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).

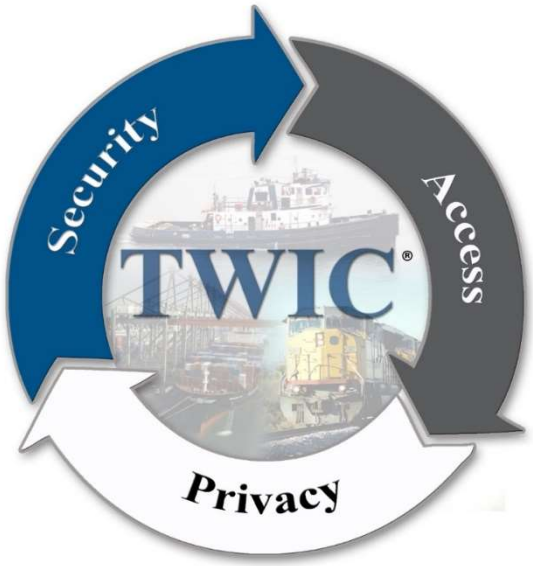
IMPORTANT Notice: The planned TWIC card NEXGEN upgrade, described in these documents, has been designed to be backward compatible as much as possible with TWIC Legacy, but it is important to confirm that existing TWIC readers are compatible with TWIC Legacy as well as the new TWIC NEXGEN data model when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

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

This page was last updated on July 2, 2024



TWIC® Documentation

Part 1 – General Description

July 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	**Incorporated comments from Industry review**
October 2019	**Text revised for final publication**
January 2020	**Incorporated comments from Industry Round 2 review**
June 2021	**Modification of some Tags for coherence between PIV & ISO**
January 2022	**Added information about the four new TSA E-Stickers**
April 2022	**Added Header warning it is not the final release**
July 2022	**Added information about the PIN TWIC Application used in NEXGEN cards in addition to the PIV Card Application PIN used in Legacy cards**
March 2023	**Minor edits and typo corrections**
June 2023	**Minor editorial – Information added about the TWIC PIN**
July 24th, 2023	**Official first release of the document.**
August 8, 2023	**Added in all four parts of the documentation a warning related to possible changes regarding the PUK (PIV & TWIC) as well as the format and content of the PDF 417**
August 10, 2023	**Changed in all four parts the documentation: The notion of TWIC PUK and TWIC PIN has been removed. This also makes the four TWIC protected e-stickers go away. In this version, only the PDF 417 still might be modified**
September 15, 2023	**Information about the format of the card PDF 417 changed to comply with the AAMVA standard. Details in Part 2**

Acronyms and abbreviations

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
BAC	Basic Access Control
CBEFF	Common Biometric Exchange Formats Framework
CCL	Canceled Card List (formerly known as the Hotlist)
CHUID	Card Holder Unique Identifier
CIN	Card Identification Number
CIV	Commercial Identity Verification
CRL	Certificate Revocation List
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
IBIA	International Biometrics + Identity Association
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
INCITS	InterNational Committee for Information Technology Standards
ISO/IEC	International Standards Organization/ International Electrotechnical Commission
MARSEC	Marine Security
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
PACS	Physical Access Control System
PDF 417	Portable Data File (4 bars and spaces / 17 module units)
PIN	Personal Identification Verification
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
QTL	Qualified Technology List
SHA	Secure Hash Algorithm
SIA	Security Industry Association
SP 8xx	Special Publication (NIST)
STA	Secure Technology Alliance
TPK	TWIC Privacy Key
TSA	Transportation Security Administration
TWIC®	Transportation Workers Identification Credential
UUID	Universal Unique ID

Table of contents

1. Overview

1.1 Abstract

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

The **first part** (this document) presents the general concepts of TWIC from a functional standpoint, without the consideration of the details of an implementation.

The **second part** describes in detail the TWIC® card interface, the two card applications contained in the card (known as TWIC and PIV Data Model) as well as the behavior of the card during normal operation.

The **third part** describes in detail TWIC reader requirements, the type of mechanical and electrical specifications they must comply with, as well as the various options a TWIC reader manufacturer may claim. Both portable and fixed TWIC readers are described in this third part. The functions specified in this third part shall comply with all documented requirements for a TWIC reader to appear on the public Self Certified Qualified Technology List (SC-QTL) published by DHS TSA. TWIC readers that appear on the SC-QTL have been tested by their manufacturers according to a process defined by TSA based on the reader claimed features.

The **fourth part** is for informational purposes and provides guidance on how a PACS[2] can register a TWIC card, the TWIC card holder and how it may use a TWIC credential as a physical access credential in various modes of operation. Some suggestions are added in this fourth part in relation with the use of E-Stickers allowing a PACS to read but also write information of their own in the TWIC card (should TSA elect to enable this feature on TWIC cards).

A **fifth part** is under consideration to be created later as part of this series of documents. This proposed fifth part will be dedicated to a new possibility made available to NEXGEN TWIC cards allowing TWIC credentials to be activated as a Personal Identity Verification Interoperable (PIV-I) compatible card.

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[3] (IBIA), the Security Industry Association (SIA) and the Smart Card Alliance[4]. 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** (this part)
- **Part 2** – TWIC card application data model, TWIC card application card edge behavior during normal operation
- **Part 3** – TWIC reader requirements
- **Part 4** – TWIC registration and TWIC card use by a PACS
- **Part 5** – TWIC activation as a PIV-I compatible credential[5].

[1] TWIC® is registered in the U.S. Patent and Trademark Office by the U.S. Department of Homeland Security.
[2] Physical Access Control System
[3] The International Biometric Industry Association has changed its name to the International Biometric + Identity Association (www.ibia.org)
[4] Smart Card Alliance has changed its name to Secure Technology Alliance (https://www.securetechalliance.org/)
[5] This fifth part may be created in the future but is contingent to modifications in the TWIC issuance system as well as in TWIC activation stations.

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. These specifications enable varying levels of control in support of threat level risk mitigation plans.

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

It is important to take into consideration the two different types of TWIC cards described in these documents. TWIC cards are issued for a period of up to five years and this new version of a TWIC card described in this documentation (called NEXGEN TWIC) will progressively replace the millions of Legacy TWIC cards issued prior to this new TWIC card specification. Regardless, because TWIC Cards are issued for a duration 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 by TSA to TWIC cardholders.

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

Important terminology: In the four parts of this NEXGEN documentation, to avoid any confusion with a PIV[7] 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[8] documents describing the format of the data and structures to be stored in a PIV-like card. These NIST documents are: SP 800-73, SP 800-76, and SP 800-78[9]. Additionally, a PIV card is compliant with the NIST document SP 800-79 which defines the Federal trust model (Federal Bridge used by PIV and PIV-I[10]). The TWIC card does not use this trust model, as it complies with a simpler, more traditional trust model also adopted by e-Passports (described by the International Civil Aviation Organization in their ICAO 9303 documentation – https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf).

In this TWIC NEXGEN version, the format of the PDF 417 on the back of the card has changed from ASN.1 to the AAMVA format

[6] See TWIC® NexGen card FAQ on the TSA web site: https://www.tsa.gov/for-industry/twic
[7] PIV stands for Personal Identification Verification
[8] NIST stands for National Institute of Standards and Technology
[9] See list of normative references in section 2.1 for details on these Special Publications from NIST.
[10] PIV-I stands for Personal Identity Verification Interoperable

Purpose of TWIC® NEXGEN

There are multiple reasons the NEXGEN effort was pursued:

- A New generation of electronic smart card chip component was made available to TSA from the industry. This new chip provides faster operation, better reliability and more memory, all at the same price point as the current smart card chip used by TSA since 2011.
- NIST deprecated the magnetic stripe per their standard for PIV cards. Very few TWIC readers were using the magnetic stripe and hence appropriate to move to a two-dimensional bar code (PDF 417[11]) for the TWIC Privacy Key (TPK) on the back of the TWIC card. This allows devices, such as smartphones, to interact more easily with a NEXGEN TWIC card. The PDF 417 barcode also permits more information to be provided to a barcode scanner than can be placed on a magnetic stripe. It must be noted the existing linear bar code (1D) containing the Card Identification Number is unchanged from the previous design (see image of the back of the card in Part 2 Section 1.4 page 9, right bottom image).
- It was suggested by some to have the PIV card application in the TWIC card more aligned with the PIV/PIV-I/CIV documents and specifications. Noting the concern of possibly breaking of backward compatibility with existing TWIC cards and readers, this suggestion has its own unique challenges in terms of the PIV card application data and trust models in a TWIC card. That said, the NEXGEN TWIC card data model anticipates this suggestion by providing a complete independence of the PIV card application from the TWIC card application. This allows each card application to evolve independently at their own pace.
- New optional data objects have been added to the TWIC card application on the contactless modes (e.g. Cardholder Picture) allowing more functionalities, without the PIV PIN of the card being required.
- The data objects on the card, as well as the new two-dimensional bar code which may contain cardholder information, permits a TWIC card to be technically aligned to the Real ID requirements.
- A revolutionary new capability has been added in NEXGEN TWIC cards named “E-Stickers”. An E-Sticker allows the PACS industry to use the card for their own purpose, without having TSA being involved (i.e., the storage is made available by TSA but is not managed). See mainly Part 2 and Part 4 of this series of documents for examples of use.

1.3 Summary of Changes to the Previous Specification

1) A new type of Smart Card chip is used for NEXGEN TWIC and is described in this new set of documentation. Even with all the added features, this new data model provides backward compatibility with already deployed TWIC readers, allowing updated TWIC readers to take advantage of the new functionalities of the NEXGEN TWIC Data Model.
2) As TWIC cards are issued for a period of up to five years, all TWIC readers shall work with the Legacy TWIC for at least a period of five years starting from the first date of NEXGEN TWIC issuance. As such, all parts related to this new documentation take into account two types of cards which must be supported by all readers claiming conformance with NEXGEN Part 3 specification.
3) The NEXGEN TWIC card provides complete independence between the two card applications existing in TWIC credentials (PIV Data Model and TWIC). This technically allows a NEXGEN TWIC card to be activated as a PIV Interoperable (PVI-I) compatible credential if required. But PIV-I activation would break backward compatibility with Legacy TWIC card behavior, and as such, this option will not be made available until substantially all TWIC readers are conformant with the NEXGEN TWIC card data model.

[11] The Portable Data File reference 417 is defined in the ISO/IEC standard 15438 - https://www.iso.org/standard/65502.html

4) The TWIC card application in NEXGEN TWIC cards has all the cardholder information made available through either the contact or contactless interfaces without the PIN being required. This includes the cardholder digital photo, which was only available through the PIV Data Model card application on Legacy TWIC cards, Personal biographic and biometric information carried by the TWIC card application, all of which are encrypted using the card TWIC Privacy Key (TPK).

5) The Magnetic Stripe on the back of Legacy TWIC Cards has been replaced in the NEXGEN TWIC with a two-dimensional bar code (PDF417). The bar code contains the TPK as well as additional information related to the cardholder which is aligned with Real ID[12] requirements.

6) All Digital Signatures in NEXGEN TWIC cards use the Secure Hash Algorithm SHA-2 NIST-recommended message digest (hash) algorithm instead of the older SHA-1 message digest (no longer considered as secure) used in Legacy TWIC cards.

7) The Card Universal Unique Identifier (UUID) is now fully populated in all NEXGEN TWIC cards with a NIST-SP 800-74 compliant structure and the Card UUID is also added to all digitally signed data objects. The structure of this Card UUID[13] allows a reader to retrieve the FASC-N[14] in any signed data field in an attempt to preserve PACS implementations built around FASC-N values. See details in Part 2 Appendix D. The same Card UUID value is always used for both card applications in the NEXGEN TWIC card.

8) The TWIC card application in a NEXGEN TWIC has now its own TWIC Application Card Authentication Key. This key is independent of the PIV Data Model Card Authentication Key. For NEXGEN TWIC, there is no need to use the PIV Data Model card application in any of the TWIC reader modes for PACS registration.

9) New personal data containers have been added to the NEXGEN TWIC card application data model. These include the Discovery Object, Cardholder's facial photo, written signature, and biographic information. These objects are encrypted and protected by the TPK for privacy in the exchanges between the reader and the TWIC card. These containers are available on the contact as well as the contactless interface without any requirement for PIN presentation. The TPK itself has specific access conditions and cannot be read using the contactless interface.

10) Because of the new personal data containers, a new mode of operation for the TWIC credential is available with NEXGEN TWIC cards. It allows a guard to verify the photo of the cardholder without having to use the PIV Data Model card application in contact mode which requires the presentation of the PIV Card Application PIN.

11) Despite all these changes and improvements for the NEXGEN TWIC Card, TWIC readers qualified for use with Legacy TWIC cards should work with NEXGEN TWIC cards even if the readers have not been updated to process the NEXGEN TWIC additional card information.

12) A new concept has been introduced in NEXGEN TWIC cards allowing application providers to take advantage of ten free read/write data containers called E-Stickers, and four TSA controlled e-Stickers (Free read, update under card issuer's control). The use of these features is completely optional, and TWIC is not regulating the format or the use of these containers; but informative guidance and structure, along with examples of use, are provided in the Part 4 of this series of documents.

[12] For more information about REAL ID, refer to https://www.dhs.gov/real-id-public-faqs

[13] The UUID is a data structure on 16 bytes defined by the document IETF/RFC 4122. The Card UUID used by this new TWIC data model uses the mode 5 of the RFC 4122, It also should be noted that the GUID defined in the CHUID by SP 800-73 is a TLV data object which value is the Card UUID.

[14] FASC-N stands for Federal Agency Smart Credential Number

2. References

2.1 Normative References[15]

[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)

[15] 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)

2.2 Informative References

[R32] FIPS Publication 201-2 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (August 2015)

[R33] ICAO 9303 Machine Readable Travel Documents

[R34] 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)

[R35] 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..

[R36] Comparison between PIV, PIV-I and CIV from the Secure Technology Alliance. https://www.securetechalliance.org/resources/pdf/PIV_PIV-I_CIV_brief_022212.pdf

[R37] How to test TWIC cards in use in the field from the Secure Technology Alliance https://www.securetechalliance.org/twic-card-reader-challenges-with-physical-access-control-systems-a-field-troubleshooting-guide/

3. Definitions

3.1 Conformance Levels

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

3.2 Glossary of Terms

- **Card Application:** an application identified by its Application Identifier (AID) loaded (or present) in a smart card.
- **Canceled Card List (CCL)**[16]: Updated each day by the TWIC system, this list contains all the TWIC credential numbers which have been canceled. Cards which have expired do not appear in this list.
- **Card Verification Device:** 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, Ultraviolet (UV) printing, etc.)
- **Cardholder:** The person presenting the TWIC card to an operator (or to a device) and claiming the card was issued to them.
- **CIN:** Card Identification Number. Information printed on the back of the TWIC card (left bottom side using 8 digits) and in the linear one-dimensional (1D) bar code using Code 39 encoding.
- **Legitimate Cardholder**: The vetted person who was provided the TWIC card by the TSA TWIC system and whose personal and biometric information is used to personalize 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 the cardholder presenting the card.
- **PIV Data Model Card Application:** The card application present in a TWIC card, conformant to the NIST SP 800-73, SP 800-76 and SP 800-78 series of specifications.

[16] The TWIC CCL can be found at https://universalenroll.dhs.gov/ccl/CCL.CSV

- **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 for the Transportation Worker Identification Credential (TWIC) Program.
- **TWIC Legacy:** TWIC Cards conforming to the May 2012 TWIC Reader Hardware and Card Application Specification.
- **TWIC NEXGEN:** TWIC cards conforming to this TWIC card specification (see Part 2)
- **TWIC Privacy Key (TPK):** A 128-bit AES[17] symmetric key value used to encipher the biometric templates and other information that are stored on the TWIC card.
- **VCCL:** Visual Canceled Card List contains the Card Identification Numbers (CIN) canceled[18]. Used by Card verification devices not interacting electronically with the chip of the TWIC card, but verifying if the CIN of the card is canceled.

3.3 Differences between Cancellation, Suspension and Revocation

The terms **cancellation** and **suspension** apply to credential (FASC-N) or card (CIN) identifiers.
The term **revocation** applies to a certificate when it is no longer valid or an access right in a PACS is revoked.
As such, beside the validity date of the card, the usability of a TWIC card presented can be checked using the following methods:

- All unexpired cards that are **canceled** or **suspended** have their identifier on the respective canceled list (CCL for FASC-N and CIN for the VCCL). Such a card should no longer be considered valid.
- All unexpired cards that are canceled and have their card authentication certificate **revoked** are listed on the CRL (Certificate Revocation List). Such cards should no longer be considered valid, but it is important to note that the CRL does not include the suspended cards.

In addition to the authorization attached to a given card by the local system, TSA maintains the list of cards which should not be used anymore:

Table 1: Suspended or Canceled vs. Revoked

Status of a non-expired card	Credential Identifier FASC-N	Card Identifier CIN	Card Authentication Certificate
Canceled	On the CCL	On the VCCL	Revoked - On the CRL
Suspended	On the CCL	On the VCCL	**Not Revoked - Not on the CRL**

This table shows why the CCL or the VCCL shall be used to test for valid TWIC cards as the CRL does not contain the suspended cards (which may be taken off the canceled lists if the issue which created the suspension status is later resolved). See section 10 Appendix D – Differences between CCL, VCCL and CRLs – for more details.

[17] See information about the Advanced Encryption Standard in section 2.1 line [R12]
[18] The VCCL can be downloaded from: https://universalenroll.dhs.gov/canceled-card-lists

4. TWIC Modes of Operation

4.1 General

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 set of documents 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 (they all have a specific assurance level) allowing each site to create its own authentication security policy 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 either in PIV mode in PIV-compatible systems/readers as well as TWIC mode in TWIC-compatible systems/readers. TWIC contactless Card Holder Unique Identifier (CHUID) verification and TWIC contactless biometric user authentication are supported directly by the TWIC card application. Card authentication using only the TWIC card application is supported by the NEXGEN TWIC card. For Legacy TWIC, card authentication over the contactless interface is supported through the selection of the PIV card application.

Note: All data shall be retrieved from the TWIC card application for NEXGEN TWIC cards whenever possible. Legacy TWIC requires the use of the PIV card application for operations involving Active Card Authentication or cardholder facial photo access.

Section 4.2 provides an overview of all the possible modes of operation of the TWIC card, independently of the type of device using it. Part 2 of this document series (detailing the TWIC card) indicates in detail how each of these modes are implemented in the card. Part 3 of this document series (about readers using TWIC cards) describes how these operating modes shall be implemented by the various types of readers.

4.2 Modes of Operation

In addition to the basic physical inspection or "Flash Pass/Visual Inspection" mode of using an ID card, this section provides an overview[19] of the seven modes of operation, from Mode 0 to Mode 6. Only modes 1 to 6 use the electronic interface of the card.

Notes:

- Mode 1 to Mode 4 were described in the previous TWIC documentation and are available on both Legacy and NEXGEN TWIC cards. These four modes do not require an operator to observe the result of the verification (mode 1), or the results of the authentication (modes 2, 3 and 4) processes.
- Mode 5 and 6 are available on NEXGEN TWIC cards only and require an operator (local or remote).
- For all TWIC cards, this set of documents presumes that Personal Identification Numbers (PINs) are not a requirement for verification or authentication at any MARSEC level[20].

[19] Part 2 (for the card) and Part 3 (for the reader) of this series of documentation provides the details for all these modes.
[20] See Part 4 – PACS registration section, where the PIV Card Application PIN might be required for Legacy TWIC Cards to access, for example, the cardholder facial photo.

4.2.1 Flash Pass/Visual Inspection

The card is presented to an operator for access by the cardholder. No device is used in this process. The operator verifies if the card looks legitimate, if the photo printed on the card is the same as the cardholder, and if the validity date printed on the card has not expired. There is no verification against the CCL and a canceled card will not be detected by such a process. If printed security feature verification means are not used (e.g. Ultra-Violet light, micro-printing detection), **this mode is considered as providing a very low assurance level.**

4.2.2 Mode 0 - Supplement to Visual inspection (STVI)

This mode is known in some earlier documents as a "Visual CCL" mode of operation. In addition to all the verifications done for a Flash Pass/Visual Inspection operation, a Card Verification Device[21] is used to verify if the card presented to the operator is not on the canceled card list. The Card Identification Number (CIN), located on the back of the TWIC card, may be entered manually by the operator on a Card Verification Device, or automatically read using the linear one-dimensional (1D) bar code on the back of the TWIC card. The Card Verification Device verifies the CIN against the previously downloaded Visual CCL[22] database. **This mode is considered as providing a low assurance level.**

4.2.3 Mode 1 - CHUID Verification

In this mode, the TWIC Reader reads from the TWIC card (using contact or contactless communication) the Card Holder Unique Identification Number (CHUID). This information is digitally signed by the issuer and a TWIC Reader verifies the integrity and the validity of the digital signature of this Data Object. The TWIC card Expiration Date (part of the CHUID) is checked, and the unique credential identifier (also part of the CHUID) called the Federal Agency Smart Credential Number (FASC-N) is checked against the Canceled Card List - CCL[23]. Presence of a FASC-N on the CCL indicates to a TWIC reader that the TWIC card has been canceled (or suspended) by TSA and is no longer trusted. For a given PACS, in order to be accepted for access, this process may also require that the card be previously registered with the PACS**. This mode is considered as providing a low assurance level.**

4.2.4 Mode 2 - Active Card Authentication (ACA)

In this mode, the TWIC reader obtains from the TWIC card the Card Authentication Key (CAK) Certificate from either the PIV card application for Legacy TWIC cards or from the TWIC card application for NEXGEN TWIC cards. This mode requires the whole chain of trust (from the certificate to the root of trust) to be validated. The Card identifier (FASC-N) contained in this certificate is verified against the CCL[24] to make sure the card is not canceled; the Certificate Expiration Date is verified, and the card is challenged using an active card key authentication mechanism to verify its authenticity. When deployed with Path Discovery and Path Validation to a trusted Root Certification Authority (CA), the system offers a high level of assurance that the card is indeed issued by the claimed issuer, is still valid, is not altered, is not a copy of another valid card, and is not a forgery. **This mode provides a good assurance level of the authenticity of the card by verifying that the physical card being presented was issued by TSA (one factor - what you have).**

[21] This could be a smartphone with a specific application, or a simple application such as Notepad in a computer executing a search in a text file (using the CIN Visual CCL loaded every day in the device). The TWIC ADVISR app is available for IOS and Android phones.
[22] The Visual CCL contains the Card Identification Numbers (CINs) of the canceled TWIC cards with a valid expiration date.
[23] The CCL (Canceled Card List) contains the FASC-N (electronic card identifier) of the canceled TWIC Cards with a valid expiration date.
[24] This is why this mode of operation is not called Card Authentication Key (CAK as in PIV) as it requires the verification of the CCL, the CRL being optional for TWIC.

4.2.5 Mode 3 - CHUID Verification and Biometric Verification

In this mode, in addition to the CHUID verification described in Mode 1, the cardholder's live (probe) biometric sample is compared to a biometric reference data stored in the card. The biometric reference template may be read from a TWIC card at each use or may be stored in a database to which the TWIC Reader system is connected (e.g. the PACS system which previously registered the cardholder). Biometric data is distributed in a Legacy TWIC card between the TWIC card application (encrypted fingerprint template) and the PIV card application (fingerprint template and cardholder photo). A NEXGEN TWIC card has all biometric information available in both the TWIC and PIV card applications. For the NEXGEN TWIC, the biometric data in the card is encrypted in the TWIC card application for privacy protection and is digitally signed for authenticity assurance. The biometric template information is also available without encryption in the PIV card application but requires a PIN presentation. For this mode, the CHUID content signing certificate needs to be used to verify the biometric template digital signature. **This mode provides a good level of authentication that the cardholder is legitimate (one factor - who you are).**

4.2.6 Mode 4 - CHUID Verification and ACA and Biometric Verification

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

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

In this mode, supported only in NEXGEN TWIC cards, in addition to verifying the CHUID information and its signature (Mode 1), the user digital facial photo is read from the card, deciphered and its digital signature verified. The reference cardholder photo from the card is then displayed on the TWIC reader (or a display it is connected to) for the operator to compare with the cardholder life image presenting the card. **This mode provides a good level of assurance (One Factor - Who you are but requires an operator).**

4.2.8 Mode 6 - CHUID Verification and RPV and ACA

This mode provides two factor authentication. In addition to the CHUID verification (Mode 1) and Active Card Authentication (Mode 2), this mode verifies (as in Mode 5) the digital signature of the cardholder photo (reference Picture Verification) and then displays it for an operator to compare to the cardholder presenting the card. This mode, available only on TWIC NEXGEN cards, provides a **very good level of assurance (two factors: Who you are and what you have, but requires an operator).**

5. Verification Devices and TWIC Readers

This documentation considers three types of verification devices that may be used to verify the cardholder's TWIC card. Refer to Part 3 of this documentation series for more details about the various types of readers[25]. They are:

- **TWIC Readers (two types):**
  - **Fixed Physical Access Control Reader** – a TWIC reader installed in a wall, on a turnstile or similar type installation. A fixed TWIC reader normally 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 weather. Fixed TWIC readers may have a bi-directional or a one-way communication with back-end systems to which they are connected.
  - **Portable Verification Reader**– a handheld TWIC reader that may be used for portable, spot-check identity verification, including verification of the card identifier against the CCL for canceled cards. A portable TWIC verification reader may also have the ability to wirelessly communicate with an external access control system to control a door, gate, etc.
- **Card Verification Device** – These devices do not a interface with the smart card chip of the TWIC card, but use elements/information printed on a TWIC card (e.g. verification of the card not being canceled using the CIN), available even when the chip on the card is not functional.

Notes:

- The generic term "**TWIC reader**" is used in this documentation series for all readers and devices communicating electronically with the TWIC card by using the contact or the contactless interface. Fixed and Portable readers are TWIC readers described in detail in Part 3 of this documentation series. These TWIC readers are to be used by access control systems in vessels or maritime facilities, as well as for spot check verifications with the TWIC card.
- **Card Verification Devices** are not TWIC readers but may be used to supplement visual inspection of TWIC cards.
- **PACS using TWIC cards:** Part 4 of this series of documents provides guidance on how to register TWIC cards in a PACS system for use by TWIC Readers and how to take advantage of the new features available in NEXGEN TWIC cards, such as E-Stickers.

[25] See Section 4.5 of NEXGEN documentation Part 3 for more details

6. Main Differences Between TWIC Legacy, TWIC NEXGEN, PIV and PIV-I cards

As TWIC cards have evolved, the main differences between Legacy TWIC cards and NEXGEN TWIC cards are important, but NEXGEN TWIC cards maintain backward compatibility with Legacy TWIC cards. These differences may have an impact on the card usage by the TWIC reader as well as the card registration system in the PACS if required.

The NEXGEN TWIC and Legacy TWIC cards both have two card applications loaded by TSA in the card.

1. A **PIV card application** which is aligned with the NIST PIV card specification but does not adhere to the PIV-I trust model (and instead implements a closed trust model within TSA).
2. A **TWIC card application** which can be used independently of the PIV card application.

6.1 Differences between TWIC and PIV/PIV-I cards

Brief comparison between PIV cards and TWIC cards:

- PIV: Designed to be a Government Online Identity Credential
  - Always requires a PIN (when On Card Comparison – OCC) is not supported) to authenticate the cardholder
  - The card must be activated at the end of the issuance process with the cardholder present
  - The card must be re-activated (or changed) every three years
  - The card is issued by Federal Agencies to Employees and Contractors
  - Cost of card issuance borne by the issuer (often decentralized): $200 to $250
- TWIC: Designed to be a privately used Identity Credential for Physical Access
  - Modeled after the ICAO e-Passport identity credential for trust and privacy protection[26]
  - Contains both a PIV card application and a TWIC card application
  - Cards can be mailed fully activated by the TWIC card issuance system to the address provided by the applicant[27]
  - The card is issued for a period of up to five years
  - The card is issued by DHS/TSA to any qualified[28] person applying for it (for a fee)
  - Cardholder pays for the enrollment, background check and issuance of the TWIC card
  - Cost to cardholder is currently $125.25 (as of July 2022)[29].

Some requirements imposed by Federal law on TWIC cards are not possible to be met with PIV cards:

- TWIC cards offer the option of being **mailed directly** to the user (if requested) without the user having to come back to an enrollment center to be verified biometrically prior to card activation. PIV cards must be activated with the user being physically present at the end of the issuance process and cannot be mailed.
- TWIC cards are valid for up to **five years** after issuance without requiring the user to come back to an enrollment/activation center. PIV cards can be issued for up to six years but have their certificates valid only for a period of three years.
- TWIC cards are used to biometrically authenticate the cardholder's fingerprint without requiring a PIN to be presented at the point of access. PIV always requires the user to present a PIN when biometric or personal information (e.g. fingerprint) is to be used by a reader.

[26] See documentation ICAO 9303 for details (https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf)
[27] Mailing Cards to TWIC applicants is required to be an option by law (2012 House Bill H.R. 3173).
[28] TSA runs a security threat assessment background check on the applicants to verify identity and eligibility.
[29] See https://www.tsa.gov/travel/frequently-asked-questions/how-much-does-twicr-card-cost

6.2 Technical Differences Between Legacy and NEXGEN TWIC Cards:

The differences between Legacy cards and NEXGEN cards are summarized below (the details can be found in Part 2 of this series of documents):

- NEXGEN TWIC cards no longer have a magnetic stripe on the back of the card[30].
- NEXGEN TWIC cards have a two-dimensional bar code on the back of the card containing (among other data) the card-specific TWIC Privacy Key (TPK).
- Printed Security features on the NEXGEN TWIC cards have been enhanced[31].
- All digitally signed data objects in NEXGEN TWIC cards contain a fully populated Card UUID.
- All certificates in NEXGEN TWIC cards use SHA-2 hashing code instead of SHA-1 as used in Legacy TWIC cards[32].
- The TWIC card Application Identifier (AID) has changed from:
    - A0 00 00 03 67 20 00 00 01 01 01 in Legacy TWIC Cards to
    - A0 00 00 03 67 20 00 00 01 01 03 in NEXGEN TWIC cards
- The TWIC card application now has its own Card Authentication Key and related public key certificate. This private key allows active authentication of the NEXGEN TWIC card without having to select and use the PIV card application.
- Many data objects have been added in the TWIC Card application (e.g. Discovery Object, Cardholder photo, written signature, printed information). Most of these objects are protected by encryption using the TWIC Privacy Key and most of them are authenticated using a digital signature. These added objects are accessible on both the contact as well as the contactless interface.
- Ten free read-write new Data Objects called E-Stickers have been added to the data structure of the NEXGEN TWIC card. These objects can be read, written, and updated by any external application using the TWIC card application. Examples of their use are provided in Section 3 of the NEXGEN TWIC Part 4 document: “New feature in NEXGEN TWIC cards: E-Stickers”.
- Four new Data Objects called TSA controlled E-Stickers have been added to the data structure of the NEXGEN TWIC Card. These objects can be read freely over the contact as well as over the contactless interface but are created/updated under the card issuer control even after the card has been issued to the cardholder.

[30] The Magnetic stripe is optional on Federally issued cards as described in FIPS 201-2 section 4.1.4.4 for Zone 3B

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

[32] Some Legacy Cards may also use the SHA-2 hash algorithm.

7. Appendix A - Authentication Processing

7.1 Terminology: Differences Between Identifiers and Authenticators.

An **identifier** is a unique number which is generated and assigned by an authority to identify a person, an object, or a case. In the TWIC card, there are two identifiers. One identifier created to track the physical card and known as the Card Identification Number (CIN) found printed on the back of the card. The other identifier is the Unique Credential Identifier (called the Federal Agency Smart Credential Number (FASC-N), created by a Credential Management System of TSA (The FASC-N value can be found in the chip card itself) and identifies the logical credential issued for a given user[33]. The FASC-N information can also be found in the UUID (value present in the GUID of the CHUID and the Card UUID) as described in Part 2 Appendix D.

Authenticators always have an element which must be protected and should be kept secret and not shared. There are three types of authenticators:

- Passwords/Passphrases (used by a system to verify what the user should know),
- Secret/Private Keys and associated X509 certificate (using algorithms to challenge a system about the part of the secret it should know, and
- Biometric reference information (e.g. fingerprint templates, etc.) that allows electronic verification of the person claiming a given identifier or identity as its own.

In TWIC Cards, there are a total of three possible authentication factors:

- the PIV Card Application PIN (used by the PIV card application to authenticate the card holder),
- a biometric reference related to the legitimate card holder, and
- a private key protected by the card which can be cryptographically challenged by a TWIC reader, thereby allowing electronic verification that the card is authentic and was indeed issued by TSA.

Notes:

- **Identifiers** should be considered as public information, as they are displayed/exchanged in clear text and should never be used as authenticators (this is the big problem of the Social Security Number (SSN) as used in the US). Identifiers can be quite easily copied and spoofed by attackers.
- **Authenticators** should be (very) hard to copy, create or modify. They are very often linked to a specific identifier.

7.2 Authentication and Levels of Assurance

To determine the identity of a cardholder, an access control system will 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 face).

A check against an authentication factor is considered "strong" if it is difficult for an attacker to gain control, clone or compromise that factor. An access control system may achieve the required level of

[33] Another example of equivalent identifiers would be the license plate of a car (equivalent to a TWIC FASC-N when the car is registered by an authority), and the vehicle identification number (VIN) allocated by the car manufacturer to the car (equivalent to the TWIC CIN for the card).

authentication security by checking multiple factors against the card presented, the user presenting it, and information stored in its own database.

An **authentication factor** is used to link a claimant[34] 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 indeed the same person who was assigned the identifier and given the password in the first place. This is a simple example of single factor authentication where the password (or PIN) represents a single, "something you know" authentication factor and the username represents an identifier[35].

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

A TWIC card offers four different data elements that may be used to support authentication via the contactless (or contact) interface of the card:

1) CHUID data object – A strong, unique digitally signed **identifier** issued by the TWIC Program after vetting the identity of an individual and determining that said individual is eligible for the program. The CHUID contains a FASC-N identifying the credential provided to the individual.
2) TWIC biometric template – A strong "**something you are**" authentication factor that is strongly bound and unique to the individual. The TWIC biometric template is also strongly bound to the CHUID (identifier) and protected against alteration (counterfeit) by the mean of a digital signature. The biometric technology used for this template is fingerprints[36].
3) Card Authentication Certificate and Key – A strong "**something you have**" authentication factor that is strongly bound to the user's smart card through proof of possession of a never revealed private key that exists only on the user's smart card. The use of the card authentication certificate and associated private key provide strong proof that the smart card being presented to a TWIC reader is a genuine TWIC card that was issued to the individual by a trusted authority.
4) TWIC Card Holder Reference Photo – The photo of the legitimate cardholder ("another **something you are**") is stored in the TWIC card using a high resolution and is digitally signed. It allows a verification device to read and display the legitimate cardholder photo which can be used by an operator to compare with the face of the cardholder presenting the card.

Notes:

1. The CHUID is often referred to as a "weak" authentication factor but is in fact only an identifier. It should be noted that without biometric verification or card authentication, the CHUID is publicly available information (an identifier) that is transmitted over the TWIC contactless (or contact) interface in clear text and as such 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 it is a "weak" verification factor. Even in low assurance applications, the CHUID may be captured and replayed by an attacker without user consent or knowledge.

[34] The person presenting the identification card
[35] TWIC card is not used with a "what you know factor" in any TWIC authentication modes.
[36] IRIS template might be available in addition to fingerprints in the future.

2. TWIC relies on the use of Public Key Infrastructure (PKI) cryptography and includes signatures and certificates in the card. TWIC digital certificates are valid for up to five years. The consequence of these longer life certificates, compared to PIV cards, is that certain fields in the certificate have values that, by policy, are different from PIV FIPS 201[37] cards. These Object Identifiers (OIDs) are described in detail in Part 2 – "TWIC Card Application specification" and can be used to differentiate between various types of cards, all compliant with the SP 800-73 data model (PIV, PIV-I, CIV, TWIC, CAC etc.)[38].

[37] See document from NIST referenced in section 2.1 paragraph [R32]
[38] See document from the Secure Technology Alliance for details: https://www.securetechalliance.org/resources/pdf/PIV_PIV-I_CIV_brief_022212.pdf

8. Appendix B – Pro & Cons of Using the Contact vs. Contactless Interface

The TWIC card is able to interact with a reader using the contact (ISO/IEC 7816[39] compliant) or the contactless (ISO/IEC 14443[40] compliant) interface. For NEXGEN TWIC cards, the information processing is nearly identical between the two interfaces, except when dealing with the PIV card application and presenting the PIV Card Application PIN to the card.

8.1 Contact Interface

The benefits of using the contact interface are:

- Less risk of interferences from electromagnetic fields
- More private transaction exchange as an attack using a "man in the middle" model requires tampering with the reader.

The disadvantages of using the contact interface:

- Mechanical stress on the card and on the reader each time the card is used (removal from the plastic card holder, insertion in the reader, removal of the card, putting it back in the card holder).
- Possible scratches on the surface of the card (mainly on the contact plate) each time the card is used.
- Card insertion path exposure to the atmospheric elements, means that reader contacts can get dirty or oxidize. As a result, communication with the reader may not work properly requiring periodic maintenance to the reader.
- Maximum allowed communication speed with the card is slower using the contact interface, but less sensitive to radio interferences.

There are two types of mechanical contact technology used in Smart Card contact readers:

1. **Sliding contacts** are the less expensive type, but they do scratch the card upon insertion and removal. As such, they help clean the card contacts (the good thing), but also degrade the card surface each time a card is inserted (the bad thing). Since the card scratches the reader contacts, the reader contact physical interface is stressed and the reader contacts have to be changed around every 100,000 card insertions (even when the reader is used with clean cards and in an office environment). For a physical access control site having a thousand employees accessing every day at gates equipped with five lanes (with five readers), this means **the contacts of each of the readers have to be changed at least every year** (this assuming that the employees go out for lunch, using the gates, twice a day). In some harsh environments, the reader contacts must be checked much more frequently and often require even more frequent replacement. Cards used regularly with sliding contact readers may not last five years.
2. **Landing contacts** are a little more expensive than simple sliding contacts but can withstand about twice the number of insertions of sliding contacts. They do not scratch the cards as much as sliding contacts but provide little contact-cleaning benefit when landing on the chip.

Regarding Security:

1. Using readers with a TWIC card contact interface appears to provide more security and more privacy in the data exchange but considering how bank Automated Teller Machines (ATM) machines have been attacked, the prevention against **skimming** as well as **malware** attacks should be considered very seriously for devices with no attendant.

[39] See section 2.1 paragraph [R8]
[40] See section 2.1 paragraph [R9]

2. Contact readers may be disabled using simple **Denial of Service** (DoS) attacks. As such, the use of unattended contact readers should be restricted to applications where all card users do have an interest in having the system operate correctly. Using surveillance cameras might also be a potential solution.
3. Safety issues must also be considered when using contact readers in areas, or during periods of time, with **potentially explosive or flammable material** (e.g. gasoline dispenser) present.

8.2 Contactless Interface

Very often considered less private (as nearly anybody in close proximity can intercept the exchanges between the reader and the card), the contactless interface has its advantages and disadvantages as well:

The benefits of using the contactless interface are:

- No need to remove the card from the protective plastic cardholder. As such, there is no mechanical stress on the card when used.
- Easier card presentation as there is no need to exactly position the card in the contact slot with the contacts in the right orientation.

The disadvantages of using the contactless interface:

- Need to maintain the card within the reader reading range during the whole operation. For example, if the user fingerprint is captured while the card needs to be in communication with the reader, it might be difficult to hold the card and present the fingerprint at the same time (such a design is not recommended).
- Risk of electromagnetic interferences (e.g. microwaves)
- Risk of a "man of the middle" attack with an attacker listening to the exchanges between the card and the reader. This is mitigated in the TWIC card as the user information exchanged is always encrypted by a key which is not available on the contactless interface. A similar mechanism is used for e-Passports called Basic Access Control (see document ICAO 9303 for more details).[41]
-

Regarding Security:

1. Using a TWIC card contactless interface provides the same level of security (and risk) as a contact interface since all the important information exchanged is digitally signed and encrypted. But the reader may also be attacked using **skimming** as well as **malware** attacks and the reader should be protected against such attacks.
2. Contactless readers may also be disabled using a simple **Denial of Service** (DoS) attack. As such, the use of unattended contactless readers should be restricted to applications where all card users do have an interest in having the system operate correctly. The use of surveillance camera might also be a potential solution.

[41] SP 800-73 offers another method to prevent this from happening by using the Virtual Contact Interface (VCI) which provides active encrypted exchanges between the reader and the card.

9. Appendix C – Threats, Vulnerabilities and Countermeasures – An overview

The TWIC card is used to verify an identity as well as to indicate eligibility for unescorted access to a regulated maritime facility or vessel.

The access decision for a given cardholder is under the control of each maritime facility.

Verification during the TWIC Card application process: The identity of the applicant is verified by TSA when the person applies for the card; and background checks are conducted by TSA to verify that the cardholder is eligible (see https://www.tsa.gov/for-industry/twic for details).

Verification during the TWIC Card usage process: When a TWIC card is presented for use (e.g. physical access to a site), the following elements should be verified:

- **Genuine Card:** The card is a legitimate TWIC card issued by TSA. This can be verified by an operator carefully examining the printed security features, or more effectively by executing an active card authentication (TWIC mode 2).
- **Active Card:** The card has not been revoked (or canceled) and has not passed its validity date. This can be achieved by checking expiration date of the card as well as the card FASC-N against the CCL, or the card CIN against the Visual CCL.
- **Cardholder Identity:** The TWIC card contains information related to the legitimate cardholder. The Legitimate Cardholder photo is printed on the front of the TWIC card, and a digitally signed photo is stored in the card. The fingerprint templates of the legitimate cardholder are also stored in digital format encrypted, digitally signed in the card and could also be verified.
- **Card digital information**: All information in the card is digitally signed, allowing the operator to verify that the information is genuine (certified by TSA), not modified or invented, and coherent (all data objects in the card have the same card identification number or FASC-N to link the signed data to the given card). This provides assurance that the information was indeed created by TSA (the identity certification authority), has not been copied from one card to another, and has not been tampered with (integrity of information and trust in issuance authority).

Note: TWIC NEXGEN uses the FASC-N or the UUID to identify TWIC cards as both containing the same number identifying the card (see NEXGEN documentation Part 2 Appendix D).

9.1 Threats & Vulnerabilities

- **False Card:** The card was not issued by TSA. This can be detected by carefully examining the security printed features of the card; but for better assurance, a CHUID Verification should be performed, and for a higher level of assurance, an Active Card Authentication should be conducted.
- **Expired Card:** The card expiration date printed on the card should be verified; but for a more automated verification with a higher level of assurance, CHUID verification (or an Active Card Authentication) should be executed.
- **Canceled card:** When the eligibility of a cardholder changes, his/her card may be canceled (or suspended) by TSA, even before the card expires. This can be checked by using a Supplement To Visual Inspection (CIN checked against the Visual CCL), or a CHUID/FASC-N verification (check against the CCL), or an Active Card Authentication (which also checks against the CCL).
- **Misuse of a valid card by an impostor:** Verifying the photo printed on the card with the person presenting the card is a simple step; using the Reference Picture Verification provides a better assurance, and doing a Biometric Authentication is even a higher, very secure method and which may not require an operator.

- **Incoherent information on a card:** The CHUID information of a TWIC card can be read freely and could be copied on a false card. But in doing so, the cardholder identifier would not be the same on other data objects of the same card. This is why, when any user-related information is used (photo or fingerprints), it must be verified that each data object has the same Cardholder Identification number (FASC-N). Finally, there is at least one information which cannot be moved from one card to another. It is the Card Authentication Key, and as such the attached Card Authentication Certificate cannot be moved either. So, by verifying that all data objects have the same cardholder identifier and that an Active Card Authentication is successful, proves that the card is genuine and all information in it belongs to the legitimate cardholder.
- **Denial of Service[42]:** When the electronic chip of the card is destroyed, the card electronic functions are no longer available. This could be caused by a malfunctioning chip (rather rare, but possible), or because the chip was broken intentionally by an impostor attempting to use the card only as a flash pass and intentionally limiting the operator's options for possible electronic verification.

9.2 Countermeasures

The table below summarizes the actions (countermeasures) to take to circumvent a given vulnerability. For each countermeasure, the terms Low (+), Medium (++) or High (+++) indicate the level of assurance provided.

Table 2 – TWIC Cards Modes of Operation

Mode of Operation	Mode #	Operator Required	False Card	Expired Card	Cancelled Card	Impostor Identity	Incoherent Information	Denial of Service
Flash Pass	Manual	Y	+	+	-0-	+	-0-	-0-
Electronic Flash Pass	Mode 0	Y	+	+++	+++	+	-0-	-0-
CHUID Verification	Mode 1	N	++	+++	+++	-0-	-0-	+++
Active Card Authentication	Mode 2	N	+++	+++	+++	-0-	+++	+++
CHUID and Biometric Verification	Mode 3	N	++	+++	+++	+++	+++	+++
CHUID and Active Card Authentication (ACA) and Biometric Verification	Mode 4	N	+++	+++	+++	+++	+++	+++
CHUID and Reference Picture Verification (RPV)	Mode 5	Y	++	+++	+++	++	+++	+++
CHUID and Reference Picture Verification and Active Card Authentication	Mode 6	Y	+++	+++	+++	+++	+++	+++

Note: a symbol "-0-"in a cell indicates the mode of operation does not address at all (or is not relevant to) the threat listed in the column.

[42] See definition at https://techterms.com/definition/denial_of_service

10. Appendix D – Differences between CCL, VCCL and CRLs

This section provides a brief explanation concerning the TWIC Canceled Card List (CCL), the TWIC Visual Canceled Card List (VCCL), and the TWIC Certificate Revocation List (CRL).

The TWIC card supports three types of card unique identifiers:

- The **Card Identification Number (CIN)** is provided to uniquely identify the physical card. The CIN is printed on the back of the card in the lower left corner and is part of the linear one-dimensional (1D) bar code. This unique number is always visible, even when the chip in the card is not functioning. The Visual Canceled Card List (VCCL) is published every day by TSA and contains those card identifiers (CINs) which have been canceled or suspended and have not yet expired. The size of this list is currently 2 MB and can be found at https://universalenroll.dhs.gov/canceled-card-lists .
- **The Credential Identifier** is a unique identifier represented in the card data model. This identifier be found in the CHUID under the CHUID sub-field named the FASC-N. The list of non-expired canceled (or suspended) credentials is published daily by TSA (CCL) and can be found at https://universalenroll.dhs.gov/canceled-card-lists. The size of such a list is currently 9 MB.
- All TWIC cards contain several certificates attached to private keys in the card. When a certificate is revoked, it appears on the Certificate Revocation List (CRL) published by the Certificate Authority managing the trust of the system. In TWIC cards, the certificates and the card have the same life (up to 5 years), which is not always the case for PIV / PIV-I cards. For TWIC, the CRL may be used but suspended cards will not appear on it, and the size of this file is much larger than the CCL; 16 MB or more.

Note: A simple analogy can be used to understand the differences between the CIN, the FSC_-N and the Certificates of a given card.

- The CIN is to the card what a VIN (Vehicle Identification Number) is to a car.
- The FASC-N (or the Card UUID) is to the card what the tag number (License plate number) is to a car.
- The Certificates are equivalent to the insured driving licenses of the people allowed to drive the car.