THIS DOCUMENT IS CURRENTLY UNDER DEVELOPMENT AND USED AS PART OF THE NEW SC-QTL EFFORT. IT IS PROVIDED FOR REVIEW AND ALL COMMENTS OR SUGGESTIONS ARE WELCOME.

TWIC® Qualified Technology List

Navigation Guide for Applicants

July 16, 2024. V4.0

ID Technology Partners Inc.

Operations Support

Program Management Division

Vetting Programs Office

Maritime Branch

VERSION CONTROL

January 26, 2021	Initial Outline – Gerald Smith
January 31, 2021	Reformat with Contributions – Mike McCabe
January 31, 2021	Merge with Addition Content – Gerald Smith
February 1, 2021	Additional Content Added – Gerald Smith
February 2, 2021	Additional Content Added – Gerald Smith
February 4, 2021	Additional Content Added – Mike McCabe
February 4, 2021	Reformat, Revise Sections – Gerald Smith
February 8, 2021	Team Comment Resolution and Contributions – Gerald Smith
February 10, 2021	Modified 4 Modes Graphic – Gerald Smith
July, 2023	Updated NEXGEN Reference – Lars Suneborn
May 2024	Updated figure 1 -Lars Suneborn
July 15, 2024	Updated to be aligned with NEXGEN tests and modes
July 16, 2024	Document changes review – Gerald Smith
July 16, 2024	Update of point of contact and the two pages

1. Introduction

1.1 Background

The United States Congress mandated the Transportation Worker Identification Credential (TWIC) in the Maritime Transportation Security Act of 2002 (MTSA) as amended by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). The mission of the TWIC Program is to design and field a tamper resistant credential (referred to as a TWIC Card) for all maritime workers requiring unescorted physical access to secure areas of the nation's port facilities, outer continental shelf facilities, and vessels regulated under the MTSA, and all U.S. Coast Guard credentialed merchant mariners. The TWIC program is administered by the Department of Homeland Security (DHS) with joint management responsibility shared by the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA is responsible for enrollment, identity vetting and credential issuance. The Coast Guard is responsible for enforcement, access control requirements and regulations.

The TWIC card is subject to visual inspection at points of entry or can be electronically read and validated by reader devices which have been deployed by maritime operators. The TWIC Reader Hardware and Card Application Specification (hereafter, referred to as the TWIC Specification) is a set of documents issued by the TSA which describes the behavior of the TWIC card application, card interface, as well as the reader hardware performance and technical requirements. The TWIC specification addresses both fixed and portable reader devices.

The Transportation Security Administration (TSA) working with the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and other federal agencies established in 2012 a process and program to test and qualify products that read, verify, and authenticate the TWIC cards used in the TWIC Program. Products that were deemed to be compliant with the TWIC Specification were placed on a list referred to as the TWIC Qualified Technology List (QTL) intended to be used by owners and operators of regulated maritime facilities and vessels to assist in their TWIC reader purchasing decisions.

In 2012 the QTL program was established by the TSA TWIC Program Management Office. The program was based on a third party testing laboratory to determine if a vendor’s reader was conformant/in compliance with the TWIC reader specification. This process has been revised to offer an Applicant-driven self-certification process that will provide an on-going process of TWIC reader qualification by self-assessing the conformance of fixed and portable TWIC readers to the TSA TWIC specification(s). In addition to dramatically reducing the overall cost resulting from the use of a third party laboratory for the formal certification of TWIC readers, it will permit/enable faster market recognition of those Applicant readers that have completed the self-certification process at a pace determined by each Applicant.

1.2 Purpose

The purpose of this document is to provide a high-level overview and assistance to the vendor/applicant in the self-certification process of a potential TWIC reader to the Self Certified Qualified Technology List (SC QTL) and to provide the vendor/applicant with additional information needed for the following self-certified processing steps:

A) accurately completing the Applicant form and a given product capabilities claims form,
B) understanding how the completed Application form is used by TSA to determine if a vendor self-certified testing package need be generated,
C) describing the major components of the testing package sent to the Applicant,
D) use and operation/execution of the package components by the Applicant,
E) running the product specific suites of tests using TSA supplied test cards to determine conformance with the readers intended mode of operation,
F) producing the test report(s) from the report component of the testing package and sending the report back to TSA,
G) interacting with TSA for posting the self-certified product on the SC QTL, and
H) Annually certifying to TSA each SC QTL posted product is unchanged and still available.

Note: Even though many modes of operation and tests are similar between the TWIC Legacy cards and the TWIC NEXGEN cards, all test cards as well as test cases are different to make sure the complete procedures are indeed respected.

2. Definitions

For the purpose of this document, the relevant definitions given in ISO/IEC 17000, the TWIC SC QTL Administrative manual apply, together with the additional definitions:

Personal Identity Verification – The program used within the U.S. Government for physical and logical access to buildings, networks, etc. Known as PIV.

3.0 High Level Overview of the Self-Certified QTL Process

The complete process, detailed in Section 4 of the Self-Certified QTL Administrative Guide and Concepts of Operations Version is illustrated here:

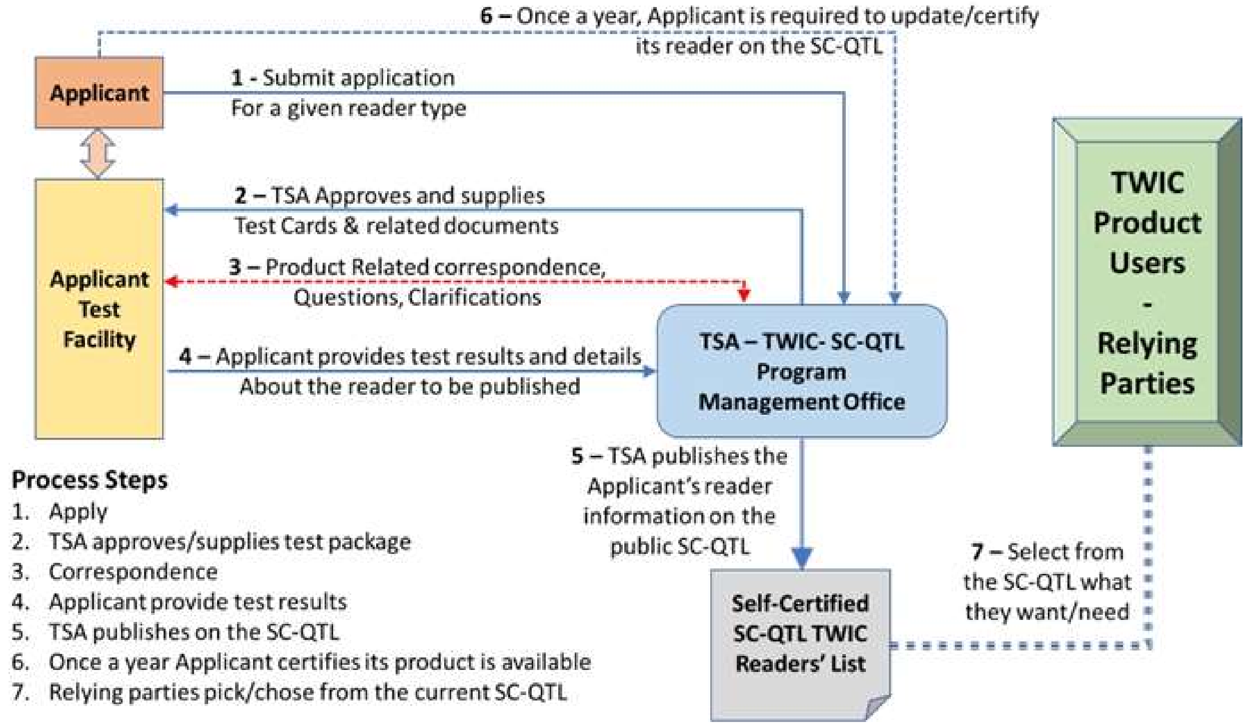

6 – Once a year, Applicant is required to update/certify its reader on the SC-QTL
Applicant
1 - Submit application
For a given reader type
TWIC Product Users - Relying Parties
2 – TSA Approves and supplies Test Cards & related documents
3 – Product Related correspondence, Questions, Clarifications
Applicant Test Facility
4 – Applicant provides test results and details About the reader to be published
TSA – TWIC- SC-QTL Program Management Office
5 – TSA publishes the Applicant's reader information on the public SC-QTL
Process Steps
1. Apply
2. TSA approves/supplies test package
3. Correspondence
4. Applicant provide test results
5. TSA publishes on the SC-QTL
6. Once a year Applicant certifies its product is available
7. Relying parties pick/chose from the current SC-QTL
7 – Select from the SC-QTL what they want/need
Self-Certified SC-QTL TWIC Readers' List

FIG. 1 -The Self-Certified QTL Process

The sections that follow focus on "what" needs to happen by the identified responsible party at each step in the process. The "how" a given "what" might be achieved is limited to providing a few suggestions when selecting from various options available with respect to each TWIC Specification reader mode of operation. Although there are more than nine possible testing configurations as described in the testing procedures document, this navigation guide focuses on the six basic modes of operation specified (six modes for NEXGEN cards and four for Legacy cards). The applicant is not required to self-certify their reader across all possible configurations. Rather, the applicant will state to TSA the applicant's product functional claims and TSA will review, approve, and provide back to the Applicant the testing and reporting criteria to be applied for the Applicant's product and the TWIC modes supported by the reader.

3.1 Applying to TSA for a Self-Certified Approval and Listing on the SC QTL

The first step in the applicant-driven self-certification process, culminating in a reader listing on the SC QTL is to prepare and submit a fully completed application package to the TSA Enrollment Services & Vetting Programs (ESVP). A separate application package must be submitted for each reader seeking listing on the SC QTL. All manufacturers s applying for TWIC NEXGEN Cards shall be also qualified to work with TWIC Legacy Cards as such cards will be in the field until 2029.

To begin the process, an applicant need only send an email to the TSA TWIC general technical support group TWIC-Technology@tsa.dhs.gov with a subject line "*Request SC QTL Application*". In the body of this email list your organization and two points of contact with their contact information (email, phone, address). Upon receipt of this email, a TWIC SC QTL Program Applicant Agreement and a TWIC SC QTL Program Product Application form will be sent to the applicant. The applicant will be directly contacted by one of the technical people in charge of managing the SC-QTL process.

Once the applicant has completed the aforementioned forms, the applicant will return the completed forms (known as an application package) to TSA. The applicant returned application package should attempt to include any available product documentation and test results obtained from appropriately accredited, third party test laboratories demonstrating conformity to non-functional technical requirements (e.g., UL, FCC) as referenced in the TWIC specification. The paragraphs that follow provide guidance on completing various sections of the application. The completed application package will then need to be returned to the TSA ESVP at TWIC-Technology@tsa.dhs.gov with a subject line "*Request for SC QTL Self-certification Kit*". Once received, TSA will review the request for correctness and completeness, prepare a self-certification kit, and forward it to the applicant.

3.1.1 Setting a Course: Deciding on what product features to test

TWIC cards and the TWIC program have a focus of using an identity credential in a physical access control environment. PIV card are more focused on logical access. These perspectives influence functionality between TWIC and PIV.

One of the most frequent questions asked of the TWIC program by stakeholders is:

What defines a TWIC reader[1]*?*

For the purpose of this document the definition of what constitutes a TWIC reader is:

1. A device, stand-alone or composed of multiple components, some of which require continuous connectivity to each other, able to connect to the TWIC card application, per specification, either over the contact interface or contactless interface.
2. The ability to read the TWIC Signed CHUID and process the information to determine/establish that :
    a. The TWIC has not expired
    b. The TWIC has not been canceled by checking the TWIC maintained Canceled Card List
    c. The TWIC Signed CHUID has not been altered (by validating the embedded Signature of Data with the provided public key within the X.509 v3 Public Key Content Signing Certificate).
3. Additionally, if fingerprint matching is supported, the capability to obtain the TWIC Privacy Key (TPK), read the enciphered Fingerprint Biometrics container, recover the cleartext fingerprint card holder reference template, obtain a live fingerprint sample and then perform a matching operation to achieve a result of PASS or FAIL.

A critical step for the Applicant is to understand what TSA considers a portable reader or fixed reader; and it is not packaging! Understanding the TSA classification rationale will simplify the Applicant's work in terms of aligning a product offering to a classification and the scope of claims to be tested by the Applicant or their designated testing entity.

TSA has chosen to classify readers based on intended operational usage.

TSA defines each reader type classification at a high level in Section 4.2.1 of the TSA SC QTL Administrative Manual. Specifically:

"*Testing falls into two basic categories:*

(A) ***Portable Reader*** *– A device that does not rely upon an always-available networked component. Physical access is ultimately determined by the portable reader (human) operator.*

(B) ***Fixed Reader*** *– A device connected to a physical access control system which may involve other components. Physical access is ultimately determined by the access control system."*

[1] TWIC cards also support a populated PIV card application to enable use of TWIC cards in a PIV only environment. Using only PIV functionality does NOT characterize a device as a TWIC reader.

Given this TSA perspective, the Applicant is strongly recommended to consider their product submission by first internally answering the following two questions:

1) Does my product require connectivity to another system to perform each transaction?
2) Does the access decision come from a central system?

If you answer YES to either question, your organization should select FIXED for the reader classification.

If you answer NO to both questions, your organization should select PORTABLE[2] for the reader classification.

Another important decision an Applicant needs to address is what TWIC specification options are to be included in the self-certification process for the product offering.

The TWIC reader specification (Part 2 of the TWIC documentation) can be confusing to designers when deciding what option is best to meet a given Mode of operation. This guide exists to suggest one possible mix of options based on the experience of TSA evaluating and observing several TWIC reader solutions since inception of issuance in October 2007.

The authors of this document leveraged TWIC reader historical knowledge to craft a suggested option per reader mode an Applicant might consider when attempting to meet all specification requirements for a given Mode of operation.

These are suggestions only, as the specification permits, in places, alternate TWIC reader options to be used driven by the nature of the Applicant's envisioned use environment, mix of technology, and prevailing policies. In the end, TSA does not mandate how a given requirement is achieved.

NOTE: Some of the suggested ideas presented here may be covered by Patents or other Intellectual Property rights unknown to either the authors or TSA.   Due diligence is recommended.

[2] The term "Standalone" is sometimes used in the various documents related to TWIC readers. A standalone reader may be fixed or portable, but does not rely on a back-end system.

Each mode defined in the TSA specification for a TWIC reader is illustrated here at a high level:

TWIC Legacy & NEXGEN Modes:

1. Mode 1: Verification of the cardholder identifier. (CHUID Verification)
2. Mode 2 – Card Authentication (card cryptographic challenge)
3. Mode 3 – Cardholder Biometric Verification (fingerprint reference)
4. Mode 4 – Card Authentication AND Cardholder biometric verification

TWIC NEXGEN Modes

5. Mode 5 – Cardholder picture verification
6. Mode 6 – Cardholder picture Verification and card authentication

Note: The PIN is never used in any TWIC modes but may be required for Legacy Cards in order to access the cardholder picture (see note on mode5).

This navigation guide suggests one path for each reader Mode: Unless specifically mentioned, the PIV card application should not be selected. All modes of operations (except mode 2 & 4 for Legacy Cards) shall be using the TWIC card application.

Mode 1 – STATIC IDENTIFICATION

The reader should employ the TWIC Signed CHUID option.

Rationale: The TWIC Signed CHUID holds the official TSA static identifier reference of the FASC-N. The TWIC Signed CHUID is also where the Content Signing Public Key X.509 v3 certificate resides for checking all signed TWIC card application data objects. The credential expiration date is present in the TWIC Signed CHUID data object. Other option paths available for Mode 1, such as the TWIC Unsigned CHUID , would require the Applicant's TWIC reader utilize the TWIC Security Data Object (SDO) to validate the unsigned CHUID was not altered. However, validation of the SDO object itself requires the TWIC Content Signing Certificate Public key, held in the TWIC Signed CHUID, thereby making use of the TWIC unsigned CHUID less attractive. The PIV card application is not used for this Mode.

Mode 2 – CRYPTOGRAPHIC AUTHENTICATION

The reader should obtain the TWIC reference FASC-N and credential expiration date from the TWIC signed CHUID. For TWIC Legacy Cards, the PIV card application should be selected. For TWIC NXEGEN cards, the TWIC card application shall be selected. The reader should then perform the proof of origin operation for card authenticity after first reading and validating the Card Authentication certificate stored in the corresponding card application. (PIV card application for Legacy cards and TWIC Card application for TWIC NEXGEN cards)).

Rationale: The TWIC Signed CHUID is the source of the reference FASC-N; not the PIV/TWIC Card Authentication Certificate. This suggestion permits comparison of the TWIC reference FASC-N to the FASC-N value present in the Subject Alternate Name extension of the Card Authentication Certificate stored in the PIV/TWIC card application

Mode 3 – BIOMETRIC AUTHENTICATION

For a contact reader, the TWIC card application is selected to obtain the reference TWIC FASC-N and credential expiration date from the TWIC signed CHUID (using Mode 1). The reader should then read the TWIC Privacy Key (TPK) object, then the enciphered Fingerprint Biometrics object, decipher the enciphered Fingerprint biometric data using the TPK, validate the biometric data header and signature and finally perform a biometric match using a live sample and the aforementioned data as the card holder reference. NOTE: The order of reading the TPK container and the TWIC enciphered Biometrics container is not critical nor enforced by the TSA testing regimen.

A contactless reader biometric match requires that the TWIC TPK information also be available to the reader; either via an online lookup service, or cached in a table organized by a FASC-N index available to the TWIC solution, or by reading the PDF 417 bar code on the back of the card for TWIC NEXGEN cards.

TSA suggests capturing the TPK, and other information accessible only over a contact interface, at time of PACS registration (if used). For a portable (or standalone) TWIC reader, the TPK shall be obtained either from the PDF 417 bar code, or by having access to a list of TPKs. Linked to a given FACS-N (pre-registration).

Specification Note: The TPK is not accessible over the contactless interface to preserve the integrity of the enciphered data object transfer security mechanism.

Rationale: Permits comparison of the reference TWIC FASC-N to the FASC-N value in the deciphered Fingerprint template patron header. The PIV card application is not used for this Mode.

Mode 4 – CARD AUTHENTICATION combined with Biometric Cardholder verification

The reader should perform a TWIC Signed CHUID read, a Mode 2 card authentication operation, and a Mode 3 TWIC biometric match. The order of operation is suggested to be a TWIC Signed CHUID read, then Mode 3 TWIC then Mode 2 for Legacy Cards to minimize selecting between card applications. As for TWIC NEXGEN cards the PIV card application should not be used, only one card application is selected and the order in which these operations are done is less critical.

Mode 4 is strongly recommended for all registration of a TWIC card.

Rationale: Provides a strong two-factor authentication process without need to enter a PIN (which is not available over the contactless interface). For TWIC Legacy cards, both the TWIC and PIV card applications must be used due to the fact cryptographic operations are limited to the PIV card application. This constraint does not exist for TWIC NEXGEN cards

Mode 5 – Cardholder Verification Picture

This mode is only available with TWIC NEXGEN cards[3]. It requires the TWIC reader to have access to the card TPK (previous card registration, access using the contact interface, or reading the PDF 417 on the back of the card) to decipher the cardholder picture read from the card. The verification of the picture has to be done either by an attendant or by a picture verification system most likely external to the reader.

Mode 6 – Card Authentication combined with cardholder Picture Verification

This mode is available only with TWIC NEXGEN cards. (see note about using TWIC legacy cards to retrieve the cardholder picture). It combines Mode 5 and Mode 2, along with Mode 1 making sure the card CHUID is coherent.

----

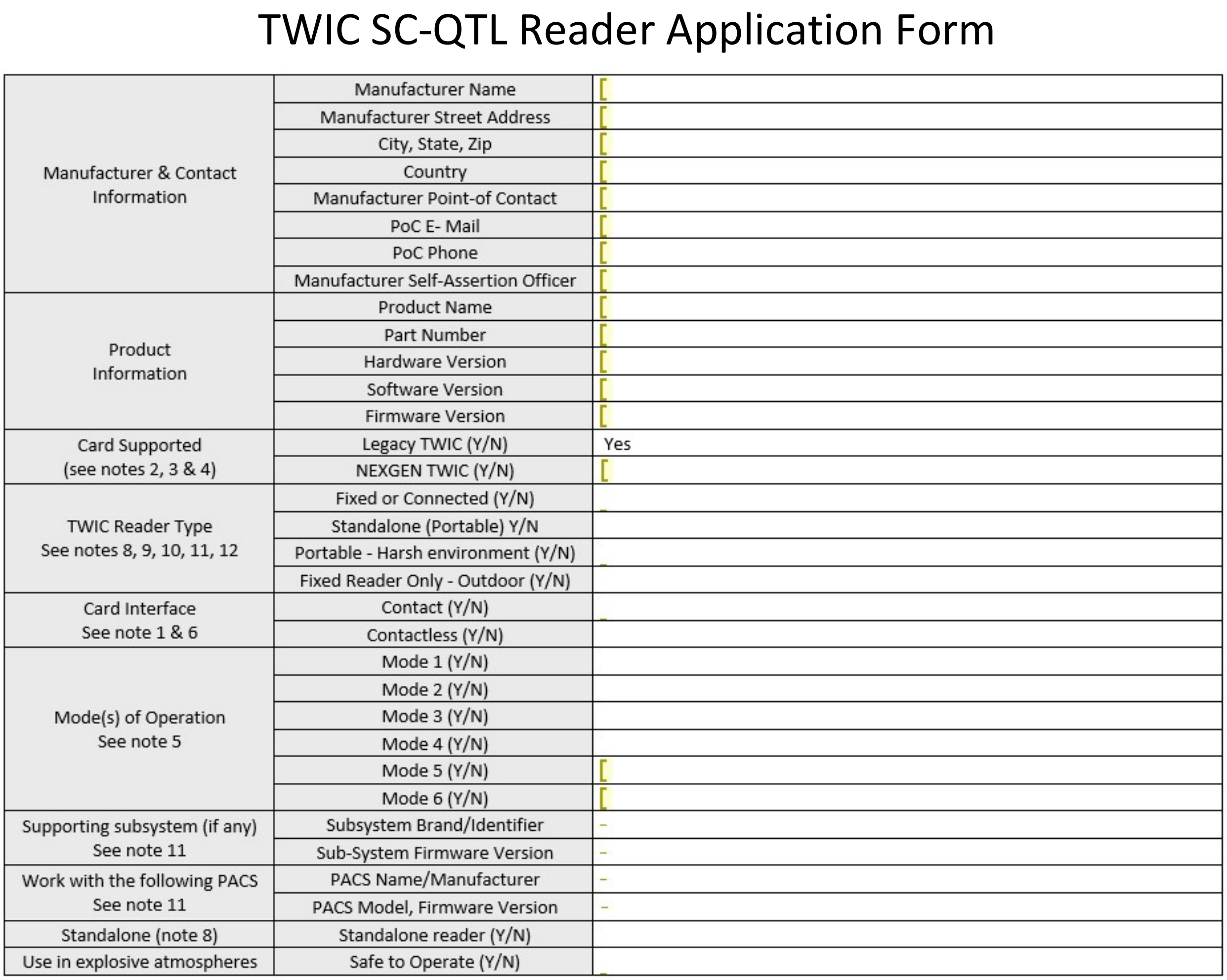
[3] For TWIC Legacy Cards, if the cardholder picture access is required (this may happen for card registration), the PIV card application may be used but will require a PIN to be presented to the card.

The suggested guidance on options detailed in this section, if all suggestions are selected by the Applicant, will likely be accepted by TSA as the rationale for each choice is known in advance.

If an Applicant’s product offering selects options different from those suggested, TSA might likely require the Applicant explain the rationale of each alternate option choice to TSA and, how they address for using their option choice all security and cross-check requirements detailed in the TWIC reader specification.

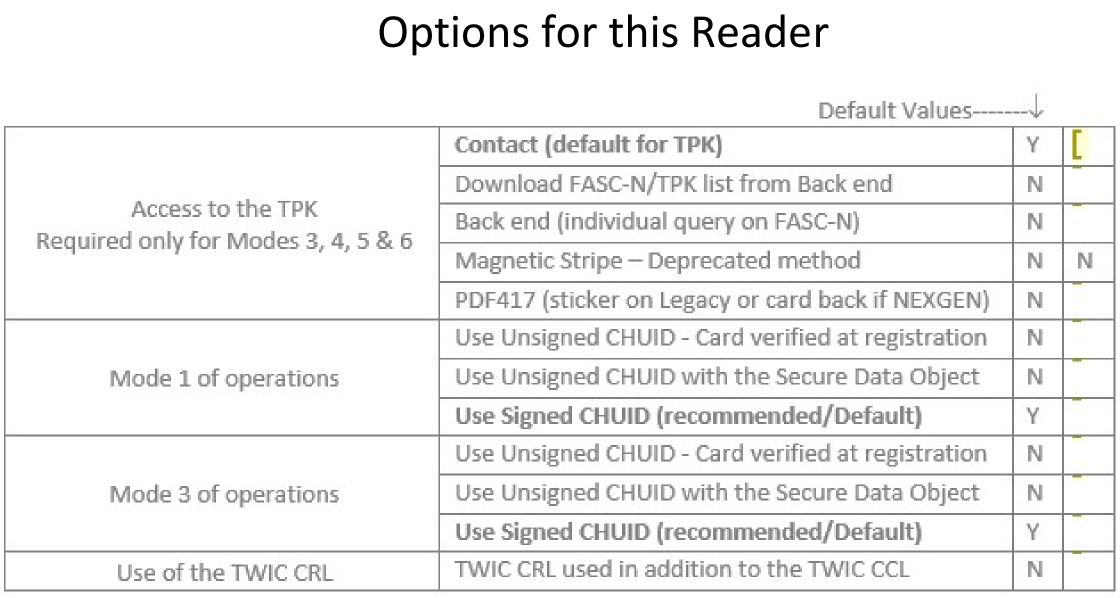
3.1.2 Sample of a Completed TWIC Reader Application Form

The form has two pages which need to be completed by the applicant:



TWIC SC-QTL Reader Application Form

Manufacturer & Contact Information	Manufacturer Name	[
	Manufacturer Street Address	[
	City, State, Zip	[
	Country	[
	Manufacturer Point-of Contact	[
	PoC E- Mail	[
	PoC Phone	[
	Manufacturer Self-Assertion Officer	[
Product Information	Product Name	[
	Part Number	[
	Hardware Version	[
	Software Version	[
	Firmware Version	[
Card Supported (see notes 2, 3 & 4)	Legacy TWIC (Y/N)	Yes
	NEXGEN TWIC (Y/N)	[
TWIC Reader Type See notes 8, 9, 10, 11, 12	Fixed or Connected (Y/N)	
	Standalone (Portable) Y/N	
	Portable - Harsh environment (Y/N)	
	Fixed Reader Only - Outdoor (Y/N)	
Card Interface See note 1 & 6	Contact (Y/N)	
	Contactless (Y/N)	
Mode(s) of Operation See note 5	Mode 1 (Y/N)	
	Mode 2 (Y/N)	
	Mode 3 (Y/N)	
	Mode 4 (Y/N)	
	Mode 5 (Y/N)	[
	Mode 6 (Y/N)	[
Supporting subsystem (if any) See note 11	Subsystem Brand/Identifier	
	Sub-System Firmware Version	
Work with the following PACS See note 11	PACS Name/Manufacturer	
	PACS Model, Firmware Version	
Standalone (note 8)	Standalone reader (Y/N)	
Use in explosive atmospheres	Safe to Operate (Y/N)	



Options for this Reader

Default Values-------↓

Access to the TPK Required only for Modes 3, 4, 5 & 6	**Contact (default for TPK)**	Y	[
	Download FASC-N/TPK list from Back end	N	
	Back end (individual query on FASC-N)	N	
	Magnetic Stripe – Deprecated method	N	N
	PDF417 (sticker on Legacy or card back if NEXGEN)	N	
Mode 1 of operations	Use Unsigned CHUID - Card verified at registration	N	
	Use Unsigned CHUID with the Secure Data Object	N	
	Use Signed CHUID (recommended/Default)	Y	
Mode 3 of operations	Use Unsigned CHUID - Card verified at registration	N	
	Use Unsigned CHUID with the Secure Data Object	N	
	Use Signed CHUID (recommended/Default)	Y	
Use of the TWIC CRL	TWIC CRL used in addition to the TWIC CCL	N	

3.2 TSA Review of the Application and Providing a Self-Test Package to the Applicant

The TSA PMO will review the Applicant's TWIC Reader Application Form for completeness and accuracy and conduct a detailed examination (product review) to assess the product's conformance to the TWIC specification and its characteristics claimed by the applicant. The reader specifications and the Applicant claims are reviewed to ensure that the reader falls within the parameters of a TWIC PMO recognized TWIC reader. The Applicant's list of proposed claims is then examined to ensure the adequacy and appropriateness of the self-tests to be identified by TSA in the self-test package. If the PMO approves the application package provided by the Applicant, the product will be registered into the TSA SC QTL system by assigning a unique SC QTL Identification number (SC QTL-ID) to be associated with the Applicant's specific combination of reader hardware, software, and the set of claims that shall comprise the self-certification testing to be performed. A self-certification kit will then be sent to the Applicant.

This kit should likely include the following:

Documentation including:

- NEXGEN Specification Part 1, Part 2 Part 3, and Part 4[4]
- TWIC Reader Test Procedures for Legacy & NEXGEN Product specific Derived Test Requirements (DTR) which is a complete list of specification functional requirements to be satisfied for each of the security modes of operation (also available on the TSA/TWIC web site)
- Specific Product Test Procedures based on the information provided in the Reader Application form. Test steps to be performed to satisfy each of the DTRs.

Tools including:

- A set of Legacy &/or NEXGEN test cards to be used in the self-certification compliance tests.
- Access information to obtain a third-party software package and related documentation for biometrically personalizing each of the test cards with the Applicant's principal investigator's fingerprints (if biometric testing Modes 3, 4 5 or 6are enabled).

A specific tool has been developed for TSA listing all the required Applicant's DTR test requirements to be tested or claimed. This DTR list is derived from the information provided in the TWIC Reader Application form. The internal TSA tool further produces a list of the specific tests to be performed as well as the test cards required to test a given DTR. This tool generates a unique list, for this reader Applicant application, of each test case and the test cards required.

The following are excerpts from an example DTR and Test Case lists produced for a fictional product (shown in the Application Form example) by the internal TSA tool:

[4] These are available on the TSA TWIC web site at: https://www.tsa.gov/twic and selecting the TWIC Technology tab.

Applicable DTRs

DTR	Description	Specification Reference	Test Procedure Reference
G.38	All TWIC reader shall have access to a system clock capable of providing the current date and time.	Section 4.4.3 - Item 4, Section 8 - Item 15	Configuration Tests, 3.1.9
CL.01	The contactless smart card TWIC reader component shall conform to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201.	Section 4.6 Contactless Interface	Applicant Documentation
CL.02	Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s.	Section 4.6 Contactless Interface	Applicant Documentation
CL.03	A TWIC Reader shall reject all of the presented cards if two or more contactless smart cards are presented at the same time in a TWIC reader's contactless field.	Section 4.6 Contactless Interface	4.10.1
CL.04	TWIC contactless readers shall require that a TWIC card, once read, shall be removed from the RF field for at least one second before attempting to read any new contactless card	Section 4.6 Contactless Interface	4.10.2
G.01	TWIC Readers shall support configuration of at least one authentication modes named 1 to 4 as described in the section TWIC Nodes of Operation	Section 4.4, Section 4.4.4	Indirectly Tested
G.03	Where necessary to operate from line voltage, a power supply approved by the reader manufacturer for use with a TWIC Reader shall be provided.	Section 6.5 - Item 1	3.1.1
G.20	A TWIC Reader (or panel, with bi-directional reader communication) shall be locally configurable with the X.509 certificate containing the public key for all currently active Certificate Authorities (CAs) that are trusted by the reader in order to verify each CA signing certificate is from a known, trusted source.	Section 4.4.4, Section 4.5, Section 4.6, Section 5.2	Configuration Tests, 3.1.6, 4.2.3, 4.2.4, 4.2.7, 4.2.8, 4.3.4, 4.3.5, 4.3.7, 4.3.8, 4.4.3, 4.4.6, 4.4.7, 4.5.7, 4.5.10, 4.5.16, 4.5.17, 4.6.16, 4.6.17, 4.7.6, 4.7.7, 4.7.17, 4.7.18, 4.7.19, 4.7.20,4.8.7,4.8.7,4.8.10,4.8.11,4.9.3,4.9.4,4.9.11,4.9.12,4.9.13,4.9.14
G.21	TWIC Readers that support multi-mode operation shall be able to accept external triggers for the mode change.	Appendix D Section D.1	Applicant Documentation
M1.01	TWIC Readers may support Signed CHUID Verification	Section 4.4.3 - Mode 1	4.2.1
M1.02	The TWIC Reader verifies that the id-TWIC-content- signing object identifier is present in the card issuer's digital signature certificate for the document signer. If the id-TWIC-content-signing object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC Reader shall reject the card.	Section 4.4.3 - Items 5 and 11	4.2.6
M1.03	TWIC Readers shall verify the CHUID signature and origin up to and including the trust anchor.	Section 4.4.3 - Item 6	4.2.3, 4.2.4, 4.2.7, 4.2.8, 4.5.7, 4.5.16, 4.5.17,4.8.10,4.8.11
M1.04	The TWIC Reader shall decode the FASC-N TLV record and extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue. If connected to a back end system, the TWIC Reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N allowing the card to be uniquely identified.	Section 4.4.3 - Item 8	4.1.2, 4.2.2, 4.3.2, 4.6.5, 4.6.12
M1.05	If a TWIC Reader is configured for expiration checking using the signed CHUID, the date encoded in the signed CHUID data object is compared to the current date/time. If the date encoded in the signed CHUID data object is before the current date/time, the Reader shall reject the card.	Section 4.4.3 - Item 4	4.2.5, 4.5.8,4.8.5
M1.06	If the TWIC Reader is configured to use the TWIC Canceled Card List to check for card revocation using the signed CHUID, the TWIC Reader checks to see if the FASC-N from the signed CHUID data object is listed on the latest version of the CCL accessed by the reader. If the FASC-N from the signed CHUID data object is listed on the latest version of the CCL accessed by the Reader, the TWIC Reader shall reject the presented card.	Section 4.4.3 - Item 9	4.2.9, 4.5.18, 4.6.18,4.8.12

Functional Test Suite 4.4 - Active Card Authentication

The purpose of this test is to verify that readers with claimed support for Active Card Authentication (Authentication Mode #2)

Test Case	Title of Test Case	Test Card Used	Expected Result	Contact Result	Contactless Result	Test Notes
4.4.1	Normal Operation	TCL-01	PASS			
4.4.2	FASC-N Check	TCL-02	PASS			
4.4.3	Trust Anchor Verification	TCL-10	FAIL			
4.4.4	Challenge Response	TCL-09	FAIL			
4.4.5	Expiration Date Check	TCL-11	FAIL			
4.4.6	Card Authentication Certificate Signature Verification	TCL-25	FAIL			
4.4.7	Subordinate CA Certificate Signature Verification	TCL-27	FAIL			
4.4.9	Canceled Card List Check	TCL-24	FAIL			

TWIC NEXGEN Test Card Configurations

The following table represents the TWIC NEXGEN test cards along with their unique configuration required for performing the test methods described in the previous Sections.

Card #	Card Identifier	PIV Application Details	TWIC Application Details
1	TCN-01		Within the FASC-N, the Individual Credential Issue (ICI) = 1.
2	TCN-02		FASC-N in the unsigned CHUID is different from all other instances of the FASC-N on the TWIC Application.
			FASC-N in the signed CHUID is different from all other instances of the FASC-N on the TWIC Application.
			FASC-N in the Card Authentication is different from all other instances of the FASC-N on the TWIC Application.
			FASC-N in the biometric doesn't match the FASC-N in the unsigned CHUID.
			FASC-N in the biometric doesn't match the FASC-N in the signed CHUID.
			FASC-N in the Picture in the data object does not match the FASC-N in the signed CHUID.
3	TCN-03		Expired Unsigned CHUID.
4	TCN-04		CHUID Signature invalid/corrupted.
5	TCN-05		Un-trusted content signing certificate in CHUID.
6	TCN-06		Expired CHUID.
7	TCN-07		Security Object signature invalid/corrupted.
8	TC-08	not used anymore.	
9	TCN-09		The private key doesn't match the public key present in the card authentication certificate.
10	TCN-10		Card auth cert signed by un-trusted CA.
11	TCN-11		An EXPIRED Card Authentication Certificate.
12	TCN-12		TPK stored on the TWIC Card is incorrect.
13	TCN-13		Signature on the picture and fingerprint biometric containers are invalid.
14	TCN-14		Data Object signing certificate does not have the content signing OID.

3.3 Applicant testing and TSA correspondence during Testing

Once the Applicant receives the self-certification kit and their SC QTL-ID from the TWIC SC QTL PMO, self-certification testing on the reader may begin. The testing should consist of completing all of the testing requirements from the list provided in the self-certification kit. If one or more functional tests fail, the Applicant needs to be aware of this if testing is performed by other than the Applicant. Any technical problems with the Applicant reader product should be resolved between the Applicant and the entity doing the testing. When consultation with the TWIC SC-QTL Point of contact is required to resolve a technical problem, the Applicant point of contact is expected by TSA to initiate the communications. In general, the Applicant or other designated point of contact may contact the TWIC SC-QTL Point of Contact for all general non-testing questions and comments related to the TWIC SC QTL program. All correspondence and communication should be directed to:

Attention: SC-QTL Point of contact
Transportation Administration
e-mail: TWIC-Technology@tsa.dhs.gov

Note: A personal contact information will be provided after the application process is initialized.

GUIDANCE: Where Mode options exist (e.g., CHUID reading) the Applicant should select ONE of the Mode options available (e.g., Mode 1 use the Signed CHUID data object) and perform only those tests identified for the selected Mode option. When reporting results each Mode option selected for testing should be clearly articulated. Refer to Section 3.1.1 for suggestions where options exist.

One card in the test set for TWIC Legacy is a NEXGEN TWIC card running on a revised smart card platform. Though meant only as a compatibility test, this card can also be used by the Applicant to evaluate the additional functionality of NEXGEN to determine if any new feature merits adding functionality to a given product offering.

In the card test set for TWIC NEXGEN, the test cards do not have the PIV card application data loaded to make sure the TWIC reader will use only the TWIC NEXGEN modes.

It is suggested the use of TWO production-issued TWIC cards be accessible to the Applicant. One of these cards would be ACTIVE (not canceled, not expired). The second card should be either EXPIRED or CANCELED. (One technique to obtain a CANCELED TWIC car is to report an ACTIVE TWIC lost to TWIC customer support and have a new ACTIVE TWIC sent as a replacement. There is a cost of $60 for obtaining a CANCELED TWIC card in this manner.

Additionally, TWIC system issued TWIC cards can be used in the self-testing environment as an “unknown issuing authority” as they are issued from a different issuance platform than all the test cards.

Once testing is completed, the Applicant has two TWIC system issued cards that can be used to validate TWIC compatibility by simply adding the TWIC card chain of trust to the list of trusted certificates / signing authorities into the product or related access control system.

3.4 Applicant Testing Results Sent to TSA

When testing is complete, the Applicant shall send a report of their product conformance testing results to the TWIC SC QTL PMO. The results report sent to TSA must be accurate and complete. This report shall include the required detailed testing results produced from each of the completed test scenarios. Copies of other certifications from additional certified testing laboratories (e.g., U.L.) used to satisfy electrical, safety, environmental and other physical requirements shall also be included as well as all required self-attestations based on Applicant claims.

If the reader has successfully passed all self-certification requirements, the testing entity shall provide a letter to that effect to the TWIC SC QTL PMO including a recommendation to list the reader on the SC QTL. This letter should also include any special experience or problems encountered while running the tests and any suggestions for improving the self-certification test procedures. Appendix D.1 of the Administrative manual provides an example of such a letter.

GUIDANCE: Informing TSA the positive characteristics of the self-certification AND the challenges that might be overcome will assist TSA in improving the self-certification over time.

3.5 TSA Review of Applicant Results and Posting to the SC QTL

Once TSA receives the Applicant Testing Results a conformity checklist for the tested product is developed by the PMO after reviewing the detailed test reports submitted. This review may take some time to complete so the Applicant needs to be patient if a listing decision is not immediately forthcoming. Checking with the TSA point of contact occasionally is encouraged.

If the PMO determines that the product does not comply, details for corrective action are provided by the PMO to the Applicant. The Applicant must provide written evidence appropriate to the resolution of non-conformities within specified time limits. Such evidence may be a self-attestation or an additional report from a testing laboratory. The Applicant also has the option of submitting an objection to the determination by filing a complaint as described in Section **Error! Reference source not found.** of the administrative manual.

If the product is determined to have satisfied the minimum set of TWIC specification requirements, the PMO issues a letter to the Applicant stating TSA's intent to post the product on the TWIC SC QTL. The letter and the listing on the SC QTL shall include the SC QTL-ID number for reference purposes and the effective date of SC QTL listing. The webpage shall also include a high-level listing of the features of the product that were tested.

GUIDANCE: Allow some time for TSA to review the self-testing results. If no correspondence is received after 30 days it may be worth checking-in with the TSA PoC for a status update.

3.6 Annual Requirement to Certify the SC QTL product is Available and Unchanged

The TWIC SC QTL webpage list those products that have successfully completed self-certification testing. In addition to the SC QTL-ID each reader listing includes information on the features of the reader that were tested (i.e., biometric interface, card interface, TPK Source, authentication modes supported, indoor or outdoor use, any limitations vis-à-vis the TWIC specification with respect to environmental requirements, etc.).

Once an applicant's reader is listed on the SC QTL it must be re-affirmed by the Applicant on an annual basis that the reader is still available and unchanged. The Applicant or their testing entity shall perform full regression testing and send the results to the TWIC QTL PMO. Failure to notify the TWIC SC QTL PMO annually may result in the product being removed from the SC QTL. The Applicant may appeal any removal from the TWIC SC QTL as defined in Section 9 Appeals of the Administrative Menu.

All Test cases are conducted as per TWIC Reader Revised Specification - V2 - 2021-12-09.

Test Cards ae using SHA 256 Hash algorithm. Note: Readers must be able to process TWIC using SHA 1 (128) and TWIC using SHA2 (256).

GUIDANCE: Simply copying the previous year's testing results is highly discouraged. TSA may supply a new card set at any time which is not guaranteed to replicate the prior card set mix of good and faulted cards.

4. Contact Information

Parties having questions as to the content, applicability, or interpretation of this document may address their comments to:

Attention: **Joshua Whann – SC-QTL Point of contact**
Transportation Security Administration
Enrollment Services & Vetting Programs (ESVP)
6595 Springfield Center Drive,
Springfield, VA 22150
e-mail: TWIC-Technology@tsa.dhs.gov

Additional Informative Attachments

Applicant Information

Please provide business headquarters information below.

Applicant Name: ____

Address: ____

Telephone: ______________________________ Fax: ______________________________

Approved Signatory:

Name: __________________________________ Title: _____________________________

Telephone: _________________________________ E-mail: ____________________________

Authorized Representative:

Name: __________________________________ Title: _____________________________

Telephone: _________________________________ E-mail: ____________________________

Agreement

By submitting this application, I/we, on behalf of ______________________________________,

Applicant

hereby acknowledge and agree to the following:

1 I/we will not use any model's SC QTL listing status in a way that, in the opinion of TSA:

1.1 Is inconsistent with the TWIC product's listing status.

1.2 Brings the credibility of DHS, TSA, or the TWIC SC QTL Program into question.

1.3 Is misleading or inaccurate.

2 I/we agree, upon withdrawal, suspension, or revocation of listing status to immediately cease and desist any and all advertising or statements claiming conformance of the affected product(s).

3 I/we will use the listing status only in the manner for which it was issued and reference only the requirements of the specific standard to which the model was found to be compliant.

4 I/we will not create or otherwise publish in any form(written, electronic, or via internet) any document, advertisement, product literature or brochure that references TSA, TWIC or the TWIC SC QTL Program in a manner that is not consistent with this agreement.

5 I/we acknowledge that failure to comply with the provisions of this agreement immediately on such request by TSA constitutes grounds for suspension or revocation of product's listing status.

6 I/we agree to maintain a system of traceability between listed model designations, serial numbers, and the purchasers of each product.

7 I/we shall not assign this agreement in whole or in part to another party.

8 I/we hold PMO officials harmless and indemnify them from fees arising from any and all claims with respect to the applicant's listed products, to the TWIC SC QTL Program, to the TWIC QTL conformance statement and/or violation of the terms and conditions of this agreement.

9 I/we agree to notify PMO in writing on company letterhead if the authorized representative changes.

10 The TWIC SC QTL Program will maintain confidential all information obtained from the applicant and will not disclose such information to any third party without the prior written approval of the Applicant.

Authorized Representative:

As the Applicant's authorized representative, I have the authority to agree to all requirements of this document on the Applicant's behalf and attest that all statements are correct and made in good faith.

______________________________ ______________________________

Signature of Authorized Representative Date

TWIC SC QTL PMO Representative Acknowledgement:

______________________________ ______________________________

Signature Date

____

Name (Please print/type)