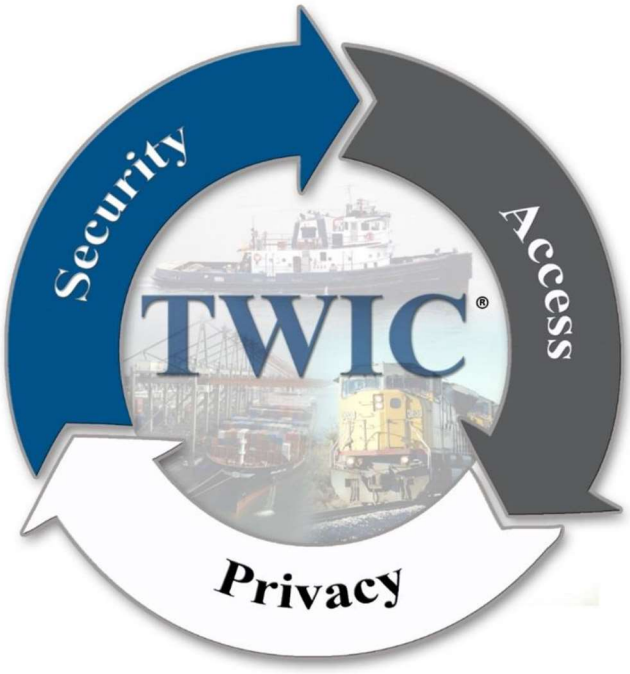

TWIC® Self -Certified Qualified Technology List

TWIC Reader Test Procedures for Legacy & NEXGEN

May 2024

Document Version 4

ID Technology Partners Inc.
Operations Support
Program Management Division
Vetting Programs Office
Maritime Branch

Revision History

Version / Date	Edits / Changes
V 0.1, 12/08/2014	Initial Draft. This document combines the Transportation Worker Identification Credential (TWIC) Qualified Technology List (QTL) Program Fixed Physical Access Control Reader Test Procedures and Portable TWIC Reader Test Procedures documents.
V 1.1 2021-02-25	Modifications of the document to adapt to the new Self-Certification QTL process.
V 2.1 2022-03-03	Correction of errors in all tests in which the card TC-08 was said to be used. This card is not used anymore in this version.
V 2.1 2022-03-03	Correction of test description 3.8.3 about the one second delay between two contactless cards presentation
V 3.0 2022-10-17	Fixed the incorrect numbering of the chapters related to the test case numbers.
V 4.0 2023-08-03	Removed unused test cases and indicated test cards not used any more. Added warning about SHA-256 being used in NEXGEN backward compatibility test.
V 4.a 2023-08-04	Added in Section 14.3 information about SHA-1 and SHA-256 to be supported.
V1 2024-04-17	Update of the document with the new SC-QTL procedures using the TWIC Legacy & NEXGEN Part 2 specification.
V1 2024-04-19	Updated for Tests Procedures for both Legacy & NEXGEN. Added the test card names for Legacy & NEXGEN
V3 2024-04-23	Incorporates all tests for Legacy & NEXGEN.
V4 2024-05-10	Added a new test card for Legacy protocol tests making sure the reader will work with old legacy cards in the field still using SHA-128 algorithm.

TABLE OF CONTENTS

List of Tables

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 (known 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 automatically read and validated by reader devices which have been deployed by maritime operators. The TWIC NEXGEN & Legacy – Part 3 – Reader Specification (hereafter, referred to as the TWIC Reader Specification) is a document issued by the Transportation Security Administration (TSA) which describes the expected behavior of a TWIC Reader, as well as the reader and back-end hardware performance and technical requirements. The TWIC Reader Specification addresses both fixed and portable[1] reader devices. The behavior of the TWIC Card itself is described in the TWIC NEXGEN & Legacy - Part 2 Card Specification.

The Transportation Security Administration (TSA) working with the Department of Homeland Security (DHS), has established a process and program allowing vendors to self-test and qualify TWIC reader products that read, verify, and authenticate the TWIC cards used in the TWIC Program. Products that are deemed to be compliant with the TWIC Reader Specification will be placed on a list referred to as the TWIC Self-Certified Qualified Technology List (SC-QTL) which can be used by owners and operators of regulated maritime facilities and vessels to assist in their TWIC reader and back-end systems purchasing decisions.

The TSA TWIC Program Management Office operating under the TSA Office of Security Policy and Industry Engagement (OSPIE) has established the SC-QTL program to provide an on-going process of TWIC reader self-certification process assessing the conformance of fixed and portable TWIC readers with the TWIC specification.

1.2 Purpose and Scope

Per the TWIC Reader specification, a Portable TWIC Reader is defined as a *handheld TWIC reader that may be used for portable, spot-check identity verification*. Additionally, a Fixed TWIC Reader is defined as a *TWIC reader installed in a wall, turnstile or similar type installation which communicates with an external access control system to control a door, gate, turnstile, etc. Fixed TWIC readers may operate in indoor environments or in outdoor environments exposed to the weather*.

[1] Some Portable TWIC Readers are Standalone, meaning without any permanent connection with a back-end system.

This Test Procedure provides details on the functional test methods that need to be executed by an Applicant's Fixed or Portable TWIC Reader to be listed on the Self-Certified Qualified Technology List (SC-QTL). Conformance to the test methods specified in this document may not result in the Card Reader being listed on the SC-QTL. The Product shall meet all applicable requirements as listed within the relevant test cases for this Reader. prior to being deemed as conformant and listed on the SC-QTL.

1.3 Summary of Changes to the Card Specification

This document uses the new version of the TWIC documentation which replaces the old 2012 Reader and Card Specification. This 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 TWIC NEXGEN cards,
4. Part 4 – TWIC registration and TWIC card use by a PACS.

The above documents cover the two types of TWIC cards: Legacy (being currently issued and using a chip named V7) as well as the soon to come new TWIC card called NEXGEN (which uses a new Chip called V8 and should replace TWIC Legacy sometime in 2024).
A TWIC reader must be qualified to work with at least the TWIC Legacy cards as well as using the TWIC NEXEGN card in backward compatibility mode). A specific suite of TWIC NEXGEN test cards is used to test the TWIC reader, which wants to take advantage of the improved functions available in the TWIC NEXGEN version.
The main changes between the TWIC 2012 specification and this newer version of the TWIC documentation are listed hereafter:

- All cards now issued (Legacy as well as NEXGEN) are using the SHA-256 algorithm instead of the now obsolete SHA-1 version. Nevertheless, as old TWIC Legacy cards are in circulation for at least the next five years, the TWIC reader shall be able to use either of these algorithms.
- As the TWIC Cards use different types of chip, the ATR (Answer-to-Reset) may be different and only the use of the TWIC AID (Application Identifier) is to be used to find out the type of card presented to the reader (Legacy or NEXGEN).
- The use of the Magnetic Stripe is deprecated and will not be available on TWIC NEXGEN cards. Nevertheless, if the TWIC reader uses this method to access the TPK it could be done, but this will not work on TWIC NEXGEN cards used in backward compatibility and as such the reader would fail the tests.
- The use of the unsigned CHUID is no longer recommended and will be deprecated in the future.
- These tests use some test cards named according to the following structure:
    - PRL-xx Cards used to register test Legacy Cards.
    - TCL-xx Cards used to run the various tests for Legacy cards and NEXGEN card (TCL-38) in backward compatibility mode.
    - PRN-xx Cards used to register test NEXGEN cards.
    - TCN-xx Cards used to run the various tests for TWIC NEXGEN cards.

- In the test procedures, when a test card is mentioned, the generic term TCL/N-xx will be used allowing to cover both TCL-xx cards for Legacy and TCN-xx cards for NEXGEN.
- In the test procedures, when a test card used for registration is mentioned, the generic term PRL/N-xx will be used allowing to cover both PRL-xx cards for Legacy and PRN-xx cards for NEXGEN.
- As all TWIC Legacy test cards will have the FASC-N starting by 7099-7099-xxxx or 7099-8038-xxxx, and all TWIC NEXGEN test cards will have the FASC-N starting by 7099-7199-xxxx or 7099-8138-xxxx. In the test procedures, when a FASC-N is explicitly mentioned, it will be listed as 7099-7y99-xxxxx or 7099-8y38-xxxxx with "y" being a zero (0) for TWIC Legacy and a (1) for TWIC NEXGEN test cards.

1. In Table 2, Product Interfaces and Options for Accessing the TPK, it indicates that for each Mode (Authentication or Verification), the Interface to be tested is Optional (either contact or contactless). However, for each supported Authentication or Verification Mode, either Contact or Contactless **must** be selected.
2. If CCL is supported and the TPK source is TPK Registration, then the reader unit under test must not have the CCL configured until after Configuration Suite 2 - Test Card Registration is executed, as PRL-10 (for Legacy) or PRN-10 (for NEXGEN) contains the hot listed FASC-N and would fail card registration.
3. Protocol Test Suite 1 - TWIC Protocol Tests, reader mode configuration. As these tests are protocol tests and not behavioral tests, the reader unit under test may be configured in any of the supported modes for these tests.

Note: The differences between Verification and Authentication have to do with the level of trust the mode operates in. CHUID mode 1 (either signed or unsigned) is only a verification mode. The Active Card Authentication mode (ACA mode 2) is an authentication as it uses an active challenge with the card which proves the card has been issued by a trusted entity and has not been copied. The Biometric verification mode 3 provides an authentication of the legitimate cardholder, but outside of the control of the card. The Biometric & ACA mode 4 is considered as an authenticated mode because it includes the ACA.
In this document, the use of the term "Authentication" may mean verification or authentication from the security standpoint but is used to make sure the test procedure is conducted correctly.

1.4 Understanding the Test Procedures

Applicants that are interested in developing Fixed or Portable TWIC Reader products conformant to the TWIC Reader specification and supporting TWIC Legacy cards and possibly TWIC NEXGEN cards need to reference this test procedure to determine:

a. the functional test methods and test cases that apply to the TWIC Reader per Verification or Authentication mode and
b. the expected results for each test case within each test method in order to assert conformity to the TWIC Specification.

This document describes the functional test methods that need to be executed with the appropriate accreditation scope.

Table 1 below provides an example of a test case and provides a description of what information each row provides within the test case table.

Direct Requirement(s):	*<Requirement Identifier within the Derived Test Requirement Document extracted from the TWIC specification that is directly being tested by the test case.>*
Test Description:	*<Description of the functional requirement the test case is aimed at testing.>*
Test Applicability:	*<Identifies in what conditions/scenarios the test case needs to be executed.>*
Test Card(s):	*<Identifies the test cards necessary to execute the test case.>*
Test Process:	*<Describes the various activities (in steps) that need to be completed as part of the test case.>*
Expected Result:	*<Describes the expected results for the test case.>*

Table 1 - Sample Test Case

A Fixed or Portable TWIC Reader may support the required functionality through several configurations' options and interfaces. Based on the capability of the submitted product, the test methods within this document will need to be repeated for each supported configuration and interface option.

Table 2 identifies the set of options permissible for TWIC Readers based on the TWIC Reader specification which defines the reader unit under test.

Mode #	Authentication/Verification Mode Description	Interfaces to be tested		TPK Access to be tested
		Contact	Contactless	
1	Unsigned CHUID without Signature Verification	Optional	Optional	N/A
1	Unsigned CHUID with SDO Verification	Optional	Optional	N/A
1	Signed CHUID With Signature Verification	Optional	Optional	N/A
2	Active Card Authentication	Optional	Optional	N/A
3	Biometric Verification using Unsigned CHUID	Optional	Optional	Back-end System
				TWIC Card (magnetic stripe)
				TWIC Card (contact Interface)
				PDF 417
3	Biometric Verification Using Signed CHUID	Optional	Optional	Back-End System
				TWIC Card (magnetic stripe)
				TWIC Card (contact Interface)
				PDF 417
4	Biometric Verification with Card Authentication	Optional	Optional	Back End System
				TWIC Card (magnetic stripe)
				TWIC Card (contact Interface)
				PDF 417
The modes below are available only on TWIC NEXGEN cards				
5	Picture Verification	Optional	Optional	Back-end system
				TWIC Card (contact interface)
				PDF 417
6	Picture Verification with Card Authentication	Optional	Optional	Back-end system
				TWIC Card (contact interface)
				PDF 417

Table 2 - Portable TWIC Reader Interfaces and Options for Accessing the TPK

Notes:

- The use of contact or contactless interface is optional, but at least one should be selected.
- The use of the Unsigned CHUID is mentioned in this table (for mode 1 and mode 3) but not recommended. The tests will require the TWIC reader to at least support Signed CHUID with signature verification.
- The use of the magnetic stripe is deprecated and not recommended anymore as this feature will not be available on TWIC NEXGEN
- The use of a PDF 417 bar code for Legacy Cards requires a sticker to be printed with the TPK value; this sticker may be added to the TWIC plastic cardholder. The use of the format described in the NEXGEN specification Part 2 (section 4.9) is recommended.

References

2 Normative References[2]

[R1] TWIC NEXGEN & Legacy – Part 2 – Card Specification

[R2] TWIC NEXGEN & Legacy – Part 3 – Reader Specification

[R3] Tech_Bulletin_TWIC_2023_001-SHA-256 in Legacy

[R4] Tech_Bulletin_TWIC_2022_001-SC-QTL

[2] The technical bulletins (also called Technical Advisories) are available by sending an e-mail to the following address: TWIC-Technology@TSA.DHS.GOV

3 Configuration Test Methods

This section describes in detail the configuration test methods that apply to a TWIC Physical Access Control Reader under the TWIC Specification. Each test method and the applicable test cases shall be executed for every reader unit under test.

3.1 Configuration Test Suite 1: Reader Feature Configuration Test

This test method shall be executed for all reader units under test. The purpose of this test is to verify that reader configuration requirements have been satisfied by configuring all claimed reader features of the reader configuration under test. Note that this test suite provides a script of the configuration steps described in the TWIC SC-QTL Program Reader Test Procedures under each documented test suite. This test is a prerequisite for executing functional test suites for the reader configuration under test. Configuration of the reader for each feature should result in a normal status indication by the reader upon completion of each configuration operation.

3.1.1 Test Case 1.1: Reader electrical configuration and power-up

Direct Requirement(s):	G.03
Test Description:	The purpose of this test case is to configure reader power and any reader external interface connections such as to networks or PACS test interfaces (as applicable) and verify the ability of the TWIC reader to execute a normal power-up sequence prior to continuing reader configuration and test.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	N/A
Test Process:	1. Setup reader electrical configuration including any required external interfaces and power-up reader. 2. Document the results from the configuration.
Expected Result:	Reader provides normal indication after power-up.

3.1.2 Test Case 1.2: Configuration of Smart Card Interface Type

Direct Requirement(s):	G.36
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure smart card interface type, for readers with smart card interface type as a selectable configuration option.

Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to configurable smart card interfaces
Test Card(s):	N/A
Test Process:	1. Configure the reader smart card interface type 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.3 Test Case 1.3: Configuration of TPK Source

Direct Requirement(s):	G.30
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure TPK source (magstripe, contact interface, PDF 417 or TPK registration), for readers with TPK source as a selectable configuration option.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to configurable TPK source
Test Card(s):	N/A
Test Process:	1. Configure/download the reader TPK source. 2. Document the results from the configuration.
Expected Result:	Reader indicates normal completion of configuration.

3.1.4 Test Case 1.4: Configuration of Biometric Retry Counter

Direct Requirement(s):	B.2
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure the biometric retry counter.
Test Applicability:	▪ Applies to all authentication modes requiring biometric authentication. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	N/A
Test Process:	1. Configure the reader biometric retry counter to 3. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.5 Test Case 1.5: Configuration of Root CA Certificate

Direct Requirement(s):	G.20
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure the TWIC root CA certificate.
Test Applicability:	▪ Applies to all authentication modes requiring signature verification or card authentication. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	N/A
Test Process:	1. Configure TWIC test root CA certificate using ../Certificates/Test_Root_v4.cer. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.6 Test Case 1.6: Configuration of Subordinate CA Certificate

Direct Requirement(s):	G.20
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure the TWIC subordinate CA certificate.
Test Applicability:	▪ Applies to all authentication modes requiring signature verification or card authentication. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	N/A
Test Process:	1. Configure TWIC test subordinate CA certificate using ../Certificates/Test_CA1_v4.cer. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.7 Test Case 1.7: Configuration of Reader Authentication Mode

Direct Requirement(s):	G.01
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure supported TWIC authentication modes.
Test Applicability:	▪ Applies to all readers with selectable authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	N/A
Test Process:	1. Configure reader in supported reader authentication modes. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.8 Test Case 1.8: Test Case Deleted

3.1.9 Test Case 1.9: Configuration of Reader Time Base

Direct Requirement(s):	P.4, G.38
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure the reader date and time. This configuration is mandatory for readers supporting expiration checking.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all readers supporting expiration checking.
Test Card(s):	N/A
Test Process:	1. Configure reader time base to current date/time. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.10 Test Case 1.10: Configuration of PACS Interface Mode

Direct Requirement(s):	PO.6, F.13
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure PACS interface mode where PACS interface mode is a selectable option and is mandatory for readers supporting multiple PACS interface modes.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all readers supporting multiple PACS interface modes
Test Card(s):	N/A
Test Process:	1. Configure the PACS interface mode. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.11 Test Case 1.11: Test Case Deleted

3.1.12 Test Case 1.12: Configuration of TWIC Canceled Card List [3]

Direct Requirement(s):	P.1, F.21
Test Description:	The purpose of this test case is to configure TWIC Canceled Card List checking
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all TWIC readers and systems
Test Card(s):	N/A
Test Process:	1. Configure reader with TWIC Canceled Card List Checking. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.13 Test Case 1.13: Configuration of TWIC Certificate Revocation List

Direct Requirement(s):	PO.1, FO.8
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to load a test TWIC Certificate Revocation List.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all readers supporting CRL checking.
Test Card(s):	N/A
Test Process:	1. Configure reader with TWIC Certificate Revocation List using ../Certificates/revoked.crl. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

3.1.14 Test Case 1.14: Configuration of TWIC Certificate Revocation List Checking

Direct Requirement(s):	PO.1, FO.8
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to configure TWIC Certificate Revocation List checking where this checking is a selectable option.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all readers supporting CRL checking.
Test Card(s):	N/A
Test Process:	1. Configure reader for TWIC Certificate Revocation List Checking. 2. Document the results from the configuration.
Expected Result:	Reader/test fixture indicates normal completion of configuration.

[3] IF the TPK Source for the reader unit under test is TPK Registration, do NOT configure the CCL at this time. Indicate "False" under Operator Observation, indicate that the CCL needs to be set up after the execution of Configuration Test Suite 2: Test Card Registration in Additional Operator Observations, and override the failed test status to passed.

3.1.15 Test Case 1.15: Reader Log File Creation and Export

Direct Requirement(s):	G.32, G.33, G.34
Test Description:	The purpose of this test case is to verify the ability of the TWIC reader to create, view and export the TWIC reader log file.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing. ▪ Applies to all readers.
Test Card(s):	N/A
Test Process:	1. Execute procedure to view and export reader log file. 2. Document the results from the configuration.
Expected Result:	Reader log file is viewable and exportable.

3.1.16 Test Case 1.16: Test Case Deleted

3.1.17 Test Case 1.17: Test Case Deleted

3.1.18 Test Case 1.18: Test Case Deleted

3.2 Configuration Test Suite 2: Test Card Registration

This test method shall be executed for all reader units under test when a card registration is required. The purpose of this configuration suite is to register TPKs to support testing of the reader under test, when only the contactless interface is used. Note that this test suite provides a script of the test card registration steps for readers supporting registration of TWIC Privacy Keys. All TPKs and corresponding FASC-Ns present in all test cards must be correctly registered for all test cards in the full test card set. This test is a prerequisite for executing functional test suites for the reader configuration under test. Registration for each credential should result in a normal status indication by the reader upon completion of each operation.

3.2.1 Test Case 2.1: Registration of Test FASC-N 7099-7y99-001131-1-1-0000045831170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001131-1-1-0000045831170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-01
Test Process:	1. Present test card PRL/N-01 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.2 Test Case 2.2: Registration of Test FASC-N 7099-7y99-001132-1-1-0000045832170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001132-1-1-0000045832170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-02
Test Process:	1. Present test card PRL/N-02 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.3 Test Case 2.3: Registration of Test FASC-N 7099-7y99-001133-1-1-0000045833170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001133-1-1-0000045833170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-03
Test Process:	1. Present test card PRL/N-03 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.4 Test Case 2.4: Registration of Test FASC-N 7099-7y99-001134-1-1-0000045834170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001134-1-1-0000045834170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-04
Test Process:	1. Present test card PRL/N-04 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.5 Test Case 2.5: Registration of Test FASC-N 7099-7y99-001135-1-1-0000045835170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001135-1-1-0000045835170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-05
Test Process:	1. Present test card PRL/N-05 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.6 Test Case 2.6: Registration of Test FASC-N 7099-7y99-001136-1-1-0000045836170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001136-1-1-0000045836170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-06
Test Process:	1. Present test card PRL/N-06 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.7 Test Case 2.7: Registration of Test FASC-N 7099-7y99-001137-1-1-0000045837170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-7y99-001137-1-1-0000045837170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-07
Test Process:	1. Present test card PRL/N-07 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

3.2.8 Test Case 2.8: Test Case Deleted

3.2.9 Test Case 2.9: Test Case Deleted

3.2.10 Test Case 2.10: Registration of Test FASC-N 7099-9y38-000003-1-1-0000405028170992 and TPK

Direct Requirement(s):	G.30
Test Description:	The purpose of this configuration case is to register the test FASC-N 7099-9y38-000003-1-1-0000405028170992.
Test Applicability:	▪ Applies to all authentication modes. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	PRL/N-10
Test Process:	1. Present test card PRL/N-10 to the reader for TPK registration. 2. Observe the log generated to review the results. 3. Document the results from the configuration.
Expected Result:	Registration completed without indication of failure.

Note for this test procedure: The test cards PRL-10 (for Legacy) and PRN-10 (for NEXGEN) do contain a canceled FASC-N which is on the CCL. This is to allow the test of the CCL later when presenting a card which has been registered but later cancelled. So, during this step, the CCL should not be updated yet.

3.2.11 Test Case 2.11: Test Case Deleted

3.2.12 Test Case 2.12: Test Case Deleted

4 Functional & Protocol Test Methods for TWIC Legacy and NEXGEN

This section describes in detail the functional test methods (mapped to Authentication modes) that apply to a TWIC Reader under the TWIC Reader Specification.
After completing the test configuration, each test method and the applicable test cases shall be executed for every Authentication mode claimed by the reader unit under test[4].

Details for the Test Cards to be used within each test case are described in each Section.

4.1 Functional Test Suite 1: Unsigned CHUID without Signature Verification (Authentication Mode #1)

This test method shall be executed for all products that support the Unsigned CHUID without Signature Verification Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-03, TCL-21 for Legacy tests and TCN-01, TCN-02, TCN-03, TCN-21 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test cases that apply to the Unsigned CHUID without Signature Verification Authentication mode, the reader unit under test shall be configured as stated below.

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in Unsigned CHUID without Signature Verification Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the product to use the appropriate output format under the current configuration of the unit under test (if supported). ▪ Configure the time on the product (if supported) ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect the interface of the product to the PACS (if supported). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. Commence execution of the applicable test cases within the relevant test method.

Table 3 - Reader unit under test configuration

[4] A reader unit under test (also referred to as the reader under a particular configuration option) is defined by (i) the Authentication mode, (ii) the interface being used, and (iii) the source of the TPK

4.1.1 Test Case 1.1: Unsigned CHUID without Signature Verification - Normal Operation

Direct Requirement(s):	G.01, G.07, M1O.2
Test Description:	This test is used to determine if the product supports the Unsigned CHUID without Signature Verification Authentication mode using the unsigned CHUID.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID without Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Review the output. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged corresponds to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-01 (if supported).

4.1.2 Test Case 1.2: Unsigned CHUID without Signature Verification – FASC-N Check

Direct Requirement(s):	M1.04, G.28
Test Description:	This test is used to determine if the product retrieves the FASC-N from the unsigned CHUID from the TWIC Application.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID without Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Review the output 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-02 concludes successfully. The FASC-N logged corresponds to the FASC-N in the unsigned CHUID recorded for TCL/N-02 (if supported).

4.1.3 Test Case 1.3: Unsigned CHUID without Signature Verification – Expiration Date Check

Direct Requirement(s):	M1.09, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the unsigned CHUID.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID without Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-03
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-03. 2. Review the output. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-03 since the unsigned CHUID is expired. for the Log file should indicate the unsuccessful authentication attempt (if supported).

4.1.4 Test Case 1.4: Unsigned CHUID without Signature Verification – Canceled Card List Check

Direct Requirement(s):	M1.10, P.1, F.21
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID without Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Review the output. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the TWIC Card is on the Canceled Card List. The log should indicate the given FASC-N was found on the CCL (if supported)

4.1.5 Test Case 1.5: Test Case Deleted

4.1.6 Test Case 1.6: Test Case Deleted

4.2 Functional Test Suite 2: Signed CHUID with Signature Verification (Authentication Mode #1)

This test method shall be executed for all products that support the Signed CHUID with Signature Verification Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-04, TCL-05, TCL-06, TCL-14, TCL-21, TCL-26, TCL-28 for Legacy tests TCN-01, TCN-02, TCN-04, TCN-05, TCN-06, TCN-14, TCN-21, TCN-26, TCN-28 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Signed CHUID with Signature Verification Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Signed CHUID with Signature Verification Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect the interface of the product to the PACS (if supported). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.2.1 Test Case 2.1: Signed CHUID with Signature Verification - Normal Operation

Direct Requirement(s):	G.01, G.07, M1.01
Test Description:	This test is used to determine if the product supports the CHUID verification Authentication mode using the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N recorded in the log should corresponds to the value recorded for the FASC-N in the signed CHUID of TCL/N-01 (if supported).

4.2.2 Test Case 2.2: Signed CHUID with Signature Verification – FASC-N Check

Direct Requirement(s):	M1.04, G.28
Test Description:	This test is used to determine if the product retrieves the FASC-N from the signed CHUID from the TWIC Application.
Test Applicability:	▪ Applies if the Reader supports Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-02 concludes successfully. The FASC-N recorded in the log should correspond to the FASC-N in the signed CHUID recorded for TCL/N-02 in the TWIC Application (if supported).

4.2.3 Test Case 2.3: Signed CHUID with Signature Verification – Signature Check

Direct Requirement(s):	G.20, M1.03
Test Description:	This test is used to determine if the product is able to verify the signature of the CHUID.
Test Applicability:	▪ Applies if the Reader supports Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-04
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-04. 2. Review the output. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-04 since the signature on the CHUID is broken/invalid. a transaction error code should be recorded in the reader log for the unsuccessful authentication attempt (if supported).

4.2.4 Test Case 2.4: Signed CHUID with Signature Verification – Trust Anchor Verification

Direct Requirement(s):	G.20, M1.03
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the CHUID object signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports the Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-05
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-05. 2. Review the output. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-05 since a trusted path cannot be built for the CHUID content-signer certificate. Transaction error code should be recorded in the reader output log.(if supported)

4.2.5 Test Case 2.5: Signed CHUID with Signature Verification – Expiration Date Check

Requirement(s):	M1.05, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform an expiration date check on the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-06
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-06. 2. Review the output 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-06 since the signed CHUID is expired. Transaction error code should be recorded in the reader log. (if supported)

4.2.6 Test Case 2.6: Signed CHUID with Signature Verification – CHUID Signer Check

Direct Requirement(s):	M1.02
Test Description:	This test is used to determine if the product is able to verify if the CHUID signer is an authorized issuer of TWIC Cards
Test Applicability:	▪ Applies if the Reader supports the Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-14
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-14 since the CHUID signer is not authorized. a transaction error code should be recorded in the reader log for the unsuccessful authentication attempt (if supported).

4.2.7 Test Case 2.7: Signed CHUID with Signature Verification – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-26
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-26 since the CHUID content signing certificate has an invalid signature. a transaction error code should be recorded in the reader log for the unsuccessful authentication attempt (if supported).

4.2.8 Test Case 2.8: Signed CHUID with Signature Verification – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-28
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. A transaction error code should be recorded in the reader log for the unsuccessful authentication attempt. (if supported).

4.2.9 Test Case 2.9: Signed CHUID with Signature Verification – Canceled Card List Check

Direct Requirement(s):	M1.06, P.1, F.21
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Signed CHUID with Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the TWIC Card is on the Canceled Card List. A transaction error code should be recorded in the reader log for the unsuccessful authentication attempt. (if supported).

4.2.10 Test Case 2.10: Test Case Deleted

4.2.11 Test Case 2.11: Test Case Deleted

4.3 Functional Test Suite 3: Unsigned CHUID with SDO Verification (Authentication Mode #1)

This test method shall be executed for all products that support the Unsigned CHUID with SDO Verification Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-03, TCL-05, TCL-07, TCL-14, TCL-21, TCL-26, TCL-28 for Legacy tests TCN-01, TCN-02, TCN-03, TCN-05, TCN-07, TCN-14, TCN-21, TCN-26, TCN-28 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Unsigned CHUID with SDO Verification Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Unsigned CHUID with SDO Verification Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect and configure the interface of the product to the PACS (if needed). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.3.1 Test Case 3.1: Unsigned CHUID with SDO Verification - Normal Operation

Direct Requirement(s):	G.01, G.07, M1O.1
Test Description:	This test is used to determine if the product supports the Unsigned CHUID with SDO Verification Authentication mode.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FACS-N logged corresponds to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-01 (if supported).

4.3.2 Test Case 3.2: Unsigned CHUID with SDO Verification – FASC-N Check

Direct Requirement(s):	M1.04, G.28
Test Description:	This test is used to determine if the product retrieves the FASC-N from the unsigned CHUID from the TWIC Application.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-02 concludes successfully. The FASC-N logged corresponds to the FASC-N in the unsigned CHUID recorded for TCL/N-02 (if supported).

4.3.3 Test Case 3.3: Unsigned CHUID with SDO Verification – Expiration Date Check

Direct Requirement(s):	M1.09, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the unsigned CHUID.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-03
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-03. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-03 since the unsigned CHUID is expired. The log should indicate the error code for the unsuccessful authentication attempt (if supported).

4.3.4 Test Case 3.4: Unsigned CHUID with SDO Verification – Trust Anchor Verification

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the security data object signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-05
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-05. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-05 since a trusted path cannot be built for the security object content signer. The log should indicate the error code for the unsuccessful authentication attempt (if supported).

4.3.5 Test Case 3.5: Unsigned CHUID with SDO Verification – Signature Check

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product is able to verify the signature of the security data object (SDO).
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-07
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-07. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-07 since the signature on the security object is invalid. The log should indicate an error code for the unsuccessful authentication attempt (if supported).

4.3.6 Test Case 3.6: Unsigned CHUID with SDO Verification – Signing Certificate Verification

Direct Requirement(s):	M1.08
Test Description:	This test is used to determine if the product is able to verify if the CHUID signer is an authorized issuer of TWIC Cards
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing..
Test Card(s):	TCL/N-14
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-14 since the CHUID signer is not authorized. The log should indicate an error code for the unsuccessful authentication attempt (if supported).

4.3.7 Test Case 3.7: Unsigned CHUID with SDO Verification – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-26
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-26 since the CHUID signing certificate has an invalid signature. The log should indicate a transaction error code for the unsuccessful authentication attempt (if supported).

4.3.8 Test Case 3.8: Unsigned CHUID with SDO Verification – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID with SDO Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-28
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. The log should indicate a transaction error code output for the unsuccessful authentication attempt (if supported).

4.3.9 Test Case 3.9: Unsigned CHUID with SDO Verification – Canceled Card List Check

Direct Requirement(s):	M1.10, P.1, F.21
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Unsigned CHUID without Signature Verification Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the TWIC Card is on the Canceled Card List. The log should indicate a transaction error code for the unsuccessful authentication attempt (if supported).

4.3.10 Test Case 3.10: Test Case Deleted

4.3.11 Test Case 3.11: Test Case Deleted

4.4 Functional Test Suite 4: Active Card Authentication (Authentication Mode #2)

This test method shall be executed for all products that support the Active Card Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test. For TWIC Legacy cards the PIV Card application shall be selected and for TWIC NEXGEN cards the TWIC Card application shall be selected.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

GEN	TCL-01, TCL-02, TCL-09, TCL-10, TCL-11, TCL-23, TCL-24, TCL-25, TCL-27 for Legacy tests TCN-01, TCN-02, TCN-09, TCN-10, TCN-11, TCN-23, TCN-24, TCN-25, TCN-27 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Active Card Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Active Card Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate Cas within the product. ▪ Configure the time on the product (if supported) ▪ Configure the product's logging capabilities ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Ensure the product has network connectivity and the capability to download CRLs. Configure the CRL URL (if required or applicable) ▪ Connect the interface of the product to the PACS (if supported). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method. ▪ For TWIC Legacy cards, the PIV card application is to be selected ▪ For TWIC NEXGEN cards, the TWIC card application is to be used.

4.4.1 Test Case 4.1: Active Card Authentication – Normal Operation

Direct Requirement(s):	G.01, G.07, M2.1, M2.2
Test Description:	This test is used to determine if the product supports the Active Card Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Active Card Authentication mode ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the signed CHUID of TCL/N-01 (if supported).

4.4.2 Test Case 4.2: Active Card Authentication – FASC-N Check

Direct Requirement(s):	M2.2, M2.5, G.28
Test Description:	This test is used to determine if the product retrieves the FASC-N from the card authentication certificate. For TWIC Legacy Cards the PIV Card application has to be used, and for TWIC NEXGEN Cards, the TWIC Card application has to be used.
Test Applicability:	▪ Applies if the Reader supports the Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-02 concludes successfully. The FASC-N in the log should correspond to the FASC-N in the card authentication certificate for TCL/N-02 (if supported).

4.4.3 Test Case 4.3: Active Card Authentication – Trust Anchor Verification

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the card authentication certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-10
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-10. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-10 since a trusted path cannot be built for the card authentication certificate. The log should record a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.4 Test Case 4.4: Active Card Authentication – Challenge Response

Direct Requirement(s):	M2.2, M2.6
Test Description:	This test is used to determine if the product is able to perform an asymmetric card authentication private key and certificate operation, such as general authenticate on a challenge of at least 127 bytes of unique data.
Test Applicability:	▪ Applies if the Reader supports Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-09
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-09. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-09 because the private and public keys of the card authentication certificate are not part of a pair. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.5 Test Case 4.5: Active Card Authentication – Expiration Date Check

Requirement(s):	M2.2, M2.4, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports the Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-11
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-11. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-11 since the card authentication certificate is expired. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.6 Test Case 4.6: Active Card Authentication – Card Authentication Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-25
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-25. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-25 since the card authentication certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.7 Test Case 4.7: Active Card Authentication – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-27
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-27. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-27 since the card authentication certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.8 Test Case 4.8: Active Card Authentication – CRL Check

Direct Requirement(s):	PO.1, FO.8, M2O.1
Test Description:	This test is used to determine if the product is able to check the card authentication certificate's status against a CRL.
Test Applicability:	▪ Applies if the Reader supports the Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-23
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-23. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-23 since the card authentication certificate is revoked. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.9 Test Case 4.9: Active Card Authentication – Canceled Card List Check

Direct Requirement(s):	M2.7, P.1, F.21, G.28
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Active Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-24
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-24. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-24 since the FASC-N on the card authentication certificate is on the Canceled Card List. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.4.10 Test Case 4.10: Test Case Deleted

4.4.11 Test Case 4.11: Test Case Deleted

4.4.12 Test Case 4.12: Test Case Deleted

4.5 Functional Test Suite 5: Biometric Verification Using Signed CHUID Authentication (Authentication Mode #3)

This test method shall be executed for all products that support the Biometric Verification Using Signed CHUID Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-04, TCL-05, TCL-06, TCL-12, TCL-13, TCL-14, TCL-15, TCL-18, TCL-19, TCL-20, TCL-21, TCL-26, TCL-28 for Legacy tests TCN-01, TCN-02, TCN-04, TCN-05, TCN-06, TCN-12, TCN-13, TCN-14, TCN-15, TCN-18, TCN-19, TCN-20, TCN-21, TCN-26, TCN-28 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Biometric Verification Using Signed CHUID Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Biometric Verification Using Signed CHUID Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ .Configure the source of the TPK. ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect the interface of the product to the PACS (if supported). ▪ Configure the product to lock access after "n" failed biometric 1:1 matching attempts. ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.5.1 Test Case 5.1: Biometric Verification Using Signed CHUID Authentication - Normal Operation

Direct Requirement(s):	G.01, G.07, M3.1, M3.5
Test Description:	This test is used to determine if the product supports Biometric Verification Using Signed CHUID Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.5.2 Test Case 5.2: Biometric Verification Using Signed CHUID Authentication – Secondary Finger

Direct Requirement(s):	M3.1, M3.5
Test Description:	This test is used to determine if the product supports the Biometric Verification Using Signed CHUID Authentication mode using the secondary enrolled finger of the test operator.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01 using the secondary fingerprint loaded. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.5.3 Test Case 5.3: Biometric Verification Using Signed CHUID Authentication – Reader Lockout I

Direct Requirement(s):	M3.5, M3.6, B.2
Test Description:	This test is used to verify that the biometric verification using signed CHUID completes successfully during the "n^{th}" attempt, after "n-1" failed finger matching attempts.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n-1" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.5.4 Test Case 5.4: Signed CHUID with Signature Verification + Biometric User Authentication – Reader Lockout II

Direct Requirement(s):	B.2, M3.6
Test Description:	This test is used to verify that the biometric verification and signed CHUID fails and locks the reader after "n" attempts of using non-matching finger.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.

Expected Result:	Authentication shall fail for TCL/N-01 since the number of attempts has been exceeded. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.5 Test Case 5.5: Biometric Verification Using Signed CHUID Authentication – FASC-N Check

Direct Requirement(s):	M3.2, M3.4, G.28
Test Description:	This test is used to determine if the product checks that the FASC-N from the signed CHUID matches that in the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-02 because the FASC-N in the signed CHUID doesn't match that in the biometric. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.6 Test Case 5.6: Biometric Verification Using Signed CHUID Authentication – Invalid CHUID Signature

Direct Requirement(s):	M1.3, M3.2
Test Description:	This test is used to determine if the product is able to verify the signature of the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-04
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-04. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-04 since the signature on the signed CHUID is broken/invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.7 Test Case 5.7: Biometric Verification Using Signed CHUID Authentication – Trust Anchor Verification

Direct Requirement(s):	G.20, M1.3, M3.2
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the CHUID object signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-05
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-05. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-05 since a trusted path cannot be built for the CHUID signer. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.8 Test Case 5.8: Biometric Verification Using Signed CHUID Authentication – Expiration Date Check

Direct Requirement(s):	M1.05, M3.2, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-06
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-06. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-06 since the signed CHUID is expired. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.9 Test Case 5.9: Biometric Verification Using Signed CHUID Authentication – TPK Check

Direct Requirement(s):	G.30, FO.6, G.37
Test Description:	This test is used to determine if the product is able to decrypt the encrypted biometric using the TPK from the TWIC Card
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-12
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-12. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-12 since the TPK is incorrect. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.10 Test Case 5.10: Biometric Verification Using Signed CHUID Authentication – Biometric Signature Verification

Direct Requirement(s):	G.20, M3.2
Test Description:	This test is used to determine if the product is able capable of verifying the signature on the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-13
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-13. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-13 since the biometric signature is broken/invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.11 Test Case 5.11: Biometric Verification Using Signed CHUID Authentication – Biometric Signer Check

Direct Requirement(s):	M3.2, M3.3
Test Description:	This test is used to determine if the product is able capable of verifying whether the biometric signer is authorized.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.

Test Card(s):	TCL/N-14
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-14 since the biometric signer was not authorized. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.12 Test Case 5.12: Biometric Verification Using Signed CHUID Authentication – FASC-N Match

Direct Requirement(s):	M3.2, M3.4
Test Description:	This test is used to determine if the product uses the FASC-N from the Signed CHUID and the Biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-15
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-15. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-15 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the signed CHUID of TCL/N-15 (if supported).

4.5.13 Test Case 5.13: Biometric Verification Using Signed CHUID Authentication – Minutiae = 0

Direct Requirement(s):	B.1
Test Description:	This test is used to determine if the product checks if the number of minutiae is zero and denies access when performing a Biometric Verification using Signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-18
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-18. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication fails for TCL/N-18 since the number of minutiae on the card is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.14 Test Case 5.14: Biometric Verification Using Signed CHUID Authentication – Finger Views = 0

Direct Requirement(s):	B.1
Test Description:	This test is used to determine if the product checks if the number of finger views in the Biometric Data Block is zero, and denies access, when performing Biometric Verification using Signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-19
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-19. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-19 since the number of finger views in the BDB is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.15 Test Case 5.15: Biometric Verification Using Signed CHUID Authentication – Finger Views = 1

Direct Requirement(s):	M3.5
Test Description:	This test is used to determine that the product performs biometric and signed CHUID verification, matching the operator's fingerprint against the template containing a single, usable fingerprint minutia.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-20
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-20. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-20 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the signed CHUID of TCL/N-20 (if supported).

4.5.16 Test Case 5.16: Biometric Verification Using Signed CHUID Authentication – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03, M3.2
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-26
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-26 since the CHUID content signing certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.17 Test Case 5.17: Biometric Verification Using Signed CHUID Authentication – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03, M3.2
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-28
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.18 Test Case 5.18: Biometric Verification Using Signed CHUID Authentication – Canceled Card List Check

Direct Requirement(s):	M1.06, P.1, FO.7
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification Using Signed CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the FASC-N is on the Canceled Card List. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.5.19 Test Case 5.19: Test Case Deleted

4.5.20 Test Case 5.20: Test Case Deleted

4.6 Functional Test Suite 6: Biometric Verification using Unsigned CHUID Authentication (Authentication Mode #3)

This test method shall be executed for all products that support the Biometric Verification using Unsigned CHUID Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-03, TCL-05, TCL-07, TCL-12, TCL-13, TCL-14, TCL-16, TCL-18, TCL-19, TCL-20, TCL-21, TCL-26, TCL-28 for Legacy tests TCN-01, TCN-02, TCN-03, TCN-05, TCN-07, TCN-12, TCN-13, TCN-14, TCN-16, TCN-18, TCN-19, TCN-20, TCN-21, TCN-26, TCN-28 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Biometric Verification using Unsigned CHUID Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Biometric Verification using Unsigned CHUID Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate Cas within the product. ▪ Configure the time on the product (if supported) ▪ Configure the source of the TPK. ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect the interface of the product to the PACS (if supported). ▪ Configure the product to lock access after "n" failed biometric 1:1 matching attempts. ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.6.1 Test Case 6.1: Biometric Verification using Unsigned CHUID Authentication – Normal Operation

Direct Requirement(s):	G.01, G.07, M1O.2, M3.5
Test Description:	This test is used to determine if the product supports Biometric Verification using Unsigned CHUID Authentication mode.
Test Applicability:	▪ Applies if the Reader supports unsigned CHUID with SDO Verification + Biometric Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-01 (if supported).

4.6.2 Test Case 6.2: Biometric Verification using Unsigned CHUID Authentication – Secondary Finger

Direct Requirement(s):	M1O.2, M3.5
Test Description:	This test is used to determine if the product is capable of using the secondary finger for performing the 1:1 biometric match when performing biometric verification using Biometric Verification using Unsigned CHUID Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01 using the secondary fingerprint loaded. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-01 (if supported).

4.6.3 Test Case 6.3: Biometric Verification using Unsigned CHUID Authentication – Reader Lockout I

Direct Requirement(s):	M3.5, M3.6, B.2
Test Description:	This test is used to verify that the biometric verification using unsigned CHUID with security data object verification completes successfully during the "n^{th}" attempt, after "n-1" failed finger matching attempts.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n-1" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-01 (if supported).

4.6.4 Test Case 6.4: Biometric Verification using Unsigned CHUID Authentication – Reader Lockout II

Direct Requirement(s):	M3.5, M3.6, M3.7, B.2
Test Description:	This test is used to verify that the Biometric Verification using Unsigned CHUID fails and locks the reader after "n" attempts of using non-matching finger.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01 3. Observe the log generated to review the results.

	4. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-01 since the number of attempts has been exceeded. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.5 Test Case 6.5: Biometric Verification using Unsigned CHUID Authentication – FASC-N Check

Direct Requirement(s):	M1.04, G.28
Test Description:	This test is used to determine if the product checks that the FASC-N from the unsigned CHUID matches that in the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-02 because the FASC-N in the unsigned CHUID doesn't match that in the biometric. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.6 Test Case 6.6: Biometric Verification using Unsigned CHUID Authentication – Expiration Date Check

Direct Requirement(s):	M1.09, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the unsigned CHUID.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-03
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-03. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-03 since the unsigned CHUID is expired. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.7 Test Case 6.7: Biometric Verification using Unsigned CHUID Authentication – Trust Anchor Verification

Direct Requirement(s):	M1.07
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the security data object signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-05
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-05. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-05 since a trusted path cannot be built for the security data object signer. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.8 Test Case 6.8: Biometric Verification using Unsigned CHUID Authentication – Signature Check

Direct Requirement(s):	M1.07
Test Description:	This test is used to determine if the product is able to verify the signature of the security data object during the Biometric Verification using Unsigned CHUID Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-07
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-07. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-07 since the signature on the security data object is invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.9 Test Case 6.9: Biometric Verification using Unsigned CHUID Authentication – TPK Check

Direct Requirement(s):	G.30, FO.6, G.37
Test Description:	This test is used to determine if the product is able to decrypt the encrypted biometric using the TPK from the TWIC Card
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-12
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-12. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-12 since the TPK is incorrect. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.10 Test Case 6.10: Biometric Verification using Unsigned CHUID Authentication – Biometric Signature Verification

Direct Requirement(s):	M3.3
Test Description:	This test is used to determine if the product is able capable of verifying the signature on the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-13
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-13. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-13 since the biometric signature is broken/invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.11 Test Case 6.11: Biometric Verification using Unsigned CHUID Authentication – Biometric Signer Check

Direct Requirement(s):	M1.08
Test Description:	This test is used to determine if the product is able capable of verifying whether the biometric signer is authorized.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-14
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-14 since the biometric signer was not authorized. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.12 Test Case 6.12: Biometric Verification using Unsigned CHUID Authentication – FASC-N Match

Direct Requirement(s):	M1.04
Test Description:	This test is used to determine if the product checks that the FASC-N from the unsigned CHUID matches that in the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-16
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-16. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-16 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-16 (if supported).

4.6.13 Test Case 6.13: Biometric Verification using Unsigned CHUID Authentication – Minutiae = 0

Direct Requirement(s):	B.1
Test Description:	This test is used to determine if the product checks if the number of minutiae is zero and denies access during a Biometric Verification using Unsigned CHUID Authentication.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-18
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-18. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-18 since the number of minutiae on the card is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.14 Test Case 6.14: Biometric Verification using Unsigned CHUID Authentication – Finger Views = 0

Direct Requirement(s):	B.1
Test Description:	This test is used to determine if the product checks if the number of finger views in the Biometric Data Block is zero and denies access when performing a biometric verification using Unsigned CHUID with SDO Verification.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-19
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-19. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-19 since the number of finger views in the BDB is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.15 Test Case 6.15: Biometric Verification using Unsigned CHUID Authentication – Finger Views = 1

Direct Requirement(s):	M3.5
Test Description:	This test is used to determine that the product performs biometric verification using Biometric Verification using Unsigned CHUID Authentication, matching the operator's fingerprint against the template containing a single, usable fingerprint minutia.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing..
Test Card(s):	TCL/N-20
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-20. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-20 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-20 (if supported).

4.6.16 Test Case 6.16: Biometric Verification using Unsigned CHUID Authentication – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-26
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-26 since the CHUID signing certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.17 Test Case 6.17: Biometric Verification using Unsigned CHUID Authentication – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M1.07
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-28
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-28 since the content CHUID signing certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.18 Test Case 6.18: Biometric Verification using Unsigned CHUID Authentication – Canceled Card List Check

Direct Requirement(s):	M1.06, P.1, F.21
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification using Unsigned CHUID Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the FASC-N is on the Canceled Card List. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.6.19 Test Case 6.19: Test Case Deleted

4.6.20 Test Case 6.20: Test Case Deleted

4.7 Functional Test Suite 7: Biometric Verification with Card Authentication (Authentication Mode #4)

This test method shall be executed for all products that support the Biometric Verification with Card Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, TCL-02, TCL-05, TCL-09, TCL-10, TCL-11, TCL-12, TCL-13, TCL-14, TCL-17, TCL-18, TCL-19, TCL-20, TCL-21, TCL-23, TCL-25, TCL-26, TCL-27, TCL-28 for Legacy tests TCN-01, TCN-02, TCN-05, TCN-09, TCN-10, TCN-11, TCN-12, TCN-13, TCN-14, TCN-17, TCN-18, TCN-19, TCN-20, TCN-21, TCN-23, TCN-25, TCN-26, TCN-27, TCN-28 for NEXGEN tests

Configuration for Reader Unit under Test

Prior to executing any of the test methods that apply to the Biometric Verification with Card Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Biometric Verification with Card Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the source of the TPK. ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Ensure the product has network connectivity and the capability to download CRLs. Configure the CRL URL (if required or applicable). ▪ Configure the product to lock access after "n" failed biometric 1:1 matching attempts. ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.7.1 Test Case 7.1: Biometric Verification with Card Authentication - Normal Operation

Direct Requirement(s):	G.01, G.07, M2.2, M4.1, M4.5
Test Description:	This test is used to determine if the product supports the Biometric Verification with Card Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.7.2 Test Case 7.2: Biometric Verification with Card Authentication – Secondary Finger

Direct Requirement(s):	M2.2, M4.1, M4.5
Test Description:	This test is used to determine if the product is capable of using the secondary finger for performing the 1:1 biometric match when performing biometric verification using card authentication.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01 using the secondary fingerprint loaded. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.7.3 Test Case 7.3: Biometric Verification with Card Authentication – Reader Lockout I

Direct Requirement(s):	M2.2, M4.5, M4.6, B.2
Test Description:	This test is used to verify that the Biometric Verification with Card Authentication completes successfully during the "n^{th}" attempt, after "n-1" failed finger matching attempts.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n-1" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-01 (if supported).

4.7.4 Test Case 7.4: Biometric Verification with Card Authentication – Reader Lockout II

Direct Requirement(s):	M2.2, M4.5, M4.6, M4.7, B.2
Test Description:	This test is used to verify that the Biometric Verification with Card Authentication fails and locks the reader after "n" attempts of using non-matching finger.
Test Applicability:	▪ Applies if the Reader provides an automatic lockout capability ▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01. Perform authentication ("n" times) using a live fingerprint that doesn't match the fingerprint loaded on the TCL/N-01. 2. Then, perform authentication using the correct fingerprint loaded on TCL/N-01. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.

Expected Result:	Authentication shall fail for TCL/N-01 since the number of attempts has been exceeded. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.5 Test Case 7.5: Biometric Verification with Card Authentication – FASC-N Check

Direct Requirement(s):	M2.2, M4.4, G.28
Test Description:	This test is used to determine if the product checks that the FASC-N from card authentication certificate matches that in the biometric.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-02
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-02 because the FASC-N in the card authentication certificate doesn't match that in the biometric. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.6 Test Case 7.6: Biometric Verification with Card Authentication - Trust Anchor Verification I

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the CHUID signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification with Card Authentication mode ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-05
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-05. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-05 since a trusted path cannot be built for the CHUID object signer. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.7 Test Case 7.7: Biometric Verification with Card Authentication - Trust Anchor Verification II

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the card authentication certificate back to a trusted TWIC root. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports Biometric Verification with Card Authentication mode ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-10
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-10. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-10 since a trusted path cannot be built for the card authentication certificate. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.8 Test Case 7.8: Biometric Verification with Card Authentication – Challenge Response

Direct Requirement(s):	M2.2, M2.6
Test Description:	This test is used to determine if the product is able to perform an asymmetric card authentication private key and certificate operation, such as general authenticate on a challenge of at least 127 bytes of unique data when performing Biometric Verification with Card Authentication. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-09
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-09. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-09 because the private and public keys of the card authentication certificate are not part of a

	pair. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.9 Test Case 7.9: Biometric Verification with Card Authentication – Expiration Date Check

Requirement(s):	M2.2, M2.4, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the card authentication certificate. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-11
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-11. 2. Observe the log generated to review the results. 3. Document the results from the authentication `attempt.`
Expected Result:	Authentication shall fail for TCL/N-11 since the card authentication certificate is expired. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.10 Test Case 7.10: Biometric Verification with Card Authentication – TPK Check

Direct Requirement(s):	M2.2, G.30, FO.6, G.37
Test Description:	This test is used to determine if the product is able to decrypt the encrypted biometric using the TPK from the TWIC Card
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-12
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-12. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-12 since the TPK is incorrect. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.11 Test Case 7.11: Biometric Verification with Card Authentication – Biometric Signature Verification

Direct Requirement(s):	M2.2, M4.3
Test Description:	This test is used to determine if the product is able capable of verifying the signature on the biometric.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-13
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-13. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-13 since the biometric signature is broken/invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.12 Test Case 7.12: Biometric Verification with Card Authentication – Biometric Signer Check

Direct Requirement(s):	M2.2, M4.2
Test Description:	This test is used to determine if the product is able capable of verifying whether the biometric signer is an authorized issuer.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-14
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCL/N-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-14 since the biometric signer was not authorized. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.13 Test Case 7.13: Biometric Verification with Card Authentication – FASC-N Match

Direct Requirement(s):	M4.4
Test Description:	This test is used to determine if the product uses the FASC-N from the card authentication certificate and the Biometric. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-17
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-17. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-17 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCL/N-17 (if supported).

4.7.14 Test Case 7.14: Biometric Verification with Card Authentication – Minutiae = 0

Direct Requirement(s):	M2.2, B.1
Test Description:	This test is used to determine if the product checks if the number of minutiae is zero and denies access when performing biometric verification using card authentication.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-18
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-18. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-18 since the number of minutiae on the card is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.15 Test Case 7.15: Biometric Verification with Card Authentication – Finger Views = 0

Direct Requirement(s):	M2.2, B.1
Test Description:	This test is used to determine if the product checks if the number of finger views in the Biometric Data Block is zero and denies access when performing Biometric Verification with Card Authentication.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-19
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-19. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-19 since the number of minutiae on the card is zero (0). The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.16 Test Case 7.16: Biometric Verification with Card Authentication – Finger Views = 1

Direct Requirement(s):	M2.2, M4.5
Test Description:	This test is used to determine that the product performs Biometric Verification with Card Authentication, matching the operator's fingerprint against the template containing a single, usable fingerprint minutia.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-20
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-20. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCL/N-20 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the unsigned CHUID of TCL/N-20 (if supported).

4.7.17 Test Case 7.17: Biometric Verification with Card Authentication – Card Authentication Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the card authentication certificate. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-25
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-25. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-25 since the card authentication certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.18 Test Case 7.18: Biometric Verification with Card Authentication – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-26
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-26 since the CHUID content signing certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.19 Test Case 7.19: Biometric Verification with Card Authentication – Subordinate CA Certificate Signature Verification I

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the card authentication certificate. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-27
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-27. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-27 since the card authentication certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.20 Test Case 7.20: Biometric Verification with Card Authentication – Subordinate CA Certificate Signature Verification II

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-28
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.21 Test Case 7.21: Biometric Verification with Card Authentication – Canceled Card List Check

Direct Requirement(s):	M2.7, P.1, FO.7
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-21
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-21 since the FASC-N is on the Canceled Card List. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.22 Test Case 7.22: Biometric Verification with Card Authentication – CRL Check

Direct Requirement(s):	M2.2, PO.1, FO.8
Test Description:	This test is used to determine if the product is able to check the card authentication certificate's status against a CRL. The test will use the card authentication certificate from the PIV Application for TWIC Legacy Cards or the card authentication certificate from the TWIC Card application for NEXGEN cards.
Test Applicability:	▪ Applies if the Reader supports the Biometric Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCL/N-23
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-23. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCL/N-23 since the card authentication certificate is revoked. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.7.23 Test Case 7.23: Test Case Deleted

4.7.24 Test Case 7.24: Test Case Deleted

4.7.25 Test Case 7.25: Test Case Deleted

4.8 Functional Test Suite 8: Picture Verification Using Signed CHUID (Mode #5)

This test method shall be executed for all products that support the TWIC NEXGEN Picture Verification Using Signed CHUID Verification mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.
Note: TWIC Legacy cards do not have such mode.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCN-01, TCN-02, TCN-05,TCN-09, TCN-10,TCN-11, TCN-12, TCN-13, TCN-14, TCN-17, TCN-21, TCN-23, TCN-25, TCN-26, TCN-27, TCN-28 for NEXGEN tests

Configuration of Reader Unit under Test

Prior to executing any of the test methods that apply to the Picture Verification Using Signed CHUID Verification mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Picture Verification Using Signed CHUID Verification mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the source of the TPK. ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Connect the interface of the product to the PACS (if supported). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.8.1 Test Case 8.1: Picture Verification Using Signed CHUID Verification - Normal Operation

Direct Requirement(s):	G.01, G.07, M5.1, M5.5
Test Description:	This test is used to determine if the product supports Picture Verification Using Signed CHUID Verification mode.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-01
Test Process:	1. Perform a Picture Verification following procedures described in the reader's documentation using TCN-01. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Verification attempt using TCN-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCN-01 (if supported).

4.8.2 Test Case 8.2: Picture Verification Using Signed CHUID Verification – FASC-N Check

Direct Requirement(s):	M5.2, M5.4, G.28
Test Description:	This test is used to determine if the product checks that the FASC-N from the signed CHUID matches that in the Picture.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and/or contactless interface testing.
Test Card(s):	TCN-02
Test Process:	1. Perform a Picture verification following procedures described in the reader's documentation using TCN-02. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Authentication shall fail for TCN-02 because the FASC-N in the signed CHUID doesn't match that in the Picture. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.3 Test Case 8.3: Picture Verification Using Signed CHUID Verification – Invalid CHUID Signature

Direct Requirement(s):	M5.3, M5.2
Test Description:	This test is used to determine if the product is able to verify the signature of the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-04
Test Process:	1. Perform a picture verification following procedures described in the reader's documentation using TCN-04. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-04 since the signature on the signed CHUID is broken/invalid. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.4 Test Case 8.4: Picture Verification Using Signed CHUID Verification – Trust Anchor Verification

Direct Requirement(s):	G.20, M5.3, M5.2
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the CHUID object signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-05
Test Process:	1. Perform a Picture verification following procedures described in the reader's documentation using TCN-05. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-05 since a trusted path cannot be built for the CHUID signer. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.5 Test Case 8.5: Picture Verification Using Signed CHUID Verification – Expiration Date Check

Direct Requirement(s):	M1.05, M5.2, P.4, P.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the signed CHUID.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-06
Test Process:	1. Perform a picture verification following procedures described in the reader's documentation using TCN-06. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-06 since the signed CHUID is expired. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.6 Test Case 8.6: Picture Verification Using Signed CHUID Verification – TPK Check

Direct Requirement(s):	G.30, FO.6, G.37
Test Description:	This test is used to determine if the product is able to decrypt the encrypted Picture using the TPK from the TWIC Card
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-12
Test Process:	1. Perform a Picture Verification following procedures described in the reader's documentation using TCN-12. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-12 since the TPK is incorrect. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.7 Test Case 8.7: Picture Verification Using Signed CHUID Verification – Picture Signature Verification

Direct Requirement(s):	G.20, M5.4
Test Description:	This test is used to determine if the product is able capable of verifying the signature on the Picture data object.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-13
Test Process:	1. Perform a Picture Verification following procedures described in the reader's documentation using TCN-13. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-13 since the Picture signature is broken/invalid. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.8 Test Case 8.8: Picture Verification Using Signed CHUID Verification – Picture Signer Check

Direct Requirement(s):	M5.2, M5.3
Test Description:	This test is used to determine if the product is able capable of verifying whether the Picture signer is authorized.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-14
Test Process:	1. Perform Picture Verification following procedures described in the reader's documentation using TCN-14. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture verification shall fail for TCN-14 since the picture signer was not authorized. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.9 Test Case 8.9: Picture Verification Using Signed CHUID Verification – FASC-N Match

Direct Requirement(s):	M5.2, M5.4
Test Description:	This test is used to determine if the product uses the FASC-N from the Signed CHUID and the Picture.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-15
Test Process:	1. Perform a Picture verification following procedures described in the reader's documentation using TCN-15. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Verification attempt using TCN-15 concludes successfully. The FASC-N logged should correspond to the values recorded for the FASC-N in the signed CHUID of TCN-15 (if supported).

4.8.10 Test Case 8.10: Picture Verification Using Signed CHUID Verification – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03, M5.2
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-26
Test Process:	1. Perform a picture verification following procedures described in the reader's documentation using TCN-26. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture verification shall fail for TCN-26 since the CHUID content signing certificate has an invalid signature. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.11 Test Case 8.11: Picture Verification Using Signed CHUID Verification – Subordinate CA Certificate Signature Verification

Direct Requirement(s):	G.20, M1.03, M5.2
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-28
Test Process:	1. Perform a Picture verification following procedures described in the reader's documentation using TCN-28. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Authentication shall fail for TCN-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.8.12 Test Case 8.12: Picture Verification Using Signed CHUID Verification – Canceled Card List Check

Direct Requirement(s):	M1.06, P.1, FO.7, M5.7
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification Using Signed CHUID Verification mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-21
Test Process:	1. Perform a Picture Verification following procedures described in the reader's documentation using TCN-21. 2. Observe the log generated to review the results. 3. Document the results from the verification attempt.
Expected Result:	Picture Verification shall fail for TCN-21 since the FASC-N is on the Canceled Card List. The log should report a transaction error code for the unsuccessful verification attempt (if supported).

4.9 Functional Test Suite 9: Picture Verification with Card Authentication (Mode 6)

This test method shall be executed for all products that support the Picture Verification with Card Authentication mode. Individual test cases within this test method shall be executed based on the applicability to the reader unit under test.
Note: TWIC Legacy cards do not have such mode.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCN-01, TCN-02, TCN-05, TCN-09, TCN-10, TCN-11, TCN-12, TCN-13, TCN-14, TCN-17, TCN-18, TCN-19, TCN-20, TCN-21, TCN-23, TCN-25, TCN-26, TCN-27, TCN-28 for NEXGEN tests

Configuration for Reader Unit under Test
Prior to executing any of the test methods that apply to the Picture Verification with Card Authentication mode, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in the Picture Verification with Card Authentication mode. ▪ Configure the interface type to be used (if necessary) ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the source of the TPK. ▪ Configure the product's logging capabilities (if required) ▪ Configure the product to download and use a TWIC Canceled Card List (either from a website or a file location). ▪ Ensure the product has network connectivity and the capability to download CRLs. Configure the CRL Test File (if required or applicable). ▪ After configuring all applicable options within the reader unit under test, remove the power without performing a formal shutdown. Then, reapply the power and verify that the configuration has not changed. ▪ Commence execution of the applicable test cases within the relevant test method.

4.9.1 Test Case 9.1: Picture Verification with Card Authentication - Normal Operation

Direct Requirement(s):	G.01, G.07, M2.2, M6.1, M6.5
Test Description:	This test is used to determine if the product supports the Picture Verification with Card Authentication mode.
Test Applicability:	▪ Applies if the Reader supports Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-01. 2. The picture of the cardholder should be displayed on a screen. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCN-01 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCN-01 (if supported).

4.9.2 Test Case 9.2: Picture Verification with Card Authentication – FASC-N Check

Direct Requirement(s):	M2.2, M6.4, G.28
Test Description:	This test is used to determine if the product checks that the FASC-N from card authentication certificate matches that in the Picture.
Test Applicability:	▪ Applies if the Reader supports Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-02
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-02. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-02 because the FASC-N in the card authentication certificate doesn't match that in the Picture. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.3 Test Case 9.3: Picture Verification with Card Authentication - Trust Anchor Verification I

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the CHUID signer's certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Picture Verification with Card Authentication mode ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-05
Test Process:	1. Perform a picture verification following procedures described in the reader's documentation using TCN-05. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-05 since a trusted path cannot be built for the CHUID object signer. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.4 Test Case 9.4: Picture Verification with Card Authentication - Trust Anchor Verification II

Direct Requirement(s):	G.20, M2.2, M2.3
Test Description:	This test is used to determine if the product is able to verify if the Certificate Authority (CA) is trusted for issuance of TWIC Cards by performing path validation on the card authentication certificate back to a trusted TWIC root.
Test Applicability:	▪ Applies if the Reader supports Picture Verification with Card Authentication mode ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-10
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-10. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-10 since a trusted path cannot be built for the card authentication certificate. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.5 Test Case 9.5: Picture Verification with Card Authentication – Challenge Response

Direct Requirement(s):	M2.2, M2.6, M6.8
Test Description:	This test is used to determine if the product is able to perform an asymmetric card authentication private key and certificate operation, such as general authenticate on a challenge of at least 127 bytes of unique data when performing Picture Verification with Card Authentication.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-09
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-09. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-09 because the private and public keys of the card authentication certificate are not part of a pair. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.6 Test Case 9.6: Picture Verification with Card Authentication – Expiration Date Check

Requirement(s):	M2.2, M2.4, P.4, P.6, M6.6
Test Description:	This test is used to determine if the product is able to perform expiration date check on the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-11
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-11. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-11 since the card authentication certificate is expired. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.7 Test Case 9.7: Picture Verification with Card Authentication – TPK Check

Direct Requirement(s):	M2.2, G.30, FO.6, G.37
Test Description:	This test is used to determine if the product is able to decrypt the encrypted Picture using the TPK from the TWIC Card
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-12
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-12. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-12 since the TPK is incorrect. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.8 Test Case 9.8: Picture Verification with Card Authentication – Picture Signature Verification

Direct Requirement(s):	M2.2, M6.3
Test Description:	This test is used to determine if the product is able capable of verifying the signature on the Picture.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-13
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-13. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-13 since the Picture signature is broken/invalid. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.9 Test Case 9.9: Picture Verification with Card Authentication – Picture Signer Check

Direct Requirement(s):	M2.2, M6.2
Test Description:	This test is used to determine if the product is able capable of verifying whether the Picture signer is an authorized issuer.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-14
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-14. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-14 since the Picture signer was not authorized. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.10 Test Case 9.10: Picture Verification with Card Authentication – FASC-N Match

Direct Requirement(s):	M6.4
Test Description:	This test is used to determine if the product uses the FASC-N from the card authentication certificate and the Picture.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-17
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-17. 2. Picture of the cardholder should be displayed on a screen. 3. Observe the log generated to review the results. 4. Document the results from the authentication attempt.
Expected Result:	Authentication attempt using TCN-17 concludes successfully. The FASC-N logged should correspond to the FASC-N value recorded for TCN-17 (if supported).

4.9.11 Test Case 9.11: Picture Verification with Card Authentication – Card Authentication Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3, M6.7
Test Description:	This test is used to determine if the product verifies the signature of the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-25
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCN-25. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-25 since the card authentication certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.12 Test Case 9.12: Picture Verification with Card Authentication – Content Signing Certificate Signature Verification

Direct Requirement(s):	G.20, M2.2, M2.3, M6.7
Test Description:	This test is used to determine if the product verifies the signature of the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-26
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-26. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-26 since the CHUID content signing certificate has an invalid signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.13 Test Case 9.13: Picture Verification with Card Authentication – Subordinate CA Certificate Signature Verification I

Direct Requirement(s):	G.20, M2.2, M2.3, M6.7
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the card authentication certificate.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-27
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-27. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-27 since the card authentication certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.14 Test Case 9.14: Picture Verification with Card Authentication – Subordinate CA Certificate Signature Verification II

Direct Requirement(s):	G.20, M2.2, M2.3, M6.7
Test Description:	This test is used to determine if the product verifies the signature of the subordinate CA certificate for the CA key used to sign the content signing certificate.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-28
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-28. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-28 since the CHUID content signing certificate is signed by a CA key with an invalid CA certificate signature. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.15 Test Case 9.15: Picture Verification with Card Authentication – Canceled Card List Check

Direct Requirement(s):	M2.7, P.1, FO.7
Test Description:	This test is used to determine if the product is able to check if a TWIC Card is on a Canceled Card List.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-21
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-21. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-21 since the FASC-N is on the Canceled Card List. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.9.16 Test Case 9.16: Picture Verification with Card Authentication – CRL Check

Direct Requirement(s):	M2.2, PO.1, FO.8
Test Description:	This test is used to determine if the product is able to check the card authentication certificate's status against a CRL.
Test Applicability:	▪ Applies if the Reader supports the Picture Verification with Card Authentication mode. ▪ Applies to both contact and contactless interface testing.
Test Card(s):	TCN-23
Test Process:	1. Perform an authentication (Mode 2) following procedures described in the reader's documentation using TCN-23. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication shall fail for TCN-23 since the card authentication certificate is revoked. The log should report a transaction error code for the unsuccessful authentication attempt (if supported).

4.10 Protocol Test Suite 1: TWIC Protocol Tests

The following tests are independent of the Authentication mode(s) supported by the Reader. These test cases shall be executed for the Reader unit under test, as applicable.

Applicable Test Cards

The following test cards apply to this test method and its related test cases.

Test Card(s):	TCL-01, PRL-01, TCL-38 for Legacy. TCN-01 & PRN-01 for NEXGEN

Configuration for Reader Unit under Test

Prior to executing any of the test methods that apply to the TWIC Protocol Tests, the reader unit under test shall be configured as stated below:

Test Preparation and Reader Configuration Steps:	▪ Configure the product to operate in any one of the supported Authentication Modes ▪ Configure the interface type to be used (if necessary) ▪ Configure the product to use the appropriate output format under the current configuration of the unit under test ▪ Configure the Root Certification Authority (CA) and any subordinate CAs within the product. ▪ Configure the time on the product (if supported) ▪ Configure the product's logging capabilities (if required) ▪ Commence execution of the applicable test cases within the relevant test method.

4.10.1 Test Case 10.1: Multiple TWIC Card Detection

Direct Requirement(s):	CL.03
Test Description:	This test is used to determine if the product rejects all of the presented cards, if two or more contactless smart cards are presented at the same time in a reader's contactless field.
Test Applicability:	▪ Applies to contactless interface testing only
Test Card(s):	TCL/N-01 and PRL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01 and PRL/N-01 simultaneously. 2. Observe the log generated to review the results. 3. Document the results from the authentication attempt.
Expected Result:	Authentication fails for both TCL/N-01 and PRL/N-01 since the product rejects 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. No log record is required for such case.

4.10.2 Test Case 10.2: Card Removal from RF Field

Direct Requirement(s):	CL.04
Test Description:	This test is used to determine if the product requires that a TWIC card, once read, is removed from the RF field for at least one second before attempting to read any new contactless card.
Test Applicability:	▪ Applies to contactless interface testing only
Test Card(s):	TCL/N-01 and PRL/N-01
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL/N-01 2. After removing TCL/N-01 from the RF field of the reader, waiting one or more seconds, present PRL/N-01 and perform an authentication using that card. 3. Observe the log generated to review the results. 4. Record results from the authentication attempts. 5. After a successful authentication of PRL/N-01, remove it from the RF field, then present the TCL/N-01 card quickly (in less than one second), in an attempt to perform an authentication with TCL/N-01 6. Observe the log generated to review the results 7. Record results from the authentication attempts.
Expected Result:	Authentication succeeds for TCL/N-01 and PRL/N-01 if a delay of at least one second is observed. The FASC-N recorded in the log should correspond to the values recorded for TCL/N-01 and PRL/N-01 (if supported). The difference in time between authenticating TCL/N-01 and PRL/N-01 must be greater than 1 second.

4.10.3 Test Case 10.3: Normal Operation in Legacy Mode with TWIC NEXGEN Card Used in Backward Compatibility Mode

Direct Requirement(s):	G.39
Test Description:	This test is used to determine if the product is able to work with TWIC Cards having a different minor release version (e.g. NEXGEN cards). As TWIC NEXGEN cards are all using SHA-256 this test also verifies the ability for the reader to work with this version of the hash algorithm.
Test Applicability:	▪ Applies to contact and contactless ▪ Test with at least one mode to verify the card is accepted and works correctly.
Test Card(s):	TCL-38
Test Process:	1. Perform an authentication following procedures described in the reader's documentation using TCL-38 2. Observe the log generated to review the results.

	3. Record results from the authentication attempts.
Expected Result:	Authentication succeeds for TCL-38. The FASC-N recorded in the log should correspond to the value recorded for TCL-01.

Note: This test is not done with TWIC readers able (or claiming) to work with TWIC NEXGEN cards full version

4.10.4 Test Case 10.4: Use of the SHA-128 algorithm to make sure old TWIC Legacy cards will be accepted.

Direct Requirement(s):	G.39
Test Description:	This test is used to make sure the product is able to work with older TWIC in the filed which were using the SHA-128 algorithm This card is similar to the reference test card TCL-01 in terms of content.
Test Applicability:	▪ Applies to contact and contactless ▪ Test with at least one mode to verify the card is accepted and works correctly.
Test Card(s):	TCL-39
Test Process:	4. Perform an authentication mode following procedures described in the reader's documentation using TCL-39 5. Observe the log generated to review the results. 6. Record results from the authentication attempts.
Expected Result:	Authentication succeeds for TCL-39. The FASC-N recorded in the log should correspond to the value recorded for TCL-01.

5 Test Equipment

The test equipment is provided by the reader manufacturer and may vary. The TWIC cards used in the different test cases are provided by the TSA TWIC office.

5.1 Test Card Configurations

The list below identifies the baseline for all test TWIC Cards. Unless explicitly mentioned in the table below, all test cards comply with the requirements of PIV and TWIC as per their respective specifications. These include, but are not limited to:

1. The PIV Application is the default application on some of the TWIC Legacy Card. In TWIC NEXGEN, no application is selected by default. So, in all tests, it is required to do an explicit selection of the TWIC (or PIV) Card application to work with the card,
2. All data objects are formatted per the specification using BER-TLV formatting identified in SP 800-73-2, Part 1,
3. All data objects in the TWIC Legacy test cards PIV application are conformant to FIPS 201 and its support special publications,
4. All data objects on the TWIC application are conformant to the TWIC card specification,
5. In TWIC Legacy cards, the FASC-Ns are consistent within all data objects for the TWIC and PIV Application individually. More specifically, the FASC-Ns on the TWIC application are consistent for all TWIC data objects and the FASC-Ns on the PIV application are consistent for all PIV data objects unless mentioned explicitly.
6. Cryptographic key sizes and algorithms are per the specifications and within the timelines for use.
7. In TWIC Legacy, All PIV certificates are valid[5], and Signatures on objects and hashes within the security object are valid.
8. For TWIC NEXGEN test cards used for NEXGEN reader certification, the PIV card application is present but none of the data objects are populated. So, such cards cannot be used to test TWIC readers working in backward compatibility mode
9. All TWIC Legacy test cards will have the FASC-N starting by 7099-7099-xxxx or 7099-8038-xxxx
10. All TWIC NEXGEN test cards will have the FASC-N starting by 7099-7199-xxxx or 7099-8138-xxxx
11. In case reader manufacturers want to use the TPK from the PDF 417 for TWIC Legacy, the set of TWIC Legacy test cards will come with a printed PDF 417 structured according to the TWIC NEXEGN Specification part 2 (section 4.9).

[5] Valid implies that it is not expired or revoked and is within the time period for use.

5.1.1 TWIC Legacy Test Card Configurations

The following table represents the TWIC Legacy 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
01	TCL-01		Within the FASC-N, the Individual Credential Issue (ICI) = 1.
02	TCL-02	FASC-N in the Card Authentication certificate is different from all other instances of the FASC-N on the TWIC and PIV Applications.	FASC-N in the unsigned CHUID different from all other instances of the FASC-N on the TWIC Application. FASC-N in the signed CHUID different from all other instances of the FASC-N on the TWIC Application. FASC-N in the TWIC Application different from the FASC-N in the Card Authentication Certificate in the PIV 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.
03	TCL-03		Expired Unsigned CHUID.
04	TCL-04	PIV CHUID Trust anchor must be correct for test 3.2.3 to be meaningful.	CHUID Signature invalid/corrupted.
05	TCL-05	PIV CHUID Trust anchor must be correct for test 3.2.4 to be meaningful.	Un-trusted content signing certificate in CHUID.
06	TCL-06	PIV CHUID must not be expired for test 3.2.5 to be meaningful.	Expired CHUID.
07	TCL-07	Security Data Object on PIV Card application must be correct.	Security Object signature invalid/corrupted.
08	TCL-08		Card not used in tests anymore.
09	TCL-09	The private key doesn't match the public key present in the card authentication certificate.	

Card #	Card Identifier	PIV Application Details	TWIC Application Details
10	TCL-10	Card auth cert signed by un-trusted CA.	
11	TCL-11	An EXPIRED Card Authentication Certificate.	
12	TCL-12		TPK stored on the TWIC Card is incorrect.
13	TCL-13		Signature on the fingerprint biometric container is invalid.
14	TCL-14	Data Object signing certificates must have the correct OID.	Data Object signing certificate does not have the content signing OID.
15	TCL-15		FASC-Ns in the signed CHUID and the biometrics are the same but are different than all other FASC-Ns.
16	TCL-16		FASC-Ns in the unsigned CHUID and the biometrics are the same but are different than all other FASC-Ns.
17	TCL-17	FASC-N in the card authentication certificate is the same as the FASC-N in the biometric and the CHUID. All other FASC-Ns are identical but different than the card authentication certificate FASC-N.	FASC-N in the biometric is the same as the FASC-N in the card authentication certificate and the CHUID. All other FASC-Ns are identical but different than the biometric FASC-N.
18	TCL-18		Number of minutiae in fingerprint biometric = 0. The fingerprint record does not contain Biometric Data Block (BDB).
19	TCL-19		Number of finger views in BDB is zero.
20	TCL-20		Number of finger views in fingerprint biometric = 1.
21	TCL-21		FASC-N on Test Canceled Card List.
22	TC-22	Not used anymore	
23	TCL-23	A REVOKED Card Authentication Certificate.	
24	TCL-24	FASC-N on the card authentication certificate different than that on the TWIC Application and on the Canceled Card List.	
25	TCL-25	Card Authentication certificate is signed by trusted CA but has invalid signature.	

Card #	Card Identifier	PIV Application Details	TWIC Application Details
26	TCL-26		CHUID content signing certificate has an invalid signature but it chains to a trusted root.
27	TCL-27	Card Authentication certificate is signed by a subordinate CA (that chains to trusted root) with an invalid CA certificate signature.	
28	TCL-28		CHUID content signing certificate is signed by a subordinate CA (that chains to a trust root) with an invalid CA certificate signature.
29	TC-29	Not used anymore	
30	TC-30	Not used anymore	
31	TC-31	Not used anymore	
32	TC-32	Not used anymore	
33	TC-33	Not used anymore	
34	TC-34	Not used anymore	
35	TC-35	Not used anymore	
36	TC-36	Not used anymore	
37	TC-37	Not used anymore	
38	TCL-38	New Card with same information as TCL-01 but on a V8 version	Card with the same information as TCL-01, but formatted as a TWIC NEXGEN AID and on a V8 chip
39	TCL-39	Card similar to TCL-01 but using the old SHA-128 algorithm	Card similar to TCL-01 but using the old SHA-128 algorithm

Table 4 - TWIC Legacy Test Card Details

5.1.2 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
01	TCN-01		Within the FASC-N, the Individual Credential Issue (ICI) = 1.
02	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.
03	TCN-03		Expired Unsigned CHUID.
04	TCN-04		CHUID Signature invalid/corrupted.
05	TCN-05		Un-trusted content signing certificate in CHUID.
06	TCN-06		Expired CHUID.
07	TCN-07		Security Object signature invalid/corrupted.
08	TC-08	not used anymore.	
09	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.

Card #	Card Identifier	PIV Application Details	TWIC Application Details
15	TCN-15		FASC-Ns in the signed CHUID, the biometrics and the Picture are the same but are different than all other FASC-Ns.
16	TCN-16		FASC-Ns in the unsigned CHUID, the biometrics and the picture are the same but are different than all other FASC-Ns.
17	TCN-17		FASC-N in the biometric and the picture is the same as the FASC-N in the card authentication certificate and the CHUID. All other FASC-Ns are identical but different than the biometric and Picture FASC-N.
18	TCN-18		Number of minutiae in fingerprint biometric = 0. The fingerprint record does not contain Biometric Data Block (BDB).
19	TCN-19		Number of finger views in BDB is zero.
20	TCN-20		Number of finger views in fingerprint biometric = 1.
21	TCN-21		FASC-N on Test Canceled Card List.
22	TC-22	Not used anymore	
23	TCN-23		A REVOKED Card Authentication Certificate.
24	TCN-24		FASC-N on the card authentication certificate different than that on the TWIC Application and on the Canceled Card List.
25	TCN-25		Card Authentication certificate is signed by trusted CA but has invalid signature.
26	TCN-26		CHUID content signing certificate has an invalid signature, but it chains to a trusted root.
27	TCN-27		Card Authentication certificate is signed by a subordinate CA (that chains to trusted root) with an invalid CA certificate signature.
28	TCN-28		CHUID content signing certificate is signed by a subordinate CA (that chains to a trust root) with an invalid CA certificate signature.

Table 5 - TWIC NEXGEN Test Card Details

5.2 PACS Registration Card Configurations

The list below identifies the baseline for all test PACS Registration Cards. All TWIC Legacy test cards comply with the requirements of PIV and TWIC as per their respective specifications. These include, but are not limited to:

1. In TWIC Legacy cards, the PIV Application is often the default application.
2. All data objects are formatted per the specification using BER-TLV formatting identified in SP 800-73-2, Part 1,
3. All data objects on the TWIC Legacy test cards in the PIV application are conformant to FIPS 201 and its support special publications,
4. All data objects in the TWIC application are conformant to the TWIC card specification,
5. For TWIC Legacy cards, the FASC-Ns are consistent within all data objects for the TWIC and PIV Application individually. More specifically, the FASC-Ns on the TWIC application are consistent for all TWIC data objects and the FASC-Ns on the PIV application are consistent for all PIV data objects.
6. Cryptographic key sizes and algorithms are per the specifications and within the timelines for use.
7. In TWIC Legacy test cards, all PIV certificates are valid[6], and Signatures on objects and hashes within the security object are valid.
8. In TWIC NEXGEN test cards, the PIV card application is present but none of the data objects are populated.

[6] Valid implies that it is not expired or revoked and is within the time period for use.

5.2.1 TWIC Legacy PACS Registration Card Configurations

Card #	Card Identifier	PIV Application Details	TWIC Application Details
01	PRL-01		FASC-N value of 7099-7099-001131-1-1-0000045831170992.
02	PRL-02		FASC-N value of 7099-7099-001132-1-1-0000045832170992.
03	PRL-03		FASC-N value of 7099-7099-001133-1-1-0000045833170992.
04	PRL-04		FASC-N value of 7099-7099-001134-1-1-0000045834170992.
05	PRL-05		FASC-N value of 7099-7099-001135-1-1-0000045835170992.
06	PRL-06		FASC-N value of 7099-7099-001136-1-1-0000045836170992.
07	PRL-07		FASC-N value of 7099-7099-001137-1-1-0000045837170992.
08	PR-08	Not used anymore	
09	PR-09	Not used anymore	
10	PRL-10		FASC-N value of 7099-9038-000003-1-1-0000405028170992.
11	PR-11	Not used anymore	
12	PR-12	Not used anymore	

Table 6 - Test PACS Registration Card Details for TWIC Legacy Tests

5.2.2 TWIC NEXGEN PACS Registration Card Configurations

Card #	Card Identifier	PIV Application Details	TWIC Application Details
01	PN-01		FASC-N value of 7099-7199-001131-1-1-0000045831170992.
02	PN-02		FASC-N value of 7099-7199-001132-1-1-0000045832170992.
03	PN-03		FASC-N value of 7099-7199-001133-1-1-0000045833170992.
04	PN-04		FASC-N value of 7099-7199-001134-1-1-0000045834170992.
05	PN-05		FASC-N value of 7099-7199-001135-1-1-0000045835170992.
06	PN-06		FASC-N value of 7099-7199-001136-1-1-0000045836170992.
07	PN-07		FASC-N value of 7099-7199-001137-1-1-0000045837170992.
08	PN-08	Not used anymore	
09	PN-09	Not used anymore	
10	PN-10		FASC-N value of 7099-9138-000003-1-1-0000405028170992.
11	PN-11	Not used anymore	
12	PN-12	Not used anymore	

Table 7 - Test PACS Registration Card Details for TWIC NEXGEN Tests