Important note from TSA-TWIC regarding the TWIC NEXGEN & Legacy documentation

The TWIC NEXGEN & Legacy 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 before July 2024)
- TWIC NEXGEN (cards produced now).

IMPORTANT Notice: The TWIC card NEXGEN data model, described in these documents, has been designed to be backward compatible as much as possible with TWIC the Legacy data model, but it is important to confirm that existing TWIC readers are compatible with both TWIC Legacy (which will be used in the field until 2029) as well as the new TWIC NEXGEN data model even if used in backward compatibility mode.
In early 2024 changes were implemented for Legacy TWIC Cards These Legacy TWIC cards issued in 2024 do not strictly comply with the original 2012 documentation (see below).

- 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 was changed and the ATR of the chip has been different.
- In July 2024, another different chip has been used for TWIC NEXGEN card. The ATR is the main difference; all the application data are still compliant with the TWIC data models as described in the TWIC NEXGEN & Legacy Part 2 Specification. There may be some minor difference in the options used by the low-level ISO/IEC 7816 protocol between the previous chip and this latest one.

All the TWIC documentation is freely available on the TSA Web Site at: https://www.tsa.gov/twic by selecting the tab TWIC Technology.

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

This page was last updated on October 11, 2024

Transportation Worker Identification Credential
TWIC® Specification

Part 4 – TWIC® uses and registration by a PACS

July 2024

Gilles Lisimaque

Gerald Smith

Lars Suneborn

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	Modified version incorporating Round 1 comments for Industry
October 2019	Text revised for publication
January 2020	Modified version incorporating the comments from the Round 2 industry review
October 2020	Added some guidance on CCL downloading by the PACS in section 2.6
June 2021	Modification of some tags for coherence between PIV & ISO
January 2022	Added the four TSA controlled E-Stickers.
April 2022	Added information that this may not be the final release
July 2022	Added information related to the PIV Application PIN and the TWIC Application PIN used in NEXGEN
June 2023	Information added about the PIV and the TWIC PUK used to reset the application PINs when needed
July 2023	Added the example of a TSA digitally signed e-sticker to be added in the card when a TWIC card is activated for a Trusted agent
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 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.

Table of contents

1. Overview

1.1 Abstract

The Transportation Worker Identification Credential (TWIC®[1]) documentation consists of five parts which are linked. The fourth part (this document) provides some guidance on how TWIC cards can be used by a Physical Access Control System (PACS) and how they can be registered in a PACS to optimize the customer experience without degrading the security level.

This document uses the concepts presented in the first three parts of this series of documents and but does not repeat the detailed explanations of the concepts.

Because the TWIC card exists in two different versions (**Legacy TWIC** and **NEXGEN TWIC**[2]), this document will indicate what can be done, or needs to be done, with each of the type of TWIC card.

Some suggestions are also added to this fourth part in relation with the use of NEXGEN TWIC E-Stickers which are available only in NEXGEN TWIC cards.

1.2 Scope and purpose

This **document (part 4)** fits in the series of documents related to the TWIC credentials:

- 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
- Part 4 – **TWIC uses and registration by a PACS**
- Part 5 – (Future) TWIC activation into a PIV-I compatible credential[3].

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 this series of specification. As cards are issued for a period of five years, the new version of card described in this specification (called NEXGEN TWIC), does not exclude the millions of legacy TWIC cards issued prior to the deployment of NEXGEN TWIC cards conforming to this new card specification. The TWIC readers will be required to work with the prior version of the TWIC card for at least five years after NEXGEN cards will be provided to TWIC cardholders.

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

[1] TWIC® is registered in the U.S. Patent and Trademark Office by the U.S. Department of Homeland Security.
[2] Part 2 of this series of documentation exposes in depth these two types of card data model.
[3] Part 5 is deferred for future publication since it is dependent on expected modifications to TSA's Technology Infrastructure Modernization (TIM) program and the development of PIV-I activation stations.

1.3 References

For all general references, see Part 1 Section 2 of this series of documents.

- The PIV in E-PACS document[4] published by the U. S. government Identity, Credential and Access Management (ICAM) group for the use of PIV cards in government PACS might be helpful in understanding the various security threats and countermeasures which are available when smart cards are used. It should be noted that since the TWIC card has more functions than the PIV card and does not require the entry of the user's Personal Identification Number (PIN) for any of its functions (except for registration in a PACS of Legacy TWIC cards), the PIV in E-PACS document has some significant differences in the implementation of certain functions.

- Other good reference sources are provided by the Secure Technology Alliance (STA) through several white papers and publications related to PIV, Personal Identity Verification Interoperable (PIV-I) and Commercial Identity Verification (CIV)[5]. Note that NEXGEN TWIC more closely fits into the category of a CIV credential but uses a trust model similar to e-Passports.

- Informative guidance related to E-Sticker use is under development: Available documents:
  NEXGEN TWIC E-Stickers Vxx.pdf
  PACS usage of NEXGEN E-Stickers.pdf[6].
- Information about FASC-N[7] structure:
  PIV_Interoperability_Non-Federal_Issuers_May_2009.pdf[8]

1.4 Definitions

The same definitions provided in Part 1 Section 3 do apply for this document.

Some specific terms related to PACS are defined in this document in Section 2.2.

Any other new term specific to this document will be defined in the text of the document the first time it is used.

SP 800-73-4 allows each card application to use its own PIN (code 0x80) instead of the global Card Application PIN (code 0x00). Because of the behavior of Legacy TWIC cards which have been using the local application PIV Card Application PIN (as indicated in SP 800-73-1), in order to preserve backward compatibility, the TWIC NEXGEN card keeps this behavior. This information is noted in the discovery data object of each card application.

Note:
In both card applications (PIV and TWIC), a discovery data object has been added to indicate, for each individual card application, how the PIN is accepted/used. In the PIV Card Application, the PIN is a local card application PIN, and the TWIC card application indicates the TWIC card application does not have a PIN available. (see Part 2 and Part 3 for details).

---

[4] The full document name is: *Personal Identity Verification in Enterprise Physical Access Control Systems_v3_20140326.pdf*. It can be downloaded at https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/PIV-in-EPACS.pdf.
[5] These documents may be found at: https://www.securetechalliance.org/publications-physical-access/
[6] To obtain the latest version of these documents, send a request to TWIC-Technology@tsa.dhs.gov
[7] Federal Agency Smart Credential Number
[8] This document may be obtained at https://www.securetechalliance.org/resources/icam/PIV_IO_NonFed_Issuers_May2009.pdf

2. TWIC use by Access Control Systems

2.1 General

Access control Systems can be separated into two main categories:

- Automated systems, in which the physical access of a given individual is not supervised by a guard or a security officer at the time of access, OR
- Attended access control systems, in which an operator/guard[9] is involved in verifying the credential presented by a given individual and making the access decision.

It must be understood that the possession of a TWIC card provided by TSA does not automatically grant any specific access privileges - even to the legitimate cardholder.

Local access privilege is assigned as appropriate under the complete authority of each physical site location operator (facility, vessel, etc.) based on their determination of a need to grant unescorted access privileges for a given individual. The main function of registering a TWIC card in a PACS is to attach the correct access privilege(s) to a specific TWIC card for the physical site the PACS is controlling. PACS registration also allows specific cardholder information to be used as needed by the PACS (e.g., card expiration date, photo of the cardholder, etc.). The local access privilege granted to the cardholder could be limited to some specific areas, days/dates, and/or times of the day as well as in consideration of MARSEC[10] levels as determined by the maritime operator and the U.S. Coast Guard. This type of decision information is not present on the TWIC card issued by TSA and must be maintained by the PACS for each given TWIC card. The TWIC provides identity verification but the Authorization for access is decided by local security policy and entered in to the PACS for each card holder.

The TWIC card can be identified by the PACS using any of the unique identifiers in the card as follows. This varies depending on how the card is presented to the PACS or the TWIC Reader[11] (visual, contact, contactless, etc.):

- **FASC-N:** The Federal Agency Smart Credential Number is a unique card number found in the Card Holder Unique Identifier (CHUID) data object (available on either the contact or the contactless interface) or any signed data object in the TWIC card application. The structure of a FASC-N can be found in the document "*PIV_Interoperability_Non-Federal_Issuers_May_2009*"[12] on page 15.
- **UUID:** The Universally Unique Identifier in NEXGEN provides **a** unique Card Identifier on 128 bits (16 bytes). The Card UUID is available on cards issued under NEXGEN specifications in any signed object stored in the card. It can be accessed through the contact or contactless interface. The structure of the Card UUID used in NEXGEN cards allows the FASC-N to be extracted from the card UUID for backward compatibility (see Part 2 for the details of the Card UUID construction for NEXGEN TWIC credentials).
- **CIN:** The Card Identification Number is a unique card identifier that is printed on the back of the card as human-readable numeric information and in the form of a linear one dimensional (1D)

[9] The guard may be in a remote location not close to the cardholder and connected using a CCTV system.
[10] Maritime Security
[11] See definition of this term in section 2.2
[12] This document may be obtained at https://www.securetechalliance.org/resources/icam/PIV_IO_NonFed_Issuers_May2009.pdf

bar code[13]. The barcode data consists of 16 digits; the first four digits are a constant Agency Code (7099 identifying TSA) and the next four digits identifies the enrollment center; combined, these eight digits consists of the Issuer Identification Number (IIN), the last eight digits of the bar code being the unique identifier for this given card[14]. This number (Card Identification Number – CIN) is used in the Visual CCL control mode of operation[15], or when the chip of the card is not functioning. The eight digits of the CIN is not recommended to be used as a primary identifier for PACS systems[16] as it is not digitally signed.

Note: A simple analogy can be used to understand the difference between the CIN and the FASC-N 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 are to the card what the tag number (License plate number) is to a car.

2.2 Elements available to a PACS and terminology

A PACS has multiple components that work together to provide the security required by the facility it controls. This section provides a high-level description of the different elements available for a PACS and their functions. Depending on how the PACS is configured, it may use some or all of these functions. Some of these functions share similar security features with e-Passports which are machine readable travel documents used for border crossings.

Authoritative Source: In the TWIC system, TSA delivers the card only after verifying the applicant identity and checking his/her background for eligibility. All of the information (such as name, card identifier, validity date, etc.) is digitally signed (using the TSA-TWIC root of trust) by the certification authority.

Credential: Issued by TSA, the TWIC card is a credential that provides an identity document as well as assurance that the legitimate cardholder is eligible for unescorted access to regulated maritime facilities and vessels in the United States. The credential (issued for five years) contains a validity date which allows the verifier to know if the identity document is expired[17].

Certification Authority (CA): working on the behalf of TSA, the CA digitally signs all cardholder related information stored in the TWIC card. This provides assurance of authenticity (Proof of Trusted Origin) as well as integrity (not tampered with) of the information. The CA also maintains a list of certificates that have been revoked called a Certificate Revocation List (CRL). The root of trust consists of a public certificate which can be used to verify all the digital signatures attached to the card information.

Certificate Revocation List (CRL): This list is published by the Certification Authority and contains the identifier of all unexpired card certificates which have been revoked. In TWIC, as the card life (five years) is identical to the certificate life used in cards, canceling a certificate is equivalent to canceling the card itself.

[13] This linear bar code is common to Legacy TWIC and NEXGEN TWIC cards. NEXGEN TWIC cards do have an additional bar code (two dimensional PDF417) replacing the magnetic stripe. See Image of the back of the card in Part 2, section 1.4 Page 9)
[14] This structure limits the maximum total number of cards issued by TWIC to 99,999,999
[15] See Part 3 for this specific mode of operation.
[16] The CIN is not part of the digital information signed in the card and as such may be subject to attacks with fake cards.
[17] At this point in time, TWIC cards are not Real-ID compliant as the expiration date of the card is not linked to (or limited by) the immigration documents which may limit the legal residence in the United States of an applicant.

Trust Anchor: In Public Key based systems, such as TWIC, the certification authority publishes the public key which allows anyone to verify the digital signatures in all the credentials issued. The same mechanism is used for electronic passport (e-Passport) issuance where each country provides its trust anchor allowing anyone to verify that the information in the e-Passport is legitimate and should be trusted by the verifying entity.

Canceled Card List (CCL): This is a list of TWIC cards published by TSA that contains all unexpired TWIC cards that have been canceled or suspended. The CCL is simpler to use than a CRL for card validation purposes. The structure of the CCL also allows suspended cards to be re-instated. The CCL uses the card FASC-N to identify the cards instead of the card certificate numbers and is updated each day by the TWIC system. Cards which have expired are not in this list[18].

Card Issuance System: TWIC cards are printed and issued by the U.S. Government Printing Office; they may be mailed directly to the participants or to an enrollment center for the applicant to pick up. This process is quite different from many private PACS that issue their own access control cards. In such a case, the private entity is also responsible for the provisioning system including enrollment, vetting, card issuance and revocation.

Local authorization: The possession of a valid TWIC credential by the legitimate cardholder does not automatically grant access privileges to any facility. It is up to the local operator to decide if the cardholder has a legitimate reason for unescorted access. This is very similar to possessing a valid passport but also needing a visa to enter another country. Traditionally, this access privilege (the local authorization) is stored in the PACS and linked to the credential/card identifying the legitimate user. With NEXGEN cards, as in e-Passports for visas, it is now possible to additionally store the user's local access privileges in the TWIC card itself. This allows the local operator to verify the card without the reader being online with the PACS (see use of E-Stickers in section 3.1 of this document).

Card Verification Device (CVD): The CVD is defined as a device that verifies information about a TWIC card; but does not use the electronic interface of the card. CVDs can be portable (such as a smart phone) or fixed (such as a PC).

Cardholder: The cardholder is the person presenting the TWIC card to an operator or a reader device and thereby claiming that the person is the legitimate cardholder. After the cardholder identity and card itself are verified, the cardholder is deemed to be legitimate.

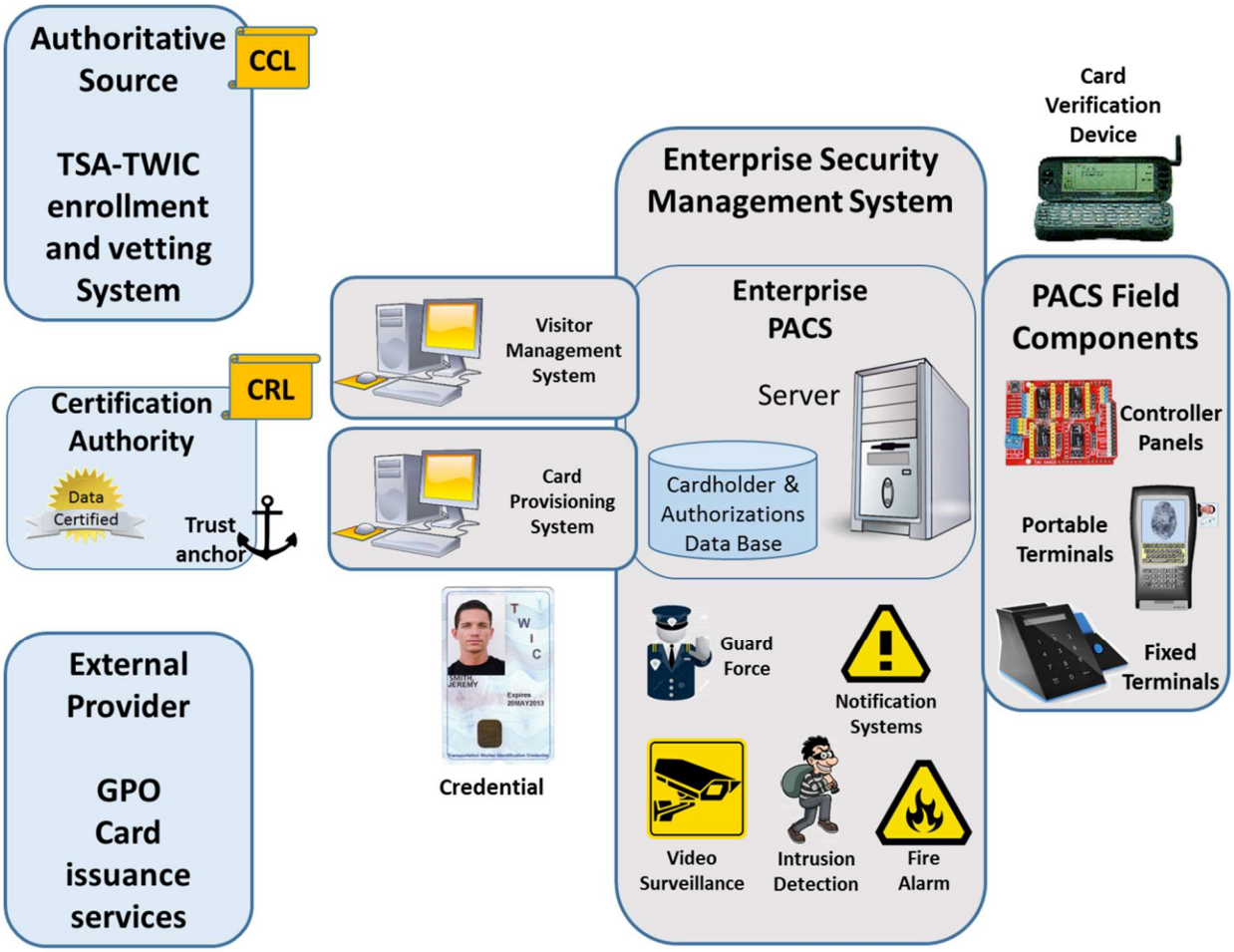
Legitimate Cardholder: This is the vetted person to whom TSA originally issued the TWIC card and where the person's personal and biometric information is printed on and/or stored in the TWIC card.

Operator/Guard: This is a person in charge of verifying the validity of a TWIC card, and/or the cardholder that is presenting the card. This person (usually a security guard) may also determine or verify if the cardholder has legitimate access rights to the facility (authorization privilege verification in addition to identity verification).

TWIC Trusted Agent: These special agents operate the TWIC activation centers and are also involved in the TWIC application process. Their TWIC card has a special activation procedure allowing them to access Federal Computer networks.

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

The diagram below provides an overview of a PACS using a TWIC credential:



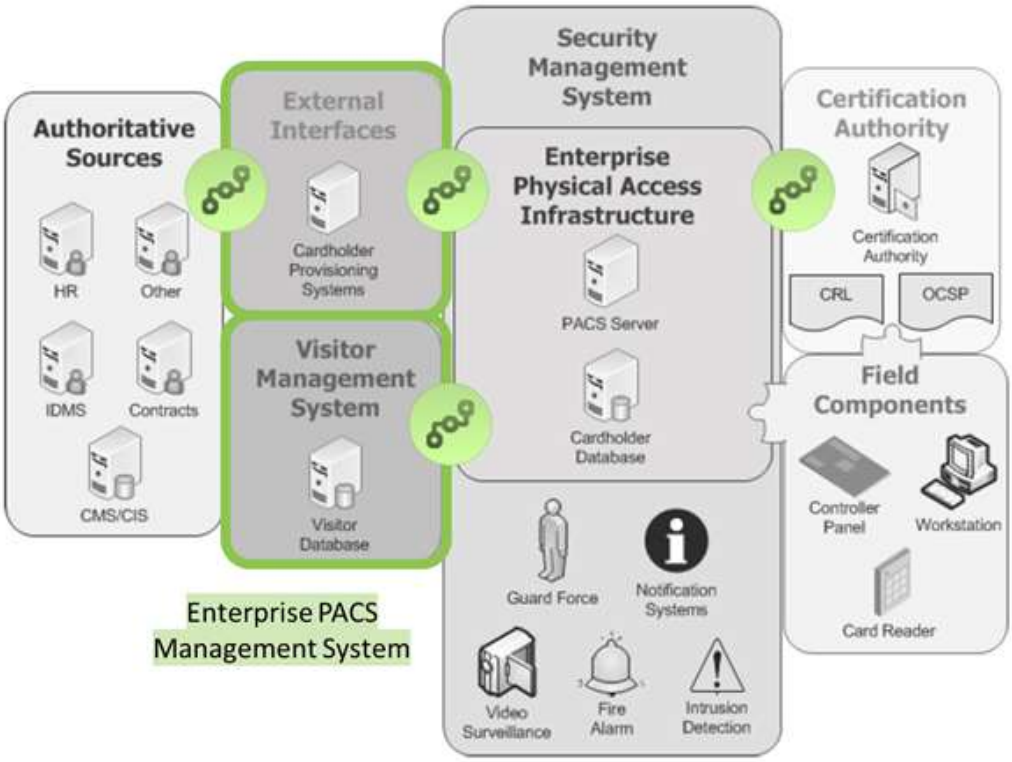
Simplified diagram showing the various sub-systems of a PACS using a TWIC card

The left of the diagram represents the elements of the system under the control of the TSA-TWIC system (blue background), and the other elements (in gray background) are under the control of the local maritime operator.

As in all simplified diagrams, not all of the details of the components are represented. For example, the PACS operator usually maintains a local Card Cancellation List of its own (Local CCL) which contains credentials for which the local access authorization has been revoked - even if the card expiration date has not been reached. Such cards are still valid as TWIC cards and could be used in other facilities, but the access privilege attached to them have been canceled in this local PACS facility.

The Card Verification Device on the top right corner of the diagram is shown outside of the PACS as it is often used as a standalone device not connected to the PACS, for purposes such as CIN Visual CCL verification (Supplement to Visual Inspection mode).

Chapter 10 of The Federal Identity Credential and Access Management (FICAM) Roadmap and Guidance provides a slightly different notional architecture for the components of an enterprise PACS environment.



This representation is given for comparison in this document as it mainly applies to Federal Systems and enterprise **PACS issuing their own cards**[19]; when the TWIC card, issued by TSA, is used in a commercial environment in various unrelated PACS. The following differences between the two diagrams must be understood as they have consequences in the architecture of the PACS and the use of the credential:

- The TWIC card is issued by TSA-TWIC (authoritative Source) independently of the enterprise system itself. As such the PACS must register the TWIC card for local access authorizations.
- TSA publishes the CCL (and the VCCL) for all TWIC cards which have been cancelled. The PACS must use the current CCL (which is updated daily) to determine if the access authorization for a presented card is still valid
- The Certification Authority is under the control of TSA and provides the public key(s) to enable all relying systems to verify that the digital signatures in TWIC cards are valid, providing certification of origin (trust) and guarantee of data integrity. The PACS must have access to the roots of trust in order to verify digital signatures of presented TWIC cards.
- The Certification authority also publishes the CRL which can be (optionally) used by the PACS to verify cards which have been revoked, in addition to the CCL.

[19] One of the biggest issues with Federal Systems based on this simplified model is that it makes it quite complex for one agency to accept, recognize and trust cards issued (and provisioned) by another agency.

- The TWIC cards are printed by the U.S. Government Printing Office (GPO) and issued to the Cardholders directly without involving/informing any specific local PACS operator or employer.
- The TWIC issuing authority (TSA) is not involved in local access authorizations which are under the sole control of the local site operator.

Note: The NEXGEN TWIC card now allows certain card elements to be created (and managed) by the local PACS (such as an access authorization to a given facility for specific days or times). This potentially allows the credential to be used by a TWIC Reader as if it was a locally issued credential, or with a reader not connected to a PACS, even when there is specific access authorization pertaining to the local site[20]. In other words, it is like the PACS issued its "local virtual credential" but is in fact loaded it in the TWIC card of the cardholder (notion of e-Stickers)

2.3 Spot verification

Not all sites need to register TWIC credentials for local access. For example, when a truck driver appears for the first time at a maritime facility, possession of a valid TWIC card and a document from its company providing information about the purpose of the visit may be sufficient to grant access. In such a case, the verification of identity, purpose and legitimacy of the card (verified by an operator) may be all that is required. The access system may then just be used to log the TWIC credential number, identity of the driver and vehicle and possibly the reason for access. A full local registration into the PACS would not be required in such a situation but depending on the level of security required by the site, the TWIC card will have to be verified/authenticated.

Devices used for this type of operation might be TWIC Portable readers (see Part 3 of this series of documents), or a simpler Card Verification Device such as a smart phone or a tablet using an application able to verify TWIC cards identifiers and check for the cancelled cards (CCL or Visual CCL). Depending on the capabilities of the reader, and the security requirements of the local site, multiple reader modes of operations are possible – including biometric verification of the cardholder (see Part 1 Section 4.3).

Some TWIC modes of operation requires an operator[21] to make the decision regarding access (or presence) once the cardholder's identity has been checked using its TWIC credential.

It is interesting to notice that the "local access (or presence) decision" (which is normally one of the functions of the PACS) may now be registered in the card itself using the NEXGEN TWIC E-Sticker capabilities (see example in section 3.1 of this document). This E-Sticker capability allows to verify, for example, that the cardholder has indeed been granted local access by the PACS management even with a TWIC Reader not online with the PACS itself.

2.4 No change in Managing the PIV Card Application PIN in NEXGEN cards

In legacy as well as in NEXGEN cards, the PIV Card Application PIN is used by the cardholder to access some information (e.g. the cardholder picture). If forgotten, it can be reset at one of the UES activation centers where the legitimate cardholder has to present its TWIC card and be biometrically authenticated.

[20] This notion of local authorization loaded in a NEXGEN TWIC card is very similar to a VISA given by a country to a passport holder of another country, or like a PACS issuing its own credential and loading its image in the TWIC card of the cardholder.
[21] The operator may be remote and should have access to a reference photo to compare with the live image of the person presenting the TWIC.

2.5 Physical Access Control System (PACS) Card Registration

Functionally, PACS card registration is used to verify that a given legitimate cardholder has authorization for access to a given area at a given time. This means that in addition to verifying the identity of the cardholder, at one point in time, the PACS has registered the cardholder identity and linked that identity to an access privilege. This privilege could include some restrictions such as specific areas, days and hours and/or MARSEC level).

The process of registering a TWIC in a PACS and assigning access privileges are under the sole control of the local operator and may vary from one site to another.

When a TWIC card is registered into a PACS, the following verifications must be made:

- The card must be valid (not expired and not revoked or cancelled), authentic and issued by TSA,
- The card must be presented/used by the legitimate owner of the card (identity verification).

Because the Maritime sector has various levels of security (in some cases based on risk assessment assigned by the Coast Guard), the PACS registration of a TWIC card must be performed with the highest security controls applicable to the level of risk at the site and considering any potential changes in MARSEC levels.

NEXGEN TWIC cards are backward compatible with Legacy TWIC cards[22] and could be used in this backward compatibility mode, but it is highly recommended to use the new functions of the NEXGEN TWIC cards for registration since there is no more requirement for use of the PIV card application (and its PIN) for the registration process. The two following sub-sections describe in detail the recommended sequence of operations to register TWIC cards in a PACS. These operations are slightly different depending on the TWIC card data model (Legacy or NEXEN).

Important terminology: In the four parts of this NEXGEN documentation, in order to avoid any confusion with a PIV card and a "PIV-like" application in TWIC cards, the following words are used:

- **PIV Data Model** means the information in the card application is compliant with the various National Institute of Standards and Technology (NIST) documents describing the format of the data and structures to be stored in a PIV-like card. These documents are: NIST Special Publications SP 800-73, SP 800-76, and SP 800-78. The PIV card is in addition compliant with the NIST document SP 800-79 which defines the trust model (Federal Bridge used by PIV and PIV-I) which the TWIC card does not use as it uses the e-Passport trust model (PKI lite)
- The TWIC card contains two card applications, each with its own AID (Application Card Identifier):
    - A PIV Data Model card application and
    - A TWIC Card Application

2.5.1 Registration of Legacy TWIC cards

For Legacy TWIC cards, the PACS registration must be performed using a contact reader if the picture of the cardholder is to be stored in the PACS data base. The cardholder is required to present the PIV Card Application PIN to the PIV card to access the photo. Other personal information (e.g., printed data object

[22] Legacy TWIC cards do use the PIV application PIN (code 0x80) to protect personal information stored in the PIV application data objects; the NEXGEN card similarly uses the same PIV PIN (code 0x80) to access the PIV PIN protected information.

and fingerprint templates) can be obtained from the TWIC card application on the TWIC card without the requirement for PIN entry. The various operations to be performed can include the following[23]:

- Basic Verification (Mode 1)
  - Insert the TWIC card into a smart card reader attached to the PACS registration system
  - Select the TWIC Card Application
  - Read the CHUID and verify that it is correctly formatted with a valid digital signature
  - Extract from the CHUID, the card identifier (FASC-N) and the expiration date
  - Verify that the card is not expired.
  - Verify that the Card is not on the CCL (the CRL can also be checked)
- Card Authentication (Mode 2)
  - Select the PIV Data Model Card Application
  - Read the Card Authentication Key certificate in the PIV card Application
  - Verify that the data object contains the same FASC-N value as in the CHUID
  - Verify that the card has not been cancelled (CCL and eventually CRL[24])
  - Verify that the Card Authentication. digital signature and the validity date of the certificate
  - Execute a Challenge Response to perform an Active Card Authentication
  - Verify that the exchange verification is successful
- Cardholder Authentication (Mode 3)
  - Read the TWIC Privacy Key (TPK) from the card (using either the magnetic stripe or the contact interface)
  - Select the TWIC Card Application (if not already selected in contact mode)
  - Read the fingerprint templates from the TWIC card
  - Decipher the encrypted fingerprint templates using the TPK
  - Verify the digital signature of the fingerprint template object read from the card
  - Decode the fingerprint template and verify its structure[25]
  - Verify that the card identifier (FASC-N) attached to the fingerprint template is the same as the FASC-N found in the CHUID
  - Verify that the card has not been cancelled (CCL and eventually CRL)
  - Ask the cardholder to present their enrolled finger to a biometric reader attached to the system
  - Perform biometric verification between the user's reference fingerprint template from the card and the live finger presented[26]
- Data collection of user information from the TWIC card (optional)
  - This should be performed only after the TWIC card has been determined to be legitimate (e.g. Mode 4 in which the card is authenticated AND the user is proven to be the legitimate holder of the card)
  - Select the PIV Data Model Card Application
  - Ask the cardholder to present its PIN on a keyboard attached to the registration system

[23] The steps described in this section are only for guidance as there are often different ways to achieve the same level of assurance. For example, using the PIV user authentication certificate (which requires a PIN presentation) authenticates the card and the user at the same time. But as this mode is not available in the TWIC card application, it is not shown here.
[24] It happens that TWIC cards may be suspended, but not cancelled. In such a case, a suspended TWIC card will be listed as cancelled in the CCL, but not revoked in the CRL.
[25] In some cards, if the user does not have usable fingerprints this template may be empty. In such a case, the user access must always involve photo verification.
[26] Note: The fingerprint template (or any other biometric characteristic of the cardholder such as iris, vein or voice) can be optionally enrolled and stored in the local PACS data base to enable the use of "operational" biometric verification at the point of entry without requiring subsequent retrieval of the fingerprint templates from the TWIC card during access transactions.

- Present the PIV Application PIN (code 0x80) to the card using the PIV Data Model card application
- Read the cardholder Personal data object which contains the name[27]
- Read cardholder photo data object
- Store the information in the PACS database (FASC-N, username, Card expiration date, card Authentication Certificate number, etc.)

2.5.2 Registration of NEXGEN TWIC cards

With NEXGEN TWIC cards, the PACS registration can be performed using either contact or contactless readers and there is no requirement to present a PIN to the card at any time for registration. All of the following steps can be performed using only the TWIC card application. As such, the selection of the TWIC card application is required. The various operations, described in more details in Part 2 of the NEXGEN specification, include the following:

- Basic Verification (Mode 1)
  - Present the TWIC card to a smart card reader attached to the registration system.
  - Read the CHUID and verify that it is correctly formatted with a valid digital signature
  - Extract the card identifier (FASC-N or Card UUID[28]) from the CHUID and the expiration date
  - Verify that the card is not expired
  - Verify that the Card is not cancelled (CCL and eventually CRL)
- Card Authentication (Mode 2)
  - Read the TWIC Card Authentication Public Key certificate
  - Verify that the data object contains the same FASC-N (or Card UUID) as the CHUID
  - Verify the Card Authentication digital signature and the validity date of the certificate
  - Verify that the card is not cancelled (CCL and eventually CRL)
  - Execute a challenge/Response for an active card authentication
  - Verify that the challenge exchange is successful
- User Authentication (Mode 3)
  - Read the TWIC Privacy Key (TPK) from the card (either by scanning the 2-D bar code on the back of the card or using the contact interface)
  - Read the cardholder fingerprint template form the TWIC card application. This data object is deciphered using the TPK
  - Verify the digital signature of the fingerprint template object read from the card
  - Decode the fingerprint template and verify its structure[29]
  - Verify that the card identifier (FASC-N) attached to the fingerprint template is the same as the FASC-N found in the CHUID
  - Verify that the card has not been cancelled (CCL and eventually CRL)
  - Ask the cardholder to present their fingerprint to a biometric reader attached to the system
  - Perform biometric verification between the user's fingerprint from the card and the fingerprint presented
- Data collection of user information from the TWIC card (optional)

[27] The user name may also be extracted from the CHUID data object in its digital signature; but this is not a recommended method.
[28] IN NEXGEN TWIC cards, it is possible to extract the FASC-N from the card UUID.
[29] In some TWIC Legacy cards, the fingerprint template may be empty indicating that the user does not have usable fingerprints. In such a case, the PACS operator must use the cardholder picture, or other means, when identity verification is required.

- This should be performed only after the card and the user have been authenticated (this is done by using TWIC authentication Mode 4 which combines Modes 2 and 3)
- Read cardholder Personal data object which contains the name
- Verify that the digital signature and the attached FASC-N is the same as in the CHUID.
- Decode this information using the TPK and extract the user name.
- Read the cardholder photo data object
- Verify that the digital signature and the attached FASC-N is the same as in the CHUID
- Decode this information and extract the cardholder photo
- Store the information in the PACS database (FASC-N, username, Card expiration date, card Authentication Certificate number, etc.)

Once a card is registered in a PACS data base, the system must periodically[30] verify that the cards registered are still valid and not canceled by the TSA TWIC system (CCL). The following section describes the functions that a PACS should perform on a regular basis (e.g. daily).

2.6 PACS maintenance for registered TWIC cards

Any PACS must maintain its cardholder data base and keep it up to date. This means making sure that registered credentials are not expired, cancelled, or revoked, and that local access authorizations attached to the credentials are still valid.

Since TWIC cards are issued by TSA, which is a different entity from the PACS, the PACS must also check for any updates by TSA which can impact the PACS registered credentials.

As such, on a regular basis (e.g. daily) the PACS must download the latest CCL[31] published by the TSA TWIC system. Alternatively, the PACS can rely on the CRL for this purpose, but as indicated before, suspended TWIC Cards appear on the CCL as cancelled, but not on the CRL as the suspended state for a TWIC card is temporary and it can be reinstated.

When the CCL is used, the following verifications must be performed by the PACS when downloading a CCL:

- IF the latest CCL cannot be downloaded (e.g. web site not accessible), the previous CCL must be used, and the PACS should issue a warning.
- The PACS must verify the CCL is not empty. This may happen sometimes when the CCL cannot be downloaded correctly. In such a case, the previous CCL must be used, and a warning issued.
- The hash Message Digest of the CCL must be verified to ensure that no card identity has been added, changed or removed from the official list.
- Since the CCL is updated daily, the PACS should download the CCL daily to ensure that it is using the latest version. If the CCL is older than three days, the PACS should issue a warning.

Using the CCL, the PACS must flag all of the registered cards which are found on the CCL and take action to either revoke the local access privilege, and/or remove the individual if this person is already on site.

[30] Recommended no more than daily as the CCL is updated once a day every morning.
[31] The TWIC CCL can be downloaded freely at https://universalenroll.dhs.gov/ccl/CCL.CSV. The integrity of the downloaded list should be checked using the hash value provided at https://universalenroll.dhs.gov/ccl/CCL.CSV.MD5

2.7 One card Profile: Activation of some TWIC Cards in UES stations

TWIC NEXEGN cards are all initialized according to the same process (this is called One Card Profile). Some are mailed directly to cardholders, some are sent to Activation centers for the cardholders to pick up and eventually have specific procedures like:

- User willing to Select (or reset) its PIV card PIN
- Activating the card for a TWIC trusted agent.

As the Trusted agents do access Federal computer networks, the Federal security rules (FIPS 201) requires their card to have the following characteristics which are not standard in other TWIC cards:

- The PIV Authentication key (activated when the user presents his/her PIN) must be generated on the card.
- The PIV key and the certificate for digital signatures must be present on the card.
- The PIV key and the certificate for key management must be present on the card (overthought TWIC does not manage expired certificates in the card).
- The cardholder must know the PIV Card Application PIN.

These elements are created/modified during the activation process done under the control of the TWIC CMS in activation centers and is specific to Trusted Agents cards[32].

The TWIC application in Trusted Agent cards is not changed, but a specific e-sticker (under TSA's control) may be used to indicate this card status.

[32] This process is very similar to the standard activation procedure of PIV cards (see SP 800-73)

3. New feature in NEXGEN TWIC cards: E-Stickers

This section presents (from a functional perspective) some of the new possibilities offered by Electronic Stickers (E-Stickers) available in NEXGEN TWIC cards[33].

E-Stickers consist of ten data objects available in NEXGEN TWIC cards which are all open to read, write, or update by any application using the NEXGEN TWIC card (e.g. a PACS system or a portable TWIC reader). In addition, the TWIC Card Application includes four TSA controlled E-sticker data objects which can be used by TSA to optionally indicate specific information about the card holder. These four TSA controlled E-Stickers are also free read but can be updated only under the card issuer control (TSA)[34].All other data objects in the card have some level of restricted access (read only, read with password, execute only, or no read [e.g. for private keys] and so on) and are, as such, protected against any modification or deletion.

The ten E-Stickers, as well as the four updated Protected Data objects are very similar in concept to a bar coded adhesive label affixed on the outside of the card (or any ID document). They also could be compared to printed visas attached to a passport booklet by a country which did not issue the passport itself. The main difference with these two analogies, is that these electronic stickers have a specific memory name & space reserved for them in the card (so they never overlap with any other information). Accessing them (in read or update mode) cannot replace, modify, delete or harm in any way any other data objects in the TWIC card.

The ten free read/write data objects have no access protection restriction; so they can be modified and/or read by any application. The four TSA controlled E-Stickers require the card issuer (TSA) to be authenticated by the card to allow an update. Because they are free-read, no critical permanent or private information should be stored in any of these objects in clear text. They are made available for convenience and might provide an opportunity to enhance the efficiency of user-specific complex transactions without requiring development of an online back-end system or having to issue a local access control/ID card to the TWIC cardholder.

The use cases presented hereafter are only suggestions, and this section does not provide any technical details or recommendations as to how to technically use these data objects. These use cases are further described in independent document dedicated to E-Stickers and protected Data Objects as referenced above. This document related to E-Sticker examples in under development with the industry collaboration and may be obtained by sending an e-mail request at TWIC-Technology@tsa.dhs.gov.

All the suggested use cases presented here may be made secure against most attacks using the classic countermeasures available for digital identities such as digital signatures, information linked to the card Identifier, day and time of validity, issuer information, etc.). More information can be found in the specific E-Sticker documentation mentioned above.

[33] A more detailed document (NEXGEN TWIC E-Sticker Vx.pdf) is under development and will be made available by sending an email request to TWIC-Technology@TSA.DHS.GOV.
[34] Requires the use of the Card Administrative Key known only by TSA.

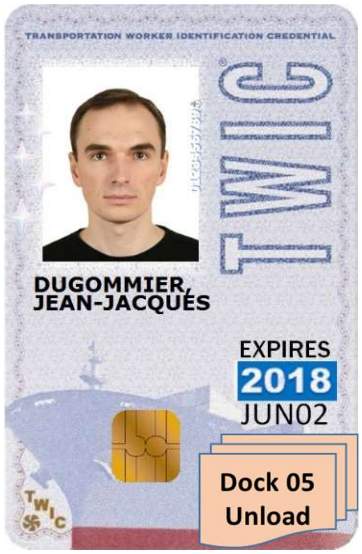
3.1 Storing PACS Authorization Conditions in a NEXGEN TWIC Card

In many large facilities, it can be quite expensive to have all readers connected to an online panel or system. For example, spot security verifications of individuals in a given area may be required to verify if persons present are allowed in the specific zone on a given day and time and at a given MARSEC level.

Such a specific authorization is usually stored in the PACS data base and linked to the credential used by the individual. But if the connection with the PACS is not available for any reason (e.g., system limitations, cost, failed connection, or sabotage), it is possible for the PACS operator to include a digitally signed information contained in the NEXGEN TWIC card that provides the authorization conditions for an individual cardholder at this specific site. This enables spot verification of access privileges of the cardholder without connection to a PACS.

Moreover, as there are up to ten E-Stickers, multiple sites are able to take advantage this capability.

3.2 Storing a Vehicle Unload Area in a NEXGEN TWIC card



A TWIC cardholder truck driver may be assigned a specific or limited location within the facility that they can access with their truck. This location and any time period restrictions can be stored in a NEXGEN TWIC Card E-Sticker data object. This information can then be read from the TWIC card by an operator or gate guard on a handheld device without requiring connection to the PACS.

The information stored in the E-Sticker can be used to verify that the truck driver is not “roaming” the area or accessing unauthorized areas. The retrieved information can also be used by the operator to direct the driver to the correct location within the site.

It is also easy to add/read more information in the E-Sticker during the entry or exit transaction at the gate, such as the time of entry and the total weight of the truck (in or out). By adding the day and time and the truck identification, all of the information pertaining to the movements of trucks can be easily collected on fixed or portable readers and transferred to the PACS later even if direct communications are not available during the entry/exit transactions.

3.3 Storing Cardholder Personal Attributes in a NEXGEN TWIC Card

In some cases, it is very useful to know if someone is qualified to perform CPR or is a qualified first responder. Having a separate card to display such an attribute would require a separate and parallel trust infrastructure. It is quite simple to load such information in the cardholder's NEXGEN TWIC card.

Once this information is stored in the card, any person reading the E-Stickers from the card can verify the qualifications of the cardholder and be assured of the authenticity of the qualifications by verifying that the information is digitally signed. Depending on the level of security attached to the information stored in the card, this may be trusted by only one entity, or multiple entities if they agree on using a shared Public Key Trust mechanism.

3.4 E-Sticker Indicating the card is used to a TWIC trusted agent

As indicated in section 2.7 TWIC trusted agent cards have a specific activation process on the PIV card application side of the card. The TWIC card application is identical to other TWIC cards, but it can be useful to know the cardholder is a trusted agent when the TWIC Card application is sued (e.g. for physical access control is some restricted area).
The following is a proposed structure of a TSA issue e-sticker to be added in the card indicating this specific status. It complies with the suggested structure of section 3.5.
The Trusted Agent e-sticker will use the e-sticker tag identifier 0xFD. As any other e-stickers, it is free read, but can be changed/updated/deleted only under the control of the TSA CMS system. (See TWIC NEXGEN specification Part 2 – section 4.7.9 on TSA controlled e-Stickers)

Details of the TWIC Trusted Agent e-sticker structure[35]:

Tag	0xFD	
Length	0x028LLL	Total Length is on three bytes
Header Tag	0x80	
Header length	0x10	(length of the header is 16 bytes)
E-Sticker code	0x54	TSA controlled e-stickers
E-Sticker Subcode	0x01	TWIC Trusted agent cards
Creator System-ID	0x7099000000000000	(TSA TWIC system)
Creation date	0x202307011025	(updated when e-sticker is created)
Data information	0x34 0x10	copy of card UUID (tag 0x34 in the CHUID on 16 bytes).
Data signature	0x3E 0x028LLL	digital signature by TSA of the whole e-sticker

[35] This structure is based on the proposed TWIC NEXGEN E-Stickers document (version V12 -2022-01-23)

3.5 Suggested Structures of E-Stickers

This section is a condensed version of the more complete document dealing with E-Stickers which is under development in cooperation with industry and will be made available by sending an e-mail request at TWIC-Technology@tsa.dhs.gov .

The following is a very quick overview of what is suggested (but not required or enforced) for E-Stickers.

The E-Stickers are accessed in the card using the ISO/IEC[36] commands described in ISO/IEC 7816-4 for reading or updating tagged data objects in smart cards[37]. The commands used to interact with the card are GET DATA and PUT DATA (version using the odd INS byte) and the standard ISO format[38].

As mentioned before, the card does not verify what is loaded in these data objects. But since they are intended to be used and shared between multiple entities, a minimum structure is suggested as follows:

- E-Sticker Tag for E-sticker data objects: (0xE1 to 0xEE & 0xFA to 0xFD)
- E-Sticker Length (length of zero in a Put Data is equivalent to an erase – One up to three bytes))
    - Header (has its own Tag and Length – A zero length header indicates a free E-Sticker):
        - Code (one byte - indicates what the E-Sticker is used for)
        - Sub-Code (one byte - Sub-indication of the E-Sticker use)
        - System ID (8 bytes - owner/creator of the E-Sticker)
        - Creation date & time (6 bytes - when the E-Sticker was created in the card)
    - Information (has its own Tag – Length)
        - Information specific to the owner (System-ID from the header)

An **empty E-Sticker** should return the following data object (Tags 0xE1 and 0xEA used as examples):
E1 02 80 00 or EA 02 80 00

It is possible that the responses returned by the card could also be: E1 00 or EA 00

But such responses are not using a correct Tag-Length-Value (TLV) structure and might indicate a non-initialized E-Sticker, which also means a data object not available for use as it is.

[36] International Standards Organization/ International Electrotechnical Commission
[37] These commands are described in detail in the TWIC card documentation (Part 2) of this series of documents.
[38] Some PIV data objects are retrieved by a command structure which is not completely ISO/IEC 7816-4 compliant as the information returned uses the Tag 0x53

Example of an E-Sticker Data Object (values below are examples):

Tag (three bytes): 0xE1 (free Read/Update E-Sticker)

Length (one up to three bytes) 0x82020A

1) Header Tag 0x80
2) Header Length 0x10
    a) Code 0x41 (Personal Cardholder Attribute)
    b) Sub-Code 0x72 (is the ACII letter H for Hazmat)
    c) System-ID/Owner 0x709965420236840 (Same as CIN of the card)
    d) Creation Date 0x201803281300 (YYYYMMDDHHMM)
3) Information tag 0xE1 (the information is a constructed data object as well)
4) Information length 0x8201F6 length on two bytes (0x01F6 = 502 bytes)

a) Example: Digitally signed information related to the HAZMAT credential
308201F206092A864886F70D010702A08201E3308201DF020103310B3 ……..
……
complete lines here are now shown because of the length of the data
……
…….6A45A0C1ABD0DC3C991A8A927DEA4D2FB15FC49D715CFD2C

4. Annexes

The two following sub-sections are also in the Part 1 document of this series but have been repeated in this part for the convenience of the reader.

4.1 Countermeasures to security threats

The table below (repeated from the annex of Part 1) summarizes the actions (countermeasures) to take in order to circumvent a given vulnerability. For each countermeasure, the terms Low (+), Medium (++) or High (+++) indicate the level of assurance provided.

Mode of Operation	Mode #	Operator Required	False Card	Expired Card	Canceled Card	Impostor Identity	Incoherent Information	Denial of Service
Flash Pass / Visual Verification	Manual	Y	+	+		+	-0-	-0-
Supplement to Visual Inspection (STVI)	Mode 0	Y	+	+++	+++	+	-0-	-0-
CHUID Verification	Mode 1	N	++	+++	+++	-0-	-0-	+++
Active Card Authentication	Mode 2	N	+++	+++	+++	-0-	+++	+++
CHUID + Biometric Verification	Mode 3	N	++	+++	+++	+++	+++	+++
CHUID + Active Card Authentication + Biometric Verification	Mode 4	N	+++	+++	+++	+++	+++	+++
CHUID + Cardholder Picture Verification	Mode 5	Y	++	+++	+++	++	+++	+++
CHUID + Cardholder Picture Verification + Active Card Authentication	Mode 6	Y	+++	+++	+++	+++	+++	+++

Note: The value -0- in a cell of the table indicates the mode of operation on the row does not address the threat indicated in the column.

4.2 Differences between Legacy TWIC cards and NEXGEN TWIC Cards:

The main differences between Legacy TWIC cards and NEXGEN TWIC cards are summarized below (the complete technical details can be found in Part 2 of this TWIC series of documents)[39]:

- NEXGEN cards do not include a magnetic stripe on the back.
- NEXGEN cards have a two-dimensional bar code printed on the back of the card containing (among other data) the card TWIC Privacy Key (TPK) (the linear bar code containing the CIN is unchanged and exists in Legacy TWIC as well as NEXCGEN TWIC cards).
- All data objects in the NEXGEN TWIC Cards contain a fully populated Card UUID in all signed data objects.
- All certificates in NEXGEN TWIC cards use the Secure Hash Algorithm SHA-2 hashing code instead of SHA-1 in Legacy cards
- 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 has its own Card Authentication key and its related certificate. This key allows active authentication of the NEXGEN TWIC card without requiring use of the PIV Data Model card application.
- Many data objects (some optional) have been added in the TWIC Card application (e.g. cardholder photo, handwritten signature, name information, etc.). These are protected by the TWIC Privacy Key and most are digitally signed. They are all accessible on both the contact as well as the contactless interface.
- Four TSA controlled E-stickers have been added to the data structure of the NEXGEN TWIC card. Ten free e-Stickers have also been added. These objects can be read, written, and updated by any application using the TWIC card. Examples of their use are provided in an annex of the Part 4 document: “TWIC uses and registration by a PACS”.

4.3 How to recognize which type of card is presented to a reader/PACS?

It sometimes can be confusing to a reader when a card using the PIV data model is presented. Is it a PIV, a PIV-I, a TWIC, a CIV, or something which looks like one of these but is different … As always, there are rules and exceptions.
This section is a simplified guide allowing a reader/PACS manufacturer to find its way in such a maze.
Note: Refer to Part 2 Section 6 if needed to find the values and meaning of the PIV and TWIC Object Identifiers (OID’s) mentioned in the following sub-sections.

4.3.1 What all these cards have in common

They all have a PIV card application with an AID of A000000308000010000100. This card Application may not always be selected by default in all cards. It is highly recommended to always issue a formal Select AID command to make sure the card has (or does not have) such an application inside.
They all abide by the data model defined by the NIST documents: SP 800-73, SP 800-76 and SP 800-78. As such they all have a FASC-N in the CHUID, but it may not always be meaningful (see next).

[39] A more complete list of differences between Legacy TWIC and NEXGEN TWIC can also be found in the Part 1 (General Description of TWIC credential in use by the maritime industry) Section 1.3 of this series of documents.

4.3.2 Personal Identity Verification (PIV) cards

PIV cards are issued by Federal Entities to personal and contractors working for the Federal government. They have a populated FASC-N with a four digit Federal Agency Code which can be found in NIST document SP 800-87 and also abide by the NIST specifications SP 800-73, SP 800-76, SP 800-78 as well as SP 800-79.

- But not all Federal Agency codes are found in the NIST document SP 800-87. For example, the code used by the Department of Homeland Security for its TSA-TWIC cards (which are issued for civilians) uses the code 7099 which indicates it is issued by DHS, but this specific code has never been registered as such by NIST in SP 800-87.
- Another exception to this rule has also to do with PIV-I cards issued by Federal Agencies to personal not yet cleared in terms of security (security clearance pending). In such a case, the card is issue by a Federal Agency for someone who will "potentially" work for the government when the clearance process is finished.

To make sure such exceptions are caught by the system using the card (including Registration or Provisioning access privileges of agencies), it is important to check the Object Identifiers (OID) used in the card certificates (e.g. the Card Authentication certificate) making sure the level of trust in the credential is what it is expected to be. See section 6 in NEXGEN documentation Part 2.

4.3.3 Personal Identity Verification Interoperable (PIV-I) cards

Defined by the documents: Personal Identity Verification Interoperability for Non-Federal Issuers[40] and the FICAM PIV-I FAQ [41], PIV-I cards are issued by private entities for non-Federal Employees, and they should have a value of "9999" in the Agency Code of the FASC-N. They abide by the same data model documents (SP 800-73, SP 800-76, SP 800-78), and use the Federal Bridge to convey trust (SP 800-79). The card issuer related information as well as the background checks (if any) related to the cardholder can be found by looking at the OIDs in the card.

4.3.4 Commercial Identity Verification (CIV) cards

Commercial Identity Verification cards are defined by the document from the Smart Card Alliance [42](now named the Security Technology Alliance).
As for PIV-I cards, they do have the same AID, same Data model, but are issued by private issuers and are not using the Federal Bridge to convey any kind of interoperable trust. They are typically issued by an issuer for its own use in a private environment.
The OID's used for such cards are under the complete control of the card issuer and may vary but cannot (or at least should not) be any of the OID's used by other registered cards (such as PIV, PIV-I or TWIC).

4.3.5 Transportation Worker Identity Credential (TWIC) Cards

As indicated in the NEXGEN set of documents, TWIC is a PIV data model abiding card, in which there is a PIV data model card application with the PIV AID, but has its own registered OID's defining the trust model they abide by, as well as a simple direct trust model similar to the e-Passport trust model)..
TWIC is also (at this point in time) the only PIV data model Card with a second Card Application inside the same card using the TWIC AID (A0 00 00 03 67 20 00 00 01 xx xy in which xx xy indicates the version of the TWIC data model).

[40] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-i-for-issuers.pdf
[41] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/PIV-I_FAQ.pdf
[42] http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

4.3.6 Conclusion. Using OIDs is the best way to find out.

The easiest way (and safest way) to find which card is presented is to use the Object Identifiers (OID) found in the various signed data objects in all circumstances.

In the context of computer security, OIDs name nearly all X.509 certificate object types, including components of policies, distinguished names, CPSs, and so on. OIDs are associated with objects in data structures commonly defined using the standard Abstract Syntax Notation number One (ASN.1) so that OIDs may be generated and processed by client and server software. Refer to ISO/IEC 8824 and 8825 specific parts for more information (see https://www.oss.com/asn1/resources/standards-define-asn1.html).

Most CAs do not create new OIDs. OIDs are typically attached to a certificate when it is created by a certificate authority using 3rd party software. For example, certificates can be associated with a policy represented by a numeric string (the OID) that controls how an application will behave. When an application encounters a certificate, it processes the OIDs, and in this case it looks for a corresponding certificate policy and changes its behavior accordingly.

As smart cards hold information in a binary format, it is important to understand the conversion of OID Dot Notation to a Tag-Length-Value representation as per Distinguished Encoding Rules (DER) of the International Standard ISO/IEC 8825-1:2015.

A Conversion example using the PIV-I content signing OID dot notation:

Dot Notation: 2.16.840.1.101.3.2.1.3.47 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) csor-certpolicy(1) fbca-policies(3) id-fpki-common-pivi-contentSigning(47)} (see http://oid-info.com/get/2.16.840.1.101.3.2.1.3.47)

TLV: **06** *0A* 60 86 48 01 65 03 02 01 03 2F

Where **06** – ISO Tag meaning "Object Identifier is the value field type"
0A – Length of the Value field (10 bytes)

Turning now to government issued smart card solutions, two immutable arcs are identified below. For PIV / PIV-I it is recommended to visit the "FICAM playbook" for additional details; see https://playbooks.idmanagement.gov/fpki/ .

PIV / PIV-I / DoD CAC PIV

PIV ROOT: 2.16.840.1.101.3 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)} (see http://oid-info.com/get/2.16.840.1.101.3)

Refer to the Federal PKI Policy Authority (FPKIPA) Registered Objects that can be found at:

https://csrc.nist.gov/projects/computer-security-objects-register/pki-registration

TSA TWIC

TWIC ROOT: 1.3.6.1.4.1.29138 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 29138} (see http://oid-info.com/get/1.3.6.1.4.1.29138)

Refer to the TWIC NEXGEN Specification Part 2 for detailed sub OID definitions.