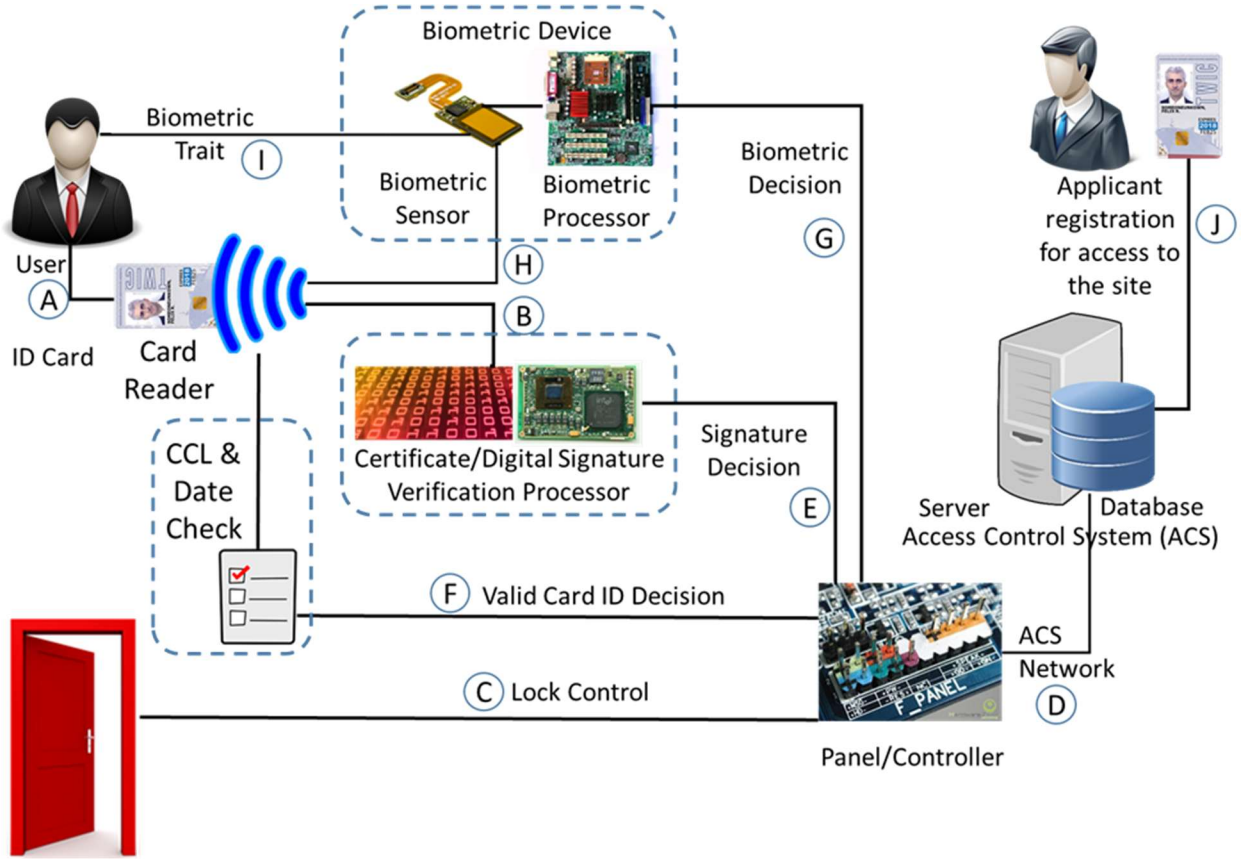


Figure 2 - Generic TWIC Access Control System

Key	Description
A	TWIC card presented by the user to the Card reader to claim an identity and access.
B	User identity code (CHUID) read from the TWIC card by the Card reader and sent to the Certificate/Digital Signature Verification Processor to validate the trust in the ID Card. This also could be an Active Card Authentication using the CAK if a higher level of assurance is required.
C	Electrical signal from the controller/panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy PACS).
D	PACS Network: Communication channel (Ethernet, RS-485, etc.) enabling data interchange between the controller/panel, PACS processor and database. Communication protocols used depends on site-specific implementation and includes user identity code data from the controller/panel as well as user access authorization data from the PACS server.

E	YES/NO indication (electrical signal or message) from the signature verification processor to the Panel/Controller conveying the result of the data identifier (or card authentication) verification/authentication trust process.
F	YES/NO indication (electrical Signal or message) from the Date & Card Cancelled List verification sub-system conveying the result about card validity (not canceled and not expired).
G	YES/NO indication (electrical signal or message) from the biometric processor to the Panel/Controller conveying the result of the user verification/authentication process.
H	User digitally signed biometric reference template of the legitimate cardholder read from the TWIC Card by the Card reader and sent to the biometric processor as reference to compare with the biometric trait measured from the cardholder (see I).
I	Biometric characteristic of the cardholder presented to the biometric sensor during an access transaction (fingerprint). This may also include interactions between the user and sensor such as indicator lights or audio cues.
J	Applicant-supplied biographic information (Card Identifier/CHUID, name, address, etc.) obtained during PACS registration via the PACS processor. For some systems, this may include a picture of the cardholder taken during enrolment.

5.2 Network-Attached TWIC Reader

A network-Attached TWIC reader[40] shall support two-way communication between the reader and the physical access control system back end. It could be a fixed reader, or a portable reader, but it is always a reader connected to a back-end system which can:

- Retrieve information from the back-end system about the card (or the user) captured during an initial enrollment.
- Provide the OK to the back-end system after all verifications have been performed to open the gate/door allowing the user access to the controlled area.
- Rely on the back end to make a decision about the user/card being authorized to access the physical location.

The requirements for a Network-Attached TWIC reader are:

- It shall be able to interact with a TWIC card using a standard ISO/IEC 14443 contactless interface.
- It shall claim one or more of the four identification/authentication modes:
  - Mode 1 - CHUID Verification (section 4.4.3),
  - Mode 2 – Active Card Authentication (section 4.4.4),
  - Mode 3 – CHUID Verification and Biometric Verification (section 4.4.5),

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

- Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric User Authentication (section 4.4.6)

- It shall be able to perform a biometric fingerprint capture and a biometric match if modes 3 or 4 are claimed.
- It shall be able to display, or send to a display, or ask the back end to display, the legitimate cardholder picture to an operator if Modes 5 or 6 are claimed by the reader.
- It shall be able to be securely configured (locally or remotely) to operate at the current security level at which the facility operates (adaptation to a given MARSEC level), or it shall be disabled for access by the back-end system to which it is connected.

Requirements for the back-end system supporting a Network-Attached TWIC reader:

- If the reader does not check the card FASC-N of the presented card against the CCL, the back-end shall perform this function.
- If the reader does not check the expiration date of the card presented, the back-end shall perform this function.
- If the reader does not verify the digital signatures of the various data objects used in an authentication process, the back-end shall perform this function.[41]
- If the reader cannot operate at the current security level required at a given time, the back-end system should indicate that the reader is disabled.

Options that may be claimed by a Network-Attached TWIC reader:

- Interface with the TWIC card using a contact interface.
- The manufacturer may claim one, or both of Modes 5 and 6:
    - Mode 5 - CHUID Verification and Electronic Visual Verification (section 4.4.7)
    - Mode 6 - CHUID Verification and Electronic Visual Verification and Active Card Authentication (section 4.4.8)
- Retrieving information from the back-end system to which it is attached (controller/panel or PACS), such as:
    - Current Date and Time if the reader verifies the card expiration date.
    - Recent CCL, if the reader checks the card FASC-N against the CCL.
    - The cardholder's picture if stored in the back-end system when the cardholder is enrolled, allowing the TWIC reader to potentially also claim Authentication Modes 5 and/or 6 on all cards (Legacy as well as NEXGEN TWIC cards).
    - The card TPK corresponding to a given FASC-N, if not retrieved directly from the card itself, by reading the TWIC Card Application Data Object 0xDFC101.

5.3 Standalone TWIC Reader

A standalone TWIC reader is a reader that does not have a two-way communications channel available, or which is connected to a PACS through a one-way communications connection.

[41] This verification may be done every other time when a card is presented, or once when the card is registered in the PACS.

It could be a fixed reader, or a portable reader, but it is a reader connected to a back-end system which can:

- Provide enough information to the back-end system after all local reader verifications have been performed to open the gate/door for user access to the location.
- Rely on the back-end system to make a decision about the user/card being authorized to access the physical location.

With such a reader, when a TWIC card is presented using the contactless interface, the TWIC Privacy Key shall be read from the card either using the magnetic stripe on Legacy TWIC cards or the two-dimensional bar code (PDF417) on the back of NEXGEN TWIC cards. If the card is used in contact mode, the TPK can be read directly from the card in the TWIC Card Application Data Object 0xDFC101.

The requirements for a Standalone TWIC reader are:

- It shall be able to interact with a TWIC card using a standard ISO/IEC 14443 contactless interface or ISO/IEC 7816 contact interface.
- It shall perform one or more of the four identification/authentication modes:
  - Mode 1 - CHUID Verification (section 4.4.3),
  - Mode 2 – Active Card Authentication (section 4.4.4),
  - Mode 3 – CHUID Verification and Biometric Verification (section 4.4.5),
  - Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric User Authentication (section 4.4.6)
- It shall be able to perform a biometric fingerprint capture and a match if Modes 3 or 4 are claimed.
- It shall be able to display, or send to a display, or ask the back-end to display, the legitimate cardholder picture to an operator if Modes 5 or 6 are claimed by the reader.
- It shall be able to be securely configured (locally or remotely) to operate at the current security level at which the facility operates (adaptation to a given MARSEC level), or it shall be disabled for access by the back-end system to which it is connected.

Requirements for the back-end to which a standalone TWIC reader is connected:

- If the reader does not check the FASC-N of the card presented against the CCL, the back-end system shall perform this function.
- If the reader does not check the expiration date of the card presented, the back-end system shall perform this function.
- If the reader does not verify the digital signatures of the various data objects used in an authentication process, the back-end system shall perform this function.[42]
- If the reader cannot operate at the current security level required at a given time, the back-end system should indicate that the reader is disabled.

[42] This verification may be performed every other time when a card is presented, or once when the card is registered in the PACS.

Options that can be claimed by a Standalone TWIC reader manufacturer:

- Interface with the TWIC card using a contact interface to retrieve the card TPK corresponding to the card FASC-N by reading the TWIC Card Application Data Object 0xDFC101.
- One of the two facial picture authentication modes:
    - Mode 5 - CHUID Verification and Reference Picture Verification (section 4.4.7)
    - Mode 6 - CHUID Verification and Reference Picture Verification and Active Card Authentication (section 4.4.8)

5.4 Portable Identity Verification with No Connectivity in Operation

A handheld portable TWIC reader may also be used to verify worker credentials in a mobile environment with no connectivity (Standalone Reader). This may be in conjunction with or as a substitute for the fixed access control TWIC readers described above. Smaller installations may not have, nor need, a complete physical access control system. In this case, a portable TWIC reader should provide an alternate means of identity verification. A Portable TWIC reader is presumed to be attended and operated by a qualified verification agent.

A portable TWIC reader (often called handheld) can be used in at least two operational settings:

- At a gate control location to interrogate credentials within a vehicle with multiple occupants.
- By authorized security personnel performing a random identity verification throughout the facility.

All Portable TWIC readers shall have the features described in section 7 (Portable TWIC Reader Physical Requirements). For all modes of operations, the reader shall have a way to access a recent CCL (or Visual CCL for Mode 0) in its memory, either by connecting to a network at least once a day, or by having a CCL file loaded into the reader (e.g. USB stick). Portable TWIC readers shall also store in their memory the root(s) of trust to verify TWIC card digital signatures.

Depending on the mode(s) of operation claimed by the reader manufacturer, and the card interface used, the portable TWIC reader will require different features to be able to execute the required operations:

- **Mode 0 - Supplement to Visual Verification (STVI)** – The Card Verification Device shall have a display and a Pin-Pad (or a Keyboard) to enable manual entry of the CIN of the card. The device may optionally have (at minimum) a linear-type bar code reader if the card identification number (CIN) is to be read automatically from the back of the TWIC card.
- **Mode 1 - CHUID Verification**
    - The reader shall have a card interface (contact or contactless)
- **Mode 2 - Active Card Authentication**
    - The reader shall have a card interface (contact or contactless)
- **Mode 3 - CHUID Verification and Biometric Verification**

- The reader shall have a card interface (contact or contactless)
- If the reader has only a contactless interface, the reader shall have a means to access/retrieve the TPK from the TWIC card:
  - For Legacy TWIC cards, the TPK shall be accessed via a magnetic stripe reader
  - For NEXGEN TWIC cards the TPK shall be accessed via a two-dimensional bar code reader (PDF 417)
- The reader shall have a mean of capturing the user's fingerprint image and comparing it to the reference biometric retrieved and deciphered from the TWIC card.

- **Mode 4 - CHUID Signing Certificate and Active Card Authentication and Biometric Verification**
  - The reader shall have a card interface (contact or contactless)
  - If the reader has only a contactless interface, the reader shall have a mean to access/retrieve the TPK from the TWIC card:
    - For Legacy TWIC cards, the TPK shall be accessed via a magnetic stripe reader.
    - For NEXGEN TWIC cards, the TPK shall be accessed via a two-dimensional bar code reader (PDF 417)
  - The reader shall have a means of capturing the user's fingerprint image and comparing it to the reference biometric retrieved and deciphered from the TWIC card.
- **Mode 5 - CHUID Verification and Electronic Visual Verification**
  - The reader shall have a card interface (contact or contactless)
  - If the reader has only a contactless interface, the reader shall have a mean to access/retrieve the TPK from the TWIC card by using a two-dimensional bar code reader (PDF 417)
  - The reader shall have a display capable of displaying the retrieved and deciphered cardholder's picture.
- **Mode 6 - CHUID Verification and Electronic Visual Verification and Active Card Authentication**
  - The reader shall have a card interface (contact or contactless)
  - If the reader has only a contactless interface, the reader shall have a mean to access/retrieve the TPK from the TWIC card by using a two-dimensional bar code reader (PDF 417)
  - The reader shall have a display capable of displaying the retrieved and deciphered cardholder's picture.

6. Fixed TWIC Reader Physical Requirements

There are several electrical and physical requirements for fixed TWIC readers. These requirements are necessary to ensure reliable and successful operation in certain operating environments.

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

Note: In this whole section, the term "TWIC reader" implies a Fixed TWIC reader.

6.1 TWIC Reader Dimensions

There are no specific requirements for TWIC reader dimensions. However, TWIC readers should be reasonably compact and versatile.

6.2 TWIC Reader Mounting

Mountings provided shall be tamper-resistant. This means that the TWIC reader should[43] have the ability to send an external signal to a back-end system in the event that there is an attempt at unauthorized penetration or removal of a TWIC reader.

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

6.3 TWIC Reader Environmental

TWIC Fixed readers may support intrinsically safe operation in a hazardous materials environment where explosive vapors are present in the atmosphere. Intrinsically safe TWIC readers shall be certified for use in explosive atmospheres.

6.3.1 Outdoor Use requirements:

1. TWIC readers shall conform to a NEMA 4 rating.
2. TWIC readers shall operate within a temperature range of -20°C to +70°C (-4°F to +158°F)[44].
3. TWIC readers shall operate in a humidity range of 5-100%, condensing.
4. TWIC readers shall be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources.
5. TWIC reader components may be offered in an enclosing cabinet that achieves the rating required.

6.3.2 Indoor Use requirements:

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

[43] The term "should" is used in this sentence as this is a highly recommended feature, but is not tested as part of the requirements for TWIC readers. This is left to the appreciation of the PACS installer as there might be other countermeasures used to prevent such an attack.

[44] It is strongly suggested to have as part of the reader an indicator turned ON (or a switch turned OFF) when the reader temperature is outside of the operating range of the reader specification. This prevents, for example, contactless readers to derive in operating frequency and then have an erratic behavior when cards are presented.

6.4 Impact Resistance

TWIC reader verification functionality shall not be degraded by low frequency vibration typical at maritime facilities stemming from sources such as vessel departure/landings, heavy foot traffic, electric carts, large HVAC systems, sub-floor bag conveyors, and outdoor truck traffic. TWIC reader manufacturers may base compliance on IEC 60068-2-64. Equivalent commercial practice or analysis may be substituted subject to approval by TSA.

6.4.1 Shock

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

6.4.2 Bump

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

6.5 Electrical Requirements

1) TWIC readers shall operate within a range of 8-48 VDC. Where necessary to operate from line voltage, a power supply approved for use with a TWIC reader shall be provided. TWIC readers may optionally support PoE or PoE+ (Power over Ethernet or Power over Ethernet Plus) in accordance with IEEE 802.3af (48VDC/15.4W max) or 802.3at (48 VDC/56W max).
2) TWIC readers shall not exceed a 2.0 Amperes current requirement.
3) TWIC readers shall provide reverse voltage protection.
4) TWIC readers shall be FCC certified.
5) TWIC readers shall return automatically to normal operation after a loss of power event.

6.6 Safety

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

TWIC readers shall not possess:

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

6.7 Electromagnetic/Vibration Compatibility

TWIC readers shall comply with the following requirements. For immunity tests the equipment shall operate normally or, if operation is interrupted, it shall not grant access.

6.7.1 47CFR18 and/or CISPR 11 (Emissions)

- All TWIC readers shall be FCC certified.

6.7.2 IEC 61000-4-2 (Electrostatic Discharge)

- Contact Discharge Mode at 2 kV and 4 kV Air Discharge Mode at 2 kV, 4 kV and 8 kV.
- Presumes 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.
- Performance Criteria B.

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

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

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

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

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

- 10 Vrms[45], 150 kHz to 80 MHz.
- Power ports and signal lines over 3 meters, 1% steps, 2.8 sec. dwell.
- Performance Criteria A.

6.7.6 IEC 61000-4-5 (Surges)

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

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

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

[45] Root-Mean-Square Voltage (Vrms) – See https://www.electronics-tutorials.ws/accircuits/rms-voltage.html

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

- 30% reduction for 0.5 periods (10 ms), Performance Criteria B.
- 60% for 5 periods (100 ms), Performance Criteria C.
- 60% for 50 periods (1 sec), Performance Criteria C.
- 95% for 250 periods (5 sec), Performance Criteria C.

7. Portable TWIC Reader Physical Requirements

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

i. confidentiality (session key)

ii. active authentication of the TWIC reader and/or, the operator using the TWIC reader.

Note: In this whole section, the term "TWIC reader" implies a portable TWIC reader.

If a portable TWIC reader has only a contact interface, the TWIC reader may access the TWIC card through either the TWIC or PIV Data Model application on the card. If the card is a Legacy TWIC, the PIV Data Model application selection and PIV Application PIN entry is required to release the cardholder picture to a TWIC reader. The cardholder's picture can be accessed without PIN entry when reading NEXGEN TWIC cards. Using the TWIC card application over the contact interface allows the TWIC reader to access the enciphered fingerprint biometric reference template along with the key (TPK) used to decipher it.

If a portable TWIC reader has only a contactless card read capability, the portable TWIC reader shall also have a magnetic stripe reader in order to access the TWIC Privacy Key on Legacy Cards, and/or a two-dimensional bar code reader to access the TPK on TWIC NEXGEN cards. The Portable TWIC Reader might also have a connection with a back-end system allowing to download the TPK indexed by the Card FASC-N as described in Appendix B. The TPK is needed to decipher the user reference biometric information held within the TWIC card application.

A portable TWIC reader shall be capable of confirming whether a TWIC card has been canceled. A portable TWIC reader shall be capable of downloading and using the most recent TWIC Canceled Card List (CCL). A portable TWIC reader may in addition support a Certificate Revocation List (CRL) subject to availability of a network connection.

7.1 Portable TWIC Reader Specific Requirements:

TWIC Portable readers may support intrinsically safe operation in a hazardous materials environment where explosive vapors are present in the atmosphere. Intrinsically safe TWIC readers shall be certified for use in explosive atmospheres.

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

7.1.1 Operational Features

1. Portable TWIC readers shall have a display suitable for user interaction.
2. Portable TWIC readers shall be able to display the current battery level.
3. Portable TWIC readers shall have a real time clock.
4. Portable TWIC readers may use a touch screen or other suitable (Keyboard or Pin-PAD) means for user input/control.
5. Portable TWIC readers should have a hibernation mode for protection against data loss.

7.1.2 Environmental Requirements

Portable TWIC readers certified for harsh conditions shall meet the following specifications:

1. MIL-STD 810F, Method 514.5 – Vibration.

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

7.1.3 Electrical Requirements

1. Portable TWIC readers should be supplied with a rechargeable battery with 12 hours minimum operational time.
2. Portable TWIC readers shall be operable while charging.
3. Portable TWIC readers should have a maximum battery recharge time of 2 hours.

7.1.4 Safety

Battery operated portable TWIC readers are not required to comply with UL 294, Standard of Safety for Access Control System Units.

Portable TWIC readers that support connection to a PACS to operate access control devices shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.

8. TWIC Reader Operational Requirements

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

1) The contactless smart card TWIC reader component shall conform to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-2.
2) Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s, dependent on the speed capability of the presented card.
3) If two or more contactless smart cards are presented at the same time in a TWIC reader's contactless field, the TWIC reader shall reject all of the presented cards.
4) TWIC readers shall require that a TWIC card, once read, shall be removed from the RF field for at least one second before attempting to read any new contactless card. This requirement is to minimize multiple reads of the same TWIC card for a single presentation.
5) Fixed TWIC readers shall be capable of reading the access control data from a TWIC card, performing the necessary authentication steps, and transmitting the credential data as required by the PACS.
6) Due to the particulars of TWIC card issuance a minimum of 3 data elements of the FASC-N should be read and forwarded to the PACS. These data elements are the Agency Code, System Code, and the Credential Number.
7) Fixed TWIC readers shall have communications ports as required by the PACS cable plant and control panels. Communication ports supported by fixed TWIC readers shall include:
    a. A unidirectional Wiegand port for connection to standard access control panels.
    b. A bidirectional RS-485 or 10/100baseT (Ethernet) for connection to computer systems or access control systems.

For fixed TWIC readers, at least one Wiegand output format shall provide a 75-bit “transparent mode” which includes 2 parity bits and 25 bits for the date. The TWIC reader shall output the following 75 bits:

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

Table 8.1 75-bit Wiegand Output Format

Fixed TWIC readers may support an additional Wiegand output format of 48 bits when a TWIC reader includes a real time clock that may be used to verify the expiration date. In this case, it is presumed that the TWIC reader has the ability to process the expiration date. Some PACS control panels may not be

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

The 48-bit Wiegand format is the same as the 75-bit transparent mode but drops the expiration date and the two parity bits as shown below:

Description	Position	Length (BITS)
Agency Code	1-14	14
System Code	15-28	14
Credential Number	29-48	20

Table 8.2 48-bit Wiegand Output Format

8) Fixed TWIC readers may support other additional Wiegand formats for legacy systems. Wiegand output formats not detailed in this specification may transmit the entire FASC-N or selected elements of the FASC-N.

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

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

11) TWIC reader visual indicators shall be visible in daylight.

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

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

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

15) All TWIC readers, or the back end doing verifications, shall have access to a system clock capable of synchronizing all readers to current date and time.

16) TWIC readers shall provide a means to create a time-stamped log of each TWIC card read for use in capturing exception conditions such as fingerprint rejections. The TWIC reader log of TWIC card reads shall include at least the date, time, the FASC-N (or the Card UUID [46]in NEXGEN TWIC cards), and a description of the TWIC card read result (e.g., SUCCESS, FAILED BIOMETRICS, etc.).

17) TWIC readers shall provide a means to export the TWIC reader log in human-readable form in the English language. Additional formats for a TWIC reader log may be supported.

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

[46] Universal Unique Identifier

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

20) TWIC readers shall support a method of changing its mode of authentication according to the current security threat level of the protected site or be disabled is they cannot accommodate the current security threat level.

9. Performance Requirements

1) TWIC readers should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to a TWIC reader and completion of the biometric match) of no more than 6 seconds. This maximum transaction time does not include the time required to acquire the TPK or a live fingerprint sample from the cardholder.
2) The biometric sub-system should provide an equal error rate (EER) of 1% (i.e. 1% false rejections at a setting of 1% false acceptance) on a per transaction basis. This presumes up to three attempts as a minimum standard error rate. TWIC readers should provide a mechanism to adjust the security level sensitivity as required.
3) Any alternatives to the use of fingerprint biometrics shall be addressed in the local operator's security plans. They could involve using the cardholder's picture (PIV/CIV mode or TWIC NEXGEN Mode 5 or 6), or site-specific operational modes using the NEXGEN E-Sticker features (see Part 4 for details).
4) Biometric-enabled TWIC readers should provide liveness detection. This is particularly important when TWIC readers are used in unattended operations.
5) Biometric processes and performance are further described in ANSI/INCITS 383.
6) It should be noted that biometric interoperability is defined as the ability of a biometric TWIC reader to perform a match from a presented biometric with the ANSI/INCITS 378 formatted enrolled templates provided on a TWIC card by TSA. Such templates shall be in compliance with NIST Special Publication 800-76-2 and ANSI/INCITS 378 profile for PIV Card templates.

10. Operational Availability

1) Biometric-enabled TWIC reader vendors shall be able to warrant either 1 million touches or 5 years operational use for their TWIC reader fingerprint sensor without degradation.
2) TWIC readers should be designed to achieve a Mean Time Between Failure (MTBF) of 25,000 hours or greater. Vendors may instead elect to warrant their MTBF for at least 3 years.

11. Delivery

1) TWIC readers shall include technical manuals covering installation, operation and maintenance.
2) TWIC readers shall be packaged suitable for shipment to a designated installation point.

Appendix A Authentication Processing

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

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

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

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

Identifiers, such as the TWIC CHUID, may be strengthened by using a digital signature. A digitally signed identifier may be used to verify that: it is a genuine identifier for an individual, said identifier was issued by the system authority, and the identifier has not been revoked or invented. However, an identifier by itself is generally public information and does not provide authentication that the individual using the identifier is the individual to whom the identifier was issued. An authentication factor, such as a password, should also exist. Further, the knowledge to satisfy a given authentication factor challenge should be limited to either the system authority (e.g. card authentication) or the individual (e.g. PIN or biometric) for whom the identifier was issued.

All TWIC cards offer one data element that may be used to support identification and two different data elements to support authentication via the contactless interface of the card:

1) CHUID data object – A strong, digitally signed **identifier** issued by the TWIC Program after vetting the identity of an individual and determining that said individual is trustworthy.
2) TWIC biometric template – A strong "something you are" **authentication** factor that is strongly bound (unique) to the individual. The TWIC biometric template is strongly bound to the CHUID (identifier) and protected against alteration (counterfeit) through digital signature.
3) Card Authentication Certificate and Key[47] – A strong "something you have" **authentication** factor that is strongly bound to the user's smart card through proof of possession of a never revealed private key that exists only on the user's smart card. The use of the card authentication certificate and associated private key provide strong proof that the smart card being presented to a TWIC reader is a genuine TWIC card that was issued to the individual by a trusted authority.

NEXGEN TWIC Cards have an additional authentication mechanism which is also related to the "what you are factor", but this mode requires an operator to perform the validation of the reference cardholder picture read from the card against the live image of the cardholder presenting it.

[47] Found in the PIV Data Model Card Application in Legacy TWIC Cards and in the TWIC Card Application for NEXGEN TWIC cards

Notes

- The CHUID is sometimes referred to as a "weak" authentication factor. It should be noted that without biometric verification or card authentication, the CHUID is a publicly available identifier that is transmitted over the TWIC contactless interface in clear text and may be captured, copied to another card or replayed, along with the digital signature attached to it. Caution should be exercised in relying solely on the CHUID as an "authentication" factor, even in low assurance applications as it may be captured by an attacker without the legitimate user consent or knowledge.
- TWIC relies on the use of a Public Key Infrastructure (PKI) to include signatures and certificates. TWIC issues five-year certificates; the consequence of these longer life certificates is certain fields in the certificate have values that, by policy, vary from FIPS 201 PKI policies.
- The table providing the complete list of all Object Identifiers (OID) which can be found in a TWIC card (Legacy and/or NEXGEN) can be found in section 6 of Part 2 [PIV and TWIC Object Identifiers] of this series of documents.
- **PIV OIDs** are registered with the Computer Security Objects Registry for which NIST is the Registration Authority. The "**PIV Root" is 2.16.840.1.101.3** {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)}.
- **TWIC OIDs** are registered with the Internet Assigned Numbers Authority (IANA). The "**TWIC Root" is defined as 1.3.6.1.4.1.29138** {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) twic-root (29138)}.
- TWIC readers shall accept either OID value when parsing a signature or certificate from either the TWIC card application or the PIV Data Model card application.

In Section 6 of Part 1 (Appendix B – Threats, Vulnerabilities and Countermeasures – An overview), a discussion about the various authentication mechanisms is presented in a chart indicating the level of assurance reached for each mode of operation.

Appendix B Using the PDF 417 for TWIC and AAMVA readers

This appendix describes in detail how TWIC readers can access the TPK information from the PDF 417 and what AAMVA compatible readers may get out of the TWIC PDF 417 bar code.

The PDF 417 structure is based on the AAMVA standard as described in the document AAMVA-2020-DLID-Card-Design-Standard.pdf. The detailed structure of the PDF 417 is described in the TWIC NEXGEN Specification Part 2 in section 4.9.

The PDF 417 consists of three different zones:

1. Header – A data string of 40 bytes long which contains the following information:
    a. In offset 23, the offset of the AAMVA ID subfile is indicated in four characters.
    b. In offset 27, the length of the AAMVA ID subfile is indicated in four characters.
    c. In offset 33, the offset of the TWIC subfile (ZTZTA) is indicated in four characters.
    d. In offset 37, the length of the TWIC subfile (ZTZTA) is indicated in four characters.
2. The AAMVA ID subfile:
    a. The various AAMVA field IDs are used to identify the various data elements.
    b. It is interesting to notice that the AAMVA data element DAQ contains the TWIC card Identification Number (CIN on 8 digits) which can be used to check if the card has been canceled (using the TWIC VCCL)
3. The Subfile ZTZTA specific to TWIC
    a. This subfile contains the TWIC Data Object TPK (0xDFC101) in characters. It must be converted to a hexadecimal string allowing to extract the TPK itself. The detailed format can be found in TWIC NEXGEN Specification Part 2 section 4.9.

Appendix C TWIC Privacy Key Network Processing

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

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

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

The XML-RPC example uses the following data:

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

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

The Base64 encoding of the FASC-N yields ->
1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==

The Base64 encoding of the TWIC Privacy Key yields ->
MDEyMzQ1Njc4OTAxMjM0NQ==

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

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

<?xml version="1.0"?>
<methodCall>
  <methodName>KeyLookup</methodName>
  <params>
    <param>
      <value><base64>1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==</base64></value>
    </param>
  </params>
</methodCall>
```

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

The input parameter value corresponds to the unique user ID (i.e. FASC-N) that was read from a TWIC card as a binary value and base64 encoded.

The response shall be, as a minimum, a base64-encoded 128-bit (16-byte) AES decipherment key:

```
HTTP/1.1 200 OK
```

```
Connection: close
Content-Length: xx
Content-Type: text/xml
Date: Fri, 19 Feb 2008 19:55:08 GMT
Server: TWICLand Frontier/5.1.2-WinNT

<?xml version="1.0"?>
<methodResponse>
  <params>
    <param>
      <value><base64> MDEyMzQ1Njc4OTAxMjM0NQ==</base64></value>
    </param>
  </params>
</methodResponse>
```

NOTE 1: The response Content-Length field was not computed for this example.

NOTE 2: The Host may elect to transmit a fixed, maximum length TPK value field (32 bytes). Transmission of a fixed length TPK value field is encouraged for extensibility reasons. The expected TPK decoded data in the (not detailed) longer response message using the example value of the TPK should be:

303132333435363738393031323334350000000000000000000000000000000000.

TWIC readers should be able to correctly extract the TPK from either form of the XML-RPC response.

Appendix D TWIC Reader Adaptability

D.1 Change of Operation Mode

TWIC readers shall support multi-mode operation and be able to accept external triggers for the mode change or being disabled if they do not support the mode required. A mode change should apply to applications such as a threat level change (e.g., maritime security or MARSEC levels).

D.2 Accepting New Operating Modes

TWIC readers should be capable of various modes whether currently defined by the Coast Guard or not. TWIC readers should be capable of supporting secure firmware modification allowing definition of new modes of operations as may be required.

D.3 Selection of the TWIC Card Application AID

All TWIC readers shall do a selection of the TWIC card application and work only with this card application as long as the AID does not indicate it is a Legacy Card. If the AID indicates it is a Legacy Card (see below), the TWIC reader shall then use the PIV Card Application for Mode 2 (ACA).
This Application selection shall be done according to the process described in the TWIC NEXGEN Specification Part 2 (TWIC Card reference document), using the ISO/IEC 7816-4 SELECT command with an argument data consisting of the partial TWIC Card Application Identifier on 9 bytes (A0 00 00 03 67 20 00 00 01).
Upon successful selection of the application, the reader will receive from the card the full AID (11 bytes) in which the two last bytes indicate the version and sub-version of the card application present in the card. This current specification applies to all cards with a version of x01 and the reader SHALL verify it can work with the version of the TWIC Card application returned.

The Full AID of a TWIC Legacy card is: A0 00 00 03 67 20 00 00 01 **01** 01 (Version = 01)
The Full AID of a TWIC NEXGEN Card is: A0 00 00 03 67 20 00 00 01 **01** 03 (Version = 01)

Notes:
As long as the version indicates x01, even if the sub-version is different from x01, it means the card data model is backward compatible with the Legacy Card Data Model (version x01, subversion x01).

See TWIC NEXGEN Part 2 documentation in section 4.1 for more detailss about the structure of the Card Application AID.

Appendix E TWIC Reader Compatibility with Other Card Types

Some sites may need to use TWIC readers and the associated PACS with other card types, in addition to the TWIC. In some situations, a TWIC reader may be required to read multiple card types such as the Department of Defense Common Access Cards (CACs) and/or the Federal Personal Identity Verification (PIV) cards. In such an environment, a TWIC reader should be capable of selecting the correct application identifier (AID) associated with these different card types and, on successful selection of a specific card application, behave in accordance with the requirements of the specific card application.

For a site that may use multiple card types, a TWIC reader should support the configuration of default AIDs as described in the next paragraph:

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

There are various methods readers may use to recognize a TWIC card from a PIV/CIV/PIV-I/CAC etc. (all SP 800-74, SP 800-76, and SP 800-76 compliant) :

- TWIC cards do have a FASC-N indicating they have been issued by a Federal Agency (DHS-TSA). The Issuer code used for TWIC cards is 7099
- TWIC cards do have specific OIDs as indicated in Part 2 allowing them to be easily distinguished from other cards.
- TWIC cards do contain the TWIC Card Application (First 9 bytes are AID = A0 00 00 03 67 20 00 00 01)

Appendix F Interpretation of the Biometric Template CBEFF Header

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

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

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

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

TWIC Readers shall ignore minutia points which are outside of the area size section provided in the template[48].

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[49].

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

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

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

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

[48] Such errors may happen when multiple fingers in which the captured area size is not the same between all the fingers, end up having some minutia point referenced outside of the size area if the maximum size area is not the one stored in the template.

[49] 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.