Provisionally-Approved Mobile Handheld Validation Reader Topology Mapping Form (MHVR 14.02)

VERSION 1.3.3 Rev B

FIPS 201 EVALUATION PROGRAM

November 3, 2017

FINAL

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
First draft	0.0.1	7/24/2014	Mapping for Mobile Handheld 14.01	Limited
Final	1.3.0	3/2/2015	Revised to synch with FRTC 1.3.0	Public
Final	1.3.3	9/8/2017	• Revised to synch with PACS FRTC v1.3.3. • Updated links to online normative references. • Added security classifications, severity level definitions, APL listing requirements. • Reactivated 12 previously deprecated test cases, clarified 16, added 58, and deprecated 14 test cases. • Biometric verification of cardholder is required at time of registration. • Security Object verification is mandatory at time of registration.	Public
Final	1.3.3 Rev A	9/18/2017	• Corrected typos. • Re-ordered and renumbered test certificate policy and interoperability test cases so that the same card can be used for multiple tests before switching to the next card. • Added one (1) missing certificate policy test case for PIV Authentication at time of access.	Public
Final	1.3.3 Rev B	11/3/2017	• Updated normative policy references for Federal Common Policy, FBCA, SSP, and PIV-I. • Updated Discovery Object tests to reflect that max retries of test cards are set to 10, not 5. • Added ICAM Test Card 54 (NFI PIV-I).	Public

Table of Contents

+

1 Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program and its FIPS 201 Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance.

2 Objectives

The FIPS 201 Evaluation Program mobile handheld evaluation process is designed to be agnostic to architecture, and focuses solely on functional testing using an end-to-end testing methodology. This document facilitates applicant mapping of the functional requirements identified in *Functional Requirements and Test Cases* [FRTC] to the categories identified in the FIPS 201 Evaluation Program's Mobile Handheld 14.02 topology.

3 Normative References

[BAA] Buy American Act Certification FAR 52.225-2
http://acquisition.gov/far/current/html/52_223_226.html

Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.27, June 29, 2017, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-common-policy.pdf

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0 March 26, 2014
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-in-epacs.pdf

[FBCA] FBCA X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), Version 2.31 June 29, 2017, or as amended
http://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA-Certificate-Policy-v2.31-06-29-17.pdf

[FIPS 201] Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases
http://idmanagement.gov/ficam-testing-program-documents

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

[M-05-24] Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

[M-06-18] Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-18.pdf

[M-11-11] OMB Memorandum M-11-11, February 3, 2011
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf

[PIV-I] CIO Council Personal Identity Verification Interoperability for Issuers, Version 2.0.1 July 27, 2017, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-i-for-issuers.pdf

[PROF] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program, Version 1.8 June 17, 2017, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-cert-profile-ssp.pdf

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads//FICAM_Roadmap_and_Implem_Guid.pdf

[Sect508] Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998
http://www.section508.gov/section508-laws

[SP800-73] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-4, Part 1-3, May 2015
http://dx.doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76-2, July 2013
http://dx.doi.org/10.6028/NIST.SP.800-76-2.pdf

[SP800-78] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-78-4, May 2015
http://dx.doi.org/10.6028/NIST.SP.800-78-4.pdf

[SP800-96] NIST SP 800-96, September 2006
http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[SP800-116] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://dx.doi.org/10.6028/NIST.SP.800-116

[SP800-153] NIST SP 800-153, February 2012
http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

[TAA] Trade Agreement Act Certification FAR 52.225-6
http://acquisition.gov/far/current/html/52_223_226.html

[UL 294] The Standard of Safety for Access Control System Units, UL Edition Number – 6, Date 05/10/2013, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_294_6

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1076_5

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number - 3, Date 10/29/2014, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1981_3

4 FIPS 201 Evaluation Program Defined Categories

The 14.02 Mobile Handheld Topology defines a handheld that combines the capability of the PACS Infrastructure and Validations System in a single handheld unit. This topology is defined as a handheld unit that works in an offline state disconnected from a PACS or Validation System. All information necessary to provide access to a cardholder is stored locally on the handheld device and is periodically updated from a central location. Note this category is defined as a single object that is procured as a single SKU. The following definitions define the objects that make up a functional element called a category:

1. ***Compatible*** components are proved to work with each other.
2. ***Interoperable*** components are tested to determine the set of like and related components with which it can reliably be operated in combinations. Interoperable components must use an industry standard (e.g., ISO, ANSI, IETF RFC) to enable standardized interfaces between components.
3. A ***subsystem*** is assembled of compatible components. Hence a subsystem would be tested and acquired as a unit or "configuration item". A subsystem may leverage an interoperable component external to the subsystem.
4. A ***category*** is made up of subsystems, compatible and/or interoperable components that meet functional requirements defined in [FRTC].

The one new category defined by this topology is the ***Mobile Handheld Validation Reader (MHVR)***. The topology requirements map with the existing APL categories ***Validation System*** and ***PACS Infrastructure,*** or the fully integrated ***PACS and Validation Infrastructure.*** This integrated topology of the MHVR with validation and PACS is described in the following sections.

4.1 Mobile Handheld Validation Reader (MHVR)

4.1.1 Mobile Handheld Functionality

A MHVR is a device that can be carried and used by personnel to confirm the validity and identity of a PIV cardholder. It is a Handheld Validation Reader and is an accepting device as defined in [E-PACS] that provides the human interface and the card interface. A MHVR may be a wholly-integrated unit, or it may be an assembly of components including:

1. Contact smart card reader;
2. Contactless smart card reader;
3. Display;
4. LED lights;
5. Audio announcers;
6. PIN pad;
7. Fingerprint sensor;
8. Other biometric modalities (e.g., iris);

9. Local storage for cached information received from the validation and PACS solution, and for storage of transaction and logging information; and
10. Secure communications for refreshing the local handheld cache (e.g., Wi-Fi, Cellular Data, Ethernet).

The MHVR is a fully offline unit, Validation information and optionally access control supporting information is cached from the trusted online source on a scheduled interval. Once cached, it operates independently for a limited period of time before becoming invalidated. It caches all access decisions and log information as needed. Once the device is returned from offline to online, all access decisions and log information is transmitted to the Centralized host.

The MHVR mobile handheld device performs functions to interact with the individual operating the device. This individual starts the MHVR application, uses their PIV/PIV-I credential to authenticate for operator/administrative access to the application and manages the transactions for individuals seeking access to a controlled area.

Under the control of the individual operating the MHVR, it interacts with the bearer of a PIV/PIV-I credential seeking access to a controlled area. All PKI and PACS access decisions are performed by the MHVR but does not necessarily actuate a physical locking mechanism, rather a grant or deny may be only a visual indication provided to the operator.

The MHVR must support a minimum of one FICAM authentication mode as defined in [E-PACS], but may also support multi-factor authentication.

4.1.1.1 MHVR operations

The MHVR must facilitate the ability to validate the card and identity of the cardholder locally. In order to achieve this requirement a method must be implemented to cache credential status information within the handheld. This may be done in many ways to achieve the functional requirements, but whatever method is used, it must ensure that any credential presented to the MHVR is valid at the time of use consistent with the information staleness requirements or otherwise indicate it is operating in a degraded assurance mode.

Cached PKI status information must be updated every 6 hours to ensure that a credential has not been placed on CRL by a CA. If cached information is older than 6 hours a visual indication must be provided to the operator warning them to connect and update the PKI status information. If not refreshed, the device may operate in a degraded mode until PKI status information is refreshed.

The MHVR, where not in communication electronically with the PACS, is first denoted as controlling access to a specific area. Authorization information for provisioned cardholders within that controlled area is cached in the handheld. Using the cached PKI and PACS authorization information the MHVR will verify the cardholder's access privileges and provide a visual "Go" or "No Go" indication to the operator. The operator then manually activates electronic locks, barriers, portals as required. Transactional data as a result of access decisions must be logged locally on the MHVR and uploaded to the host once communication has been reestablished.

4.1.2 Validation System

The Validation System acts as a centralized database that provides the necessary functions to collect the identity and card validation of the bearer of a credential. These methods, and the controls necessary to implement them, are defined fully in [E-PACS]. The Validation System must be able to collect all the necessary information to authenticate the bearer of a credential, store the information in a local database and send the information securely to the handheld. Typically, a Validation System is made up of several compatible and interoperable components that may include:

- SCVP server;
- OCSP responders;
- Caching status proxy server;
- PKI validation software; and
- PKI registration and management software.

The Validation System relies upon a registration engine that allows an administrator to register a cardholder's information and assign access control privileges. The Validation System database can run on its own physical, virtual, clustered server, or cloud-based solution. The Validation System database should be backed by an enterprise PKI validation solution that determines trust anchors and required constraints necessary to evaluate presented credentials. These enterprise validation solutions may include high-availability, consolidated OCSP responders or SCVP servers.

4.1.2.1 Validation Functionality

Validation System database functions provide the necessary information to the handheld to enable the MHVR to perform identification and authentication of the credential and the bearer of that credential locally at the MHVR according to various approved FICAM Authentication Methods. These methods and the controls necessary to implement them are defined fully in [E-PACS] and tested as an end-to-end system according to [FRTC]. Validation functions, as defined by the FIPS 201 Evaluation Program, have a direct impact on the MHVR. The interoperable components that may constitute or support the MHVR validation functionality include:

1. SCVP Servers/Clients;
2. OCSP responders; and
3. Full path discovery and validation software.

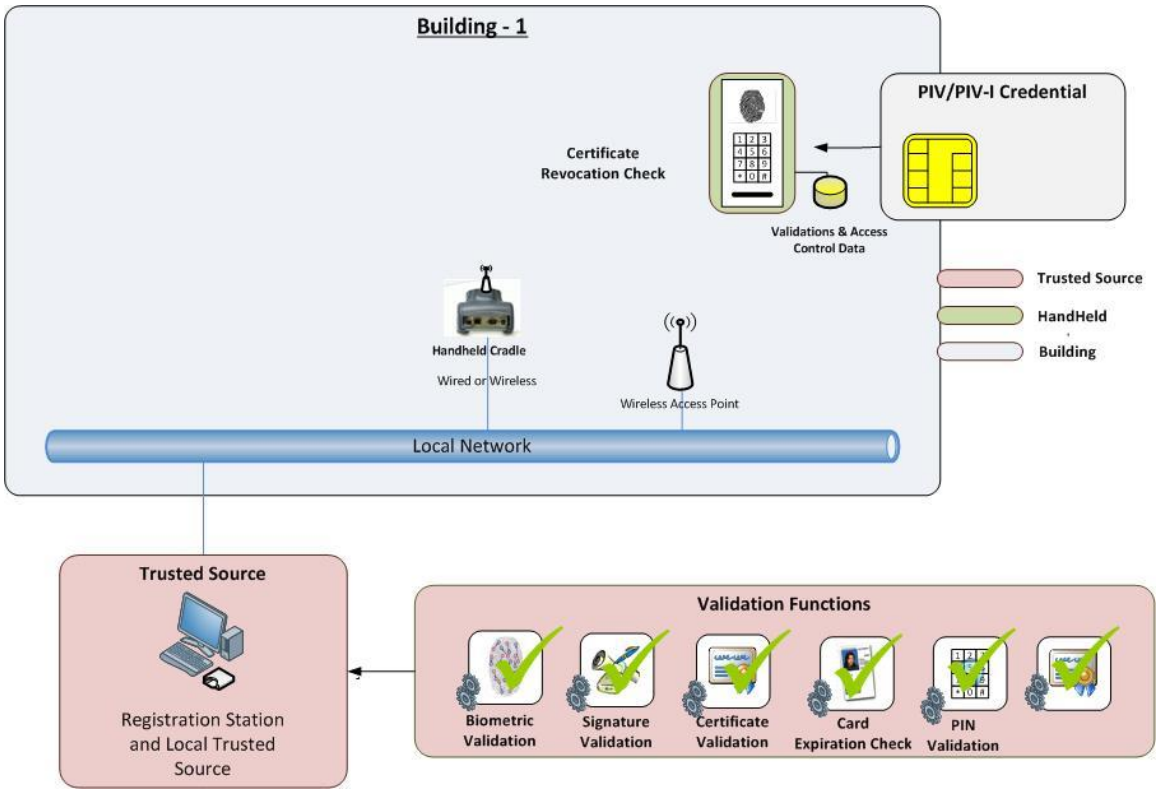
PKI validation functions are in integral part of the MHVR. As an example, a SCVP Client (and potentially server) may be part of the solution that generally resides in the same footprint as the MHVR.

4.2 Topology Diagrams

The Applicant must submit a topology diagram to the FIPS 201 Evaluation Program. The diagram must show the architectural linkage between the MHVR and the interoperable components that make up the end-to-end system. It must show which

components belong to a given category. The diagram facilitates an understanding of how a system is linked together and how it performs the functions required by [FRTC]. In other words, the diagram is a communications tool to enable the FIPS 201 Evaluation Program to understand how a given solution is put together to support end-to-end operational testing.

Figure 1 – Sample Topology diagram of MHVR



A complete topology diagram identifies every component that makes up an applicant's solution for the FIPS 201 Evaluation Program categories and provides the specific linkages (communications, internal messaging) that makes up the solution. As new topologies are adopted per [TAP], applicants must map their solution and its components into these new topologies.

4.3 APL Listing Requirements

Table 1 defines the APL listing requirements based on classification of the test case and its severity level. The program will not list a product that has a Severity 1 test case that failed (shown RED). ***Table 2*** specifies the remediation timeframes for each severity level.

Products not corrected within the given timeframe will be moved to the Removed Products List (RPL).

Table 1 - APL listing based on Test Level and Classification

Test Level / Classification	*Severity 1*	*Listed on APL*	*Severity 2*	*Listed on APL[1]*	*Severity 3*	*Listed on APL*
Security Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✗	Fail	✓
Security Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Security Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓
Usability Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Usability Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Usability Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓

Table 2 - Severity Remediation Timeframes

Severity Level	*Severity Description*	*Remediation Timeframe*
1	The identified problem results in a High impact to any of security, PACS operations, PACS availability, or other area examined.	30 days
2	The identified problem results in a Moderate impact to any of security, PACS	90 days

[1] No new solution that fails a test case labeled Security/Required Severity Level 2 (SR-2) will be listed on the APL. Existing solutions that initially passed a SR-2 test case, but in subsequent revisions fail a SR-2 test case, are subject to remediation within 90 days as specified in ***Table 2*** below.

Severity Level	*Severity Description*	*Remediation Timeframe*
	operations, PACS availability, or other area examined.	
3	The identified problem results in a Low impact to any of security, PACS operations, PACS availability, or other area examined.	1 year

a. Classification Codes and Scoring Guidelines

The Topology Mapping form includes a classification code for each test case. The classification code is shorthand that indicates the test type for the requirement is *Security* or *Usability* and whether the requirement is mandatory (*Required*) or *Optional*.

Table 3 - Classification Codes

Classification Code	*Security/Usability*
S[RO]-[123]	**Security** - A control directly impacting security of the system.
U[RO]-[123]	**Usability** - A control impacting end user system usability. Does not directly impact security.
[SU]R-[123]	**Required** - Must be present. Must work correctly: Red/Green.
[SU]O-[123]	**Optional** - May be present. If present, it must work correctly: Red/Green. Not Supported: Yellow.
Example: SR-2	**Security, Required, Severity Level 2**
Example: UO-3	**Usability, Optional, Severity Level 3**

5 Mapping

Mapping is the process of taking the functional requirements defined in [FRTC] and allocating them into the FIPS 201 Evaluation Program categories, and then indicating the specific components within your solution that perform the operations for that requirement. For example, if the requirement is for a product to validate signatures as defined in [FRTC] §2.1-Test 2.1.1, the Applicant should follow the example given in ***Table 4*** below.

Table 4 - Example Mapping Table for Time of Individual Registration Signature Verification

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
		2.0			**Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9**	**All tests use PKI-AUTH unless specifically noted.**	**Note all requirements sourced from [E-PACS] unless otherwise noted.**			`
		2.01			**Signature Verification**					
1.2.0	SR-1	2.01.01	01	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential	Registration succeeds.	PIA-2 thru PIA-7	Validation System (13.01), PACS Infrastructure (13.01), Mobile Handheld Validation Reader (14.02)	Registration Workstation, PACS application, Path Discovery and Validation engine, APL #10001, APL #10002.	EE certificate signature is validated immediately by the Validation System. The CA certificate signatures are evaluated, but may be cached by the path discovery and validation engine if they have been

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
										previously seen. The MHVR downloads the cached information on a periodic interval not to exceed 6 hours. If the hash of the cached certificate matches the computed hash of the card, the MHVR knows that the signature is valid.

In the example provided in ***Table 4***, the signature verification involves several elements. It is allocated to the PACS Infrastructure and Validation System, as both solutions require information from the credential. The PACS Infrastructure provides the registration workstation. The Validation System is doing the PKI signature verification for the end entity, and the Validation System's PDVAL engine is evaluating signatures and caching status for the CA certificate path. Clearly there are many potential combinations of components within categories that could perform this function and it is up to the applicant to describe the process of how, when, and where [FRTC] requirements are met.

If a MHVR is integrated with a PACS Infrastructure and/or Validation System in such a way that the MHVR relies solely on the host infrastructure for nonce generation, signature verification, PD-VAL, and access control decision-making, then the mapping table should include the categories of the components that meet the requirement, and should include the previously approved GSA APL number in the Components column. The Process column should include the details describing how the MHVR meets the requirement.

5.1 Topology Mapping

Table 5 contains a full topology mapping form. Working within this document has historically been difficult due to its size. Beginning with FRTC 1.3.3, we provide this artifact in the form of a Microsoft Excel workbook which allows you to hide columns as needed and maneuver more easily. You will find the Topology Mapping Workbook included in the evaluation application. Use it to provide the Lab with the PACS 14.02 topology mapping of functional requirements identified in the [FRTC] to the FIPS 201 Evaluation Program categories as defined in this document. The columns for Category(ies), Components and Process are intentionally left blank in this table. These three columns must be completed by the Applicant when submitting a component/solution to the FIPS 201 Evaluation Program for evaluation, testing, and approval.

For MHPR products, in addition to test cases 2.x.x through 7.x.x, the test cases numbered 8.x.x shall be addressed.

Table 5 - Topology Mapping for the Mobile Handheld Validation Reader 14.02 Topology – ***For reference only. Please use the FRTC 1.3.3 Topology Mapping Workbook for your Submission.***

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
		2.0			**Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9**	All tests use PKI-AUTH unless specifically noted.	Note all requirements sourced from [E-PACS] unless otherwise noted.				`
		2.01			Signature Verification						
1.2.0	SR-1	2.01.01	01	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Registration succeeds.	PIA-2 thru PIA-7	Active			
1.2.0	SR-1	2.01.02	02	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Registration succeeds.	PIA-2 thru PIA-7	Active			
1.2.0	SR-1	2.01.03	01	01	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.	Registration fails.	PIA-3.2, PIA-3.4, PIA-4, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	2.01.04	05	00	Verify product's ability to recognize invalid signature on the End Entity certificate (Invalid: Certificate Signature is Invalid).	Registration fails.	PIA-3.2, PIA-3.4, PIA-4	Active			
1.2.0	SR-1	2.01.05	23	00	Verify product's ability to recognize certificate/private key mismatch.	Registration fails.	PIA-3.2, PIA-3.4, PIA-4	Active			
		2.02			**Certificate Validity Periods**						
1.2.0	SR-3	2.02.01	01	02	Verify product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	Registration fails.	PIA-3.5, PIA-5	Active			
1.2.0	SR-1	2.02.02	10	00	Verify product's ability to reject a credential when *notAfter* date of the End Entity Signing CA is sometime in the past.	Registration fails.	PAI-3.2, PIA-3.4, PIA-4	Active			
1.2.0	SR-3	2.02.03	12	00	Verify product's ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future.	Registration fails.	PIA-3.5	Active			
1.2.0	SR-1	2.02.04	01	03	Verify product's ability to reject a credential when *notAfter* date of the intermediate certificate is sometime in the past.	Registration fails.	PIA-3.5, PIA-5	Active			
1.2.0	SR-1	2.02.05	13	00	Verify product's ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past.	Registration fails.	PIA-3.5	Active			
		2.03			**Name Chaining**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	2.03.01	01	04	Verify product's ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Registration fails.	PIA-3.2, PIA-5	Active			
		2.04			**Basic Constraints**						
1.2.0	SR-1	2.04.01	01	05	Verify product's ability to recognize when the intermediate CA certificate is missing *basicConstraints* extension.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	2.04.02	01	06	Verify product's ability to recognize when the *basicConstraints* extension is present and critical in the intermediate CA certificate but the *cA* component is false.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	2.04.03	01	07	Verify product's ability to recognize when the *basicConstraints* extension is present and not critical in the intermediate CA certificate but the *cA* component is false.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-1	2.04.04	01	08	Verify product's ability to recognize when the first certificate in the path includes *basicConstraints* extension with a *pathLenConstraint* of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	2.04.05	01	32	Verify product's ability to detect a mismatched SKID with the subject public key in the certificate.	Registration fails.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-3	2.04.06	01	33	Verify product's ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Registration fails.	PIA-3.2, PIA-5	Active			
		2.05			**Key Usage Verification**						
1.2.0	SR-1	2.05.01	01	09	Verify product's ability to recognize when the intermediate certificate includes a keyUsage extension in which *keyCertSign* is false.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	2.05.02	01	10	Verify product's ability to recognize when the intermediate certificate includes a non-critical *keyUsage* extension and rejects the path because a CA's *keyUsage* extension must always be marked critical.	Registration fails.	PIA-3.2, PIA-5, [PROF] Worksheet 3	Active			
1.2.0	SR-1	2.05.03	01	11	Verify product's ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *crlSign* is false.	Registration fails.	PIA-3.2, PIA-5	Active			
		2.06			**Certificate Policies**						
1.2.0	SR-1	2.06.01	Valid PIV	Common Policy Root	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for PIV Authentication Certificates will be set to *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.3.13) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	2.06.02	Valid PIV	Common Policy Root	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the PIV Authentication Certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-2	2.06.03	Valid PIV	CRCA Root	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to *id-fpki-certpcy-mediumHardware* (2.16.840.1.101.3.2.1.3.12) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	2.06.04	Valid PIV	CRCA Root	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-1	2.06.05	Valid PIV	Common Policy Root	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate such as *id-fpki-common-High* (2.16.840.1.101.3.2.1.3.16).	Registration fails.	PIA-3.2, PIA-5	Active			
1.2.0	SR-2	2.06.06	01	12	With required policy set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11), verify product's ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.	Registration fails.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	2.06.07	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.08	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-cardAuth* (2.16.840.1.101.3.2.1.48.13) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	2.06.09	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-common-piv-contentSignin*g (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.10	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 2.3.4.5).	Registration fails.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.11	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 3.4.5.6).	Registration fails.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	2.06.12	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-hardware* (2.16.840.1.101.3.2.1.48.78) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.13	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-cardAuth* 2.16.840.1.101.3.2.1.48.79) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.14	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-contentSigning* 2.16.840.1.101.3.2.1.48.80) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	2.06.15	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Authentication Certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Authentication certificate path (e.g., OID value 4.3.2.1).	Registration fails.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.16	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 5.4.3.2).	Registration fails.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	2.06.17	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 6.5.4.3).	Registration fails.	PIA-3.2, PIA-5	Active			
		2.07			**Generalized Time**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-3	2.07.01	01	24	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Registration succeeds.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	2.07.02	01	25	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Registration fails.	PIA-3.2, PIA-5	Active			
		2.08			**Name Constraints**						
1.2.0	SR-1	2.08.01	01	00	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.		PIA-3.2, PIA-5	Active			
1.2.0	SR-1	2.08.02	01	13	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.		PIA-3.2, PIA-5	Active			
		2.09			**Certificate Revocation Tests (CRL)**						
1.2.0	SR-1	2.09.01	01	15	The system recognizes when no revocation information is available for the End Entity certificate.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.02	01	16	The system recognizes when a second intermediate CA certificate is revoked.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.03	24	00	The system recognizes when the End Entity certificate is revoked (Invalid: Revoked Certificate).	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	2.09.04	01	18	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.05	01	19	The system recognizes when a certificate in the path points to a CRL with an expired nextUpdate value (an expired CRL).	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-3	2.09.06	01	20	The system recognizes when a certificate in the path points to a CRL with a *notBefore* Date in the future.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.07	01	21	The system recognizes when a certificate in the path has an incorrect CRL distribution point.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.08	01	17	The system recognizes when the CRL has an invalid signature.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-2	2.09.09	01	34	The system recognizes when an incorrectly formatted CRL is present in the path.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	2.09.10	01	36	The system recognizes when an invalid CRL signer is in the path.	Registration fails.	PIA-3.5, PIA-5, PIA-7	Active			
		2.10			**CHUID Verification**						
1.2.0	SR-1	2.10.01	04	00	The system recognizes when the CHUID signature is invalid and does not verify.	Registration fails.	PIA-3.2, PIA-4	Active			
1.2.0	SR-2	2.10.02	09	00	The system recognizes when the CHUID signer certificate is expired.	Registration fails.	PIA-3.6, PIA-5	Active			
1.2.0	SR-1	2.10.03	14	00	The system recognizes when the CHUID is expired.	Registration fails.	PIA-3.6	Active			
1.2.0	SR-2	2.10.04	15	00	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	2.10.05	19	00	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.3	Active			
1.2.0	SR-1	2.10.06	11	00	The system recognizes when the PKI-AUTH certificate expires after the CHUID expiration date.	Registration fails.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)	Active			
		2.11			**Facial Image Verification**						
1.2.0	SR-1	2.11.01	06	00	The system recognizes when the Facial Image signature is invalid and does not verify.	Registration fails.	PIA-3.2, PIA-4	Active			
1.3.3	SO-1	2.11.02	49	00	The system recognizes when the Facial Image CBEFF is expired.	Registration succeeds but system issues warning during registration.	[SP 800-76]	Active			
1.3.3	SO-3	2.11.03	50	00	The system recognizes when the Facial Image CBEFF will expire before the CHUID expiration date.	Registration succeeds but system issues warning during registration.	[SP 800-76]	Active			
		2.12			**Copied Containers**						
1.2.0	SR-1	2.12.01	16	00	The system recognizes when the FASC-N in the PKI-CAK certificate does not equal the FASC-N in the PIV Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
1.2.0	SR-1	2.12.02	20	00	The system recognizes when the UUID in the PKI-CAK certificate does not equal the UUID in the PIV-I Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
1.2.0	SR-1	2.12.03	17	00	The system recognizes when the FASC-N in the Facial Image does not equal the FASC-N in the PIV Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-3	2.12.04	21	00	The system recognizes when the UUID in the Facial Image does not equal the UUID in the PIV-I Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
		2.13			**Fingerprint Verification**						
1.2.0	SR-1	2.13.01	07	00	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
1.2.0	SR-1	2.13.03	Valid Credential	Common Policy Root	Verify Product's ability to accept a valid credential with a matching fingerprint.	Registration succeeds.	PIA-9	Active			
1.2.0	SR-1	2.13.04	Valid Credential	Common Policy Root	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	Registration fails.	PIA-9	Active			
1.2.0	SR-1	2.13.05	18	00	The system recognizes when the FASC-N in the Fingerprint does not equal the FASC-N in the PIV Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
1.2.0	SR-3	2.13.06	22	00	The system recognizes when the UUID in the Fingerprint does not equal the UUID in the PIV-I Auth Cert.	Registration fails.	PIA-3.2; [SP800-73], Part 1, §3.1.2	Active			
1.3.3	SO-1	2.13.07	51	00	The system recognizes when the Cardholder Fingerprints CBEFF is expired. This test case classification rises to SR-1 if access is denied at time of access when an expired biometric is encountered.	Registration fails.	[SP 800-76]	Active			
1.3.3	SO-3	2.13.08	52	00	The system recognizes when the Cardholder Fingerprints CBEFF will expire before the CHUID expiration date.	Registration succeeds but system issues warning during registration.	[SP 800-76]	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
		2.14			**Security Object Verification**		**PIA-3.2, PIA-5**				
1.2.0	SR-3	2.14.01	08	00	The system recognizes when the Security Object signature is invalid and does not verify.	Registration fails.	PIA-3.4, PIA-4, PIA-5	Active			
1.3.3	SR-2	2.14.02	38	00	The system recognizes when a hash value within the Security Object does not match its corresponding data group buffer.	Registration fails.	[SP800-73] Part 1	Active			
		2.15			**OCSP Response Checking**						
1.2.0	SR-1	2.15.01	01	00	The system successfully validates a good credential using an OCSP response with a good signature.	Registration succeeds.	PIA-3.2, PIA-3.5	Active			
1.2.0	SR-2	2.15.02	42	37	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Registration fails.	PIA-3.2, PIA-3.5, PIA-3.6	Active			
1.2.0	SR-3	2.15.03	43	38	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Registration succeeds.	PIA-3.2, PIA-3.5	Active			
1.2.0	SR-2	2.15.04	44	39	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Registration fails.	PIA-3.2, PIA-3.5, PIA-3.6	Active			
1.2.0	SR-1	2.15.05	45	40	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Registration fails.	PIA-3.2, PIA-4	Active			
		2.16			**Interoperability Testing**						
1.2.0	SR-1	2.16.01	Valid PIV	Common Policy Root	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.	Registration succeeds.	PIA-6	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	2.16.02	39	41	The system recognizes a Federally-issued PIV-I card with a FASC-N that does not begin with fourteen 9s.	Registration succeeds.	PIA-6	Active			
1.3.3	SR-1	2.16.03	02	00	The system recognizes a Federally-issued PIV-I card with a FASC-N that begins with fourteen 9s.	Registration succeeds.	PIA-6	Active			
1.3.3	SR-3	2.16.04	01	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID i*d-PIV-content-signing* (OID 2.16.840.1.101.3.6.7) is present in the content signing certificate.	Registration succeeds.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.05	01	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Registration fails.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.06	02	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID *id-fpki-pivi-content-signing* (OID 2.16.840.1.101.3.8.7) is present in the content signing certificate.	Registration succeeds.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.07	02	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Registration fails.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.08	01	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID i*d-PIV-cardAuth* (OID 2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Registration succeeds.	[FIPS 201]	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-3	2.16.09	01	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Registration fails.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.10	02	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID *id-PIV-cardAuth* (OID 2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Registration succeeds.	[FIPS 201]	Active			
1.3.3	SR-3	2.16.11	02	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Registration fails.	[FIPS 201]	Active			
1.3.3	SR-1	2.16.12	46	00	A FIPS 201-2 card can be registered using PKI-AUTH method.	Registration succeeds.	[FIPS 201]	Active			
1.3.3	SR-1	2.16.13	47	00	A FIPS 201-2 card can be registered using PKI-AUTH method with the pivFASC-N in the PIV Authentication and Card Authentication *SubjectAltName* extensions is encoded after the entryUUID.	Registration succeeds.	[FIPS 201]	Active			
1.3.3	SR-1	2.16.14	53	00	The system successfully handles cards with a slightly larger than recommended Card Authentication Certificate (2160 bytes).	Registration succeeds.	[[SP800-73]]	Active			
		2.17			**Cryptography Testing**						
1.2.0	SR-1	2.17.02	NIST #1	NIST Root	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	Registration succeeds.	[SP800-78] Table 3-1; [SP800-78] Table	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
							3-3; [Common] §6.1.5				
1.2.0	SO-3	2.17.05	NIST #2	NIST Root	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	Registration succeeds.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SR-1	2.17.07	NIST #4	NIST Root	Verify Product's ability to validate signatures using ECDSA (P-256).	Registration succeeds.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SO-3	2.17.08	NIST #5	NIST Root	Verify Product's ability to validate signatures using ECDSA (P-384).	Registration succeeds.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SR-1	2.17.10	NIST #1	NIST Root	Verify Product's ability to validate signatures using SHA-256.	Registration succeeds.	[SP800-78] Table 3-7; [Common] §6.1.5	Active			
1.2.0	SO-3	2.17.11	NIST #5	NIST Root	Verify Product's ability to validate signatures using SHA-384.	Registration succeeds.	[SP800-78] Table 3-7; [Common] §6.1.5	Active			
1.2.0	SR-1	2.17.12	NIST #1	NIST Root	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	Registration succeeds.	[SP800-78] Table 3-2	Active			
1.2.0	SR-3	2.17.14	01	35	Verify product's ability to validate signatures using RSA 4096 in the path.	Registration succeeds.	Derived from [SP800-78] Table 3-2	Active			
		2.18			**Discovery Object and PIN Usage Policy**						
1.3.0	SR-2	2.18.01	25	00	Discovery object not present. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). (E-PACS is using Application PIN).	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-2	2.18.02	25	00	Discovery object not present. Enter valid PIV Application PIN. Confirm PIV Application PIN retry counter is reset to 10. Confirm Global PIN retry counter remains at 9. (E-PACS is using the Application PIN).	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-1	2.18.03	26	00	Discovery object present and set for PIV Application PIN only. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). (E-PACS is using the Application PIN).	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-1	2.18.04	26	00	Discovery object is present and set for PIV Application PIN only. Enter valid PIV Application PIN. Confirm PIV Application PIN retry counter is reset to 10. (E-PACS is using the Application PIN).	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-1	2.18.05	27	00	Discovery object is present. PIV App and Global PINs are available. PIV Application PIN is primary. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). Confirm Global PIN retry counter remains at 10.	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-2	2.18.07	27	00	Discovery object is present. PIV Application and Global PINs are available. PIV Application PIN is primary. Enter valid PIV Application PIN. Confirm PIV Application and Global PINs are both 10. (E-PACS is using the Application PIN).	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-2	2.18.10	28	00	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Enter invalid Global PIN (e.g., 999999). Confirm PIV Application PIN retry counter remains at 10. Confirm Global PIN retry counter is decremented by one (9). (E-PACS is using the Global PIN).	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.3	SR-2	2.18.12	28	00	Discovery object is present. PIV Application and Global PINs are available. Global PIN is primary. Enter valid Global PIN. Confirm PIV Application and Global PINs are both 10. (E-PACS is using the Global PIN).	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
		4.0			**Requirements for Automated Provisioning In Accordance With [E-PACS] PIA-8**						
1.2.0	SO-2	4.01.01			The E-PACS shall accept automated provisioning from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Design analysis passes.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SO-2	4.01.02			The E-PACS shall accept automated deprovisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Design analysis passes.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94	Active			
		5.0			**Authentication at Time of Access Test Cases**						
		5.01			**Signature Verification**						
1.2.0	SR-1	5.01.01	01	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Access granted.	PIA-2 thru PIA-7	Active			
1.2.0	SO-1	5.01.02	02	00	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Access granted.	PIA-2 thru PIA-7	Active			
1.2.0	SR-1	5.01.03	01	01	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.	Access denied.	PAI-3.2, PIA-3.4, PIA-4, PIA-5	Active			
1.2.0	SR-1	5.01.04	05	00	Verify product's ability to recognize invalid signature on the End Entity certificate (Invalid: Certificate Signature is Invalid). This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	Access denied.	PAI-3.2, PIA-3.4, PIA-4	Active			
1.2.0	SR-1	5.01.05	23	00	Verify product's ability to recognize certificate/private key mismatch.	Access denied.	PAI-3.2, PIA-3.4, PIA-4	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	5.01.06	41	00	Verify product's ability to recognize public key from card does not match public key previously registered to the system. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access. .	Access denied.	PIA-3.2	Active			
		5.02			**Certificate Validity Periods**						
1.2.0	SR-3	5.02.01	01	02	Verify product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	Access denied.	PIA-3.5, PIA-5	Active			
1.2.0	SR-2	5.02.02	12	00	Verify product's ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	Access denied.	PIA-3.5	Active			
1.2.0	SR-1	5.02.03	01	03	Verify product's ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past.	Access denied.	PIA-3.5, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	5.02.04	13	00	Verify product's ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past. This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access.	Access denied.	PIA-3.5	Active			
1.2.0	SR-1	5.02.05	10	00	Verify product's ability to reject a credential when *notAfterDate* of the End Entity Signing CA is sometime in the past.	Access denied.	PAI-3.2, PIA-3.4, PIA-4	Active			
		5.03			**Name Chaining**						
1.2.0	SR-1	5.03.01	01	04	Verify product's' ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Access denied.	PIA-3.2, PIA-5	Active			
		5.04			**Basic Constraints**						
1.2.0	SR-1	5.04.01	01	05	Verify product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.04.02	01	06	Verify product's ability to recognize when the *basicConstraints* extension is present and critical in the intermediate CA certificate but the *cA* component is false.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.04.03	01	07	Verify product's ability to recognize when the *basicConstraints* extension is present and not critical in the intermediate CA certificate but the *cA* component is false.	Access denied.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	5.04.04	01	08	Verify product's ability to recognize when the first certificate in the path includes *basicConstraints* extension with a *pathLenConstraint* of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.04.05	01	32	Verify product's ability to detect a mismatched SKID with the subject public key in the certificate.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.04.06	01	33	Verify product's ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Access denied.	PIA-3.2, PIA-5	Active			
		5.05			**Key Usage Verification**						
1.2.0	SR-1	5.05.01	01	09	Verify product's ability to recognize when the intermediate certificate includes a keyUsage extension in which *keyCertSign* is false.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.05.02	01	10	Verify product's ability to recognize when the intermediate certificate includes a non-critical *keyUsage* extension and rejects the path because a CA's *keyUsag*e extension must always be marked critical.	Access denied.	PIA-3.2, PIA-5, [PROF] Worksheet 3	Active			
1.2.0	SR-1	5.05.03	01	11	Verify product's ability to recognize when the intermediate certificate includes a *keyUsage* extension in which *crlSign* is false.	Access denied.	PIA-3.2, PIA-5	Active			
		5.06			**Certificate Policies**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	5.06.01	Valid PIV	Common Policy Root	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the PIV Authentication certificate path. The explicit policy will be set to *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.3.13) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			
1.2.0	SR-1	5.06.02	Valid PIV	Common Policy Root	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the PIV Authentication certificate path (e.g., OID value 1.2.3.4).	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-2	5.06.03	Valid PIV	CRCA Root	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to *id-fpki-certpcy-mediumHardware* (2.16.840.1.101.3.2.1.3.12) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	5.06.04	Valid PIV	CRCA Root	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-1	5.06.05	Valid PIV	Common Policy Root	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate such as *id-fpki-common-High* (2.16.840.1.101.3.2.1.3.16).	Access denied.	PIA-3.2, PIA-5	Active			
1.2.0	SR-2	5.06.06	01	12	With required policy set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11), verify product's ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.	Access denied.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	5.06.07	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.08	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-cardAuth* (2.16.840.1.101.3.2.1.48.13) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	5.06.09	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-common-piv-contentSignin*g (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.10	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 2.3.4.5).	Access denied.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.11	01	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 3.4.5.6).	Access denied.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	5.06.12	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-hardware* (2.16.840.1.101.3.2.1.48.78) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.13	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-cardAuth* 2.16.840.1.101.3.2.1.48.79) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.14	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-certpcy-pivi-contentSigning* 2.16.840.1.101.3.2.1.48.80) by the relying party solution.	Access granted.	PIA-3.2, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	5.06.15	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Authentication Certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Authentication certificate path (e.g., OID value 4.3.2.1).	Access denied.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.16	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 5.4.3.2).	Access denied.	PIA-3.2, PIA-5	Active			
1.3.3	SR-1	5.06.17	02	00	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 6.5.4.3).	Access denied.	PIA-3.2, PIA-5	Active			
		5.07			**Generalized Time**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-3	5.07.01	01	24	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Access granted.	PIA-3.2, PIA-5	Active			
1.2.0	SR-3	5.07.02	01	25	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Access denied.	PIA-3.2, PIA-5	Active			
		5.08			**Name Constraints**						
1.2.0	SR-1	5.08.01	01	00	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.		PIA-3.2, PIA-5	Active			
1.2.0	SR-1	5.08.02	01	13	The system recognizes when the intermediate certificate includes a *nameConstraints* extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.		PIA-3.2, PIA-5	Active			
		5.09			**Certificate Revocation Tests (CRL)**						
1.2.0	SR-1	5.09.01	01	15	The system recognizes when no revocation information is available for the End Entity certificate.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.02	01	16	The system recognizes when a second intermediate CA certificate is revoked.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.03	24	00	The system recognizes when the End Entity certificate is revoked (Invalid: Revoked Certificate).	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.04	01	17	The system recognizes when the CRL has an invalid signature.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	5.09.05	01	18	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.06	01	19	The system recognizes when a certificate in the path has an expired nextUpdate value (an expired CRL).	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-3	5.09.07	01	20	The system recognizes when a certificate in the path points to a CRL with a *notBefore* date in the future.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.08	01	21	The system recognizes when a certificate in the path has an incorrect CRL distribution point.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.09	01	34	The system recognizes when an incorrectly formatted CRL is present in the path.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
1.2.0	SR-1	5.09.10	01	36	The system recognizes when an invalid CRL signer is in the path.	Access denied.	PIA-3.5, PIA-5, PIA-7	Active			
		5.11			**Facial Image Verification**						
1.2.0	UO-3	5.11.01	06	00	The system recognizes when the Facial Image signature is invalid and does not verify.	Access denied.	PIA-3, PIA-3.2, PIA-3.3, PIA-4	Active			
		5.12			**Fingerprint Verification**						
1.2.0	SR-1	5.12.01	07	00	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Access denied.	PIA-3, PIA-3.2, PIA-3.3, PIA-4	Active			
1.2.0	SR-1	5.12.02	Valid Credential	Common Policy Root	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	Access denied.	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	5.12.03	Valid Credential	Common Policy Root	Verify Product's ability to accept a valid credential with a matching fingerprint.	Access granted.	PIA-3 thru PIA-7	Active			
1.2.0	SR-1	5.12.04	Valid Credential	Common Policy Root	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	Access denied.	PIA-3.3	Active			
1.3.3	SO-1	5.13.05	51	00	The system recognizes when the Cardholder Fingerprints CBEFF is expired.	Access denied.	[SP 800-76]	Active			
		5.14			**OCSP Response Checking**						
1.2.0	SR-1	5.14.01	01	00	The system successfully validates a good credential using an OCSP response with a good signature.	Access granted.	PIA-3.2, PIA-3.5	Active			
1.2.0	SR-2	5.14.02	42	37	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Access denied.	PIA-3.2, PIA-3.5, PIA-3.6	Active			
1.2.0	SR-3	5.14.03	43	38	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Access granted.	PIA-3.2, PIA-3.5	Active			
1.2.0	SR-2	5.14.04	44	39	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Access denied.	PIA-3.2, PIA-3.5, PIA-3.6	Active			
1.2.0	SR-1	5.14.05	45	40	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Access denied.	PIA-3.2, PIA-4	Active			
		5.15			**Interoperability Testing**						
1.2.0	SR-1	5.15.01	Valid PIV	Common Policy Root	Various valid PIV cards (including CAC) and PIV-I cards are granted access using PKI-AUTH method.	Access granted.	PIA-6	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-1	5.15.02	39	41	The system recognizes a Federally-issued PIV-I card with a FASC-N that does not begin with fourteen 9s.	Access granted.	PIA-6	Active			
1.3.3	SR-1	5.15.03	02	00	The system recognizes a Federally-issued PIV-I card with a FASC-N that begins with fourteen 9s.	Access granted.	PIA-6	Active			
1.3.3	SR-3	5.15.04	01	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID i*d-PIV-content-signing* (2.16.840.1.101.3.6.7) is present in the content signing certificate.	Access granted.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.05	01	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Access denied.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.06	02	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID, *id-fpki-pivi-content-signing* (2.16.840.1.101.3.8.7) is present in the content signing certificate.	Access granted.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.07	02	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Access denied.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.08	01	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID *id-PIV-cardAuth*(2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Access granted.	[FIPS 201]	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.3	SR-3	5.15.09	01	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Access denied.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.10	02	00	The system recognizes when the Extended Key Usage extension *keyPurposeID* OID *id-PIV-cardAuth* (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Access granted.	[FIPS 201]	Active			
1.3.3	SR-3	5.15.11	02	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeID* OID (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Access denied.	[FIPS 201]	Active			
1.3.3	SR-1	5.15.12	46	00	A valid FIPS 201-2 card results in access granted decision using PKI-AUTH method.	Access granted.	[FIPS 201]	Active			
1.3.3	SR-1	5.15.13	47	00	A FIPS 201-2 card results in access granted decision using PKI-AUTH method with the pivFASC-N in the PIV Authentication and Card Authentication *SubjectAltName* extensions is encoded after the entryUUID.	Access granted.	[FIPS 201]	Active			
1.3.3	SR-1	5.15.14	53	00	The system successfully handles cards with a slightly larger than recommended Card Authentication Certificate (2160 bytes).	Access granted.	[SP800-73]	Active			
		5.16			**Cryptography Testing**						
1.2.0	SR-1	5.16.02	NIST #1	NIST Root	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
							3-3; [Common] §6.1.5				
1.2.0	SO-3	5.16.05	NIST #2	NIST Root	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SR-1	5.16.07	NIST #4	NIST Root	Verify Product's ability to validate signatures using ECDSA (P-256).	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SO-3	5.16.08	NIST #5	NIST Root	Verify Product's ability to validate signatures using ECDSA (P-384).	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5	Active			
1.2.0	SR-1	5.16.10	NIST #1	NIST Root	Verify Product's ability to validate signatures using SHA-256.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5	Active			
1.2.0	SO-3	5.16.11	NIST #5	NIST Root	Verify Product's ability to validate signatures using SHA-384.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5	Active			
1.2.0	SR-1	5.16.12	NIST #1	NIST Root	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	Access granted.	[SP800-78] Table 3-2	Active			
1.2.0	SR-3	5.16.14	01	35	Verify product's ability to validate signatures using RSA 4096 in the path.	Access granted.	Derived from [SP800-78] Table 3-2	Active			
		5.17			**Discovery Object and PIN Usage Policy**						
1.3.0	SR-2	5.17.01	25	00	Discovery object is not present. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). (E-PACS is using Application PIN).	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-2	5.17.02	25	00	Discovery object not present. Enter valid PIV Application PIN. Confirm PIV Application PIN retry counter is reset to 10. Confirm Global PIN retry counter remains at 9. (E-PACS is using the Application PIN).	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-2	5.17.03	26	00	Discovery object is present and set for PIV Application PIN only. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). (E-PACS is using the Application PIN).	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-2	5.17.04	26	00	Discovery object is present and set for PIV Application PIN only. Enter valid PIV Application PIN. Confirm PIV Application PIN retry counter is reset to 10. (E-PACS is using the Application PIN).	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-2	5.17.05	27	00	Discovery object is present. PIV App and Global PINs are available. PIV Application PIN is primary. Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). Confirm Global PIN retry counter remains at 10. (E-PACS is using the PIV Application PIN).	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.0	SR-2	5.17.07	27	00	Discovery object is present. PIV Application and Global PINs are available. PIV Application PIN is primary. Enter valid PIV Application PIN. Confirm PIV Application and Global PINs are both 10. (E-PACS is using the Application PIN).	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SO-2	5.17.10	28	00	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Enter invalid Global PIN (e.g., 999999). Confirm PIV Application PIN retry counter remains at 10. Confirm Global PIN retry counter is decremented by one (9).	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
1.3.3	SO-2	5.17.15	28	00	Discovery object is present. PIV Application and Global PINs are available. Global PIN is primary. Enter valid Global PIN. Confirm PIV Application and Global PINs are both 10. (E-PACS is using the Global PIN).	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Active			
		5.18			**ISO 7816-3 2006 PPS Protocol Compliance**						
1.3.3	UR-3	5.18.01	37	00	Using PKI-AUTH, system's contact readers negotiate a bit rate based on a response from a card with a PPS indicating a bit rate of 446 KBps.	Access granted.	[ISO 7816-3]	Active			
1.3.3	UR-3	5.18.02	37	00	Using PKI-CAK, the system's contactless readers recognize and negotiate a bit rate based on a response from a card with a PPS indicating a bit rate of 848 KBps.	Access granted.	[ISO 14443-4]	Active			
		7.0			**PACS Design Use Cases**						
		7.01			**Continuity of Operations Testing**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UO-3	7.01.01	01	00	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	Design analysis passes.	PCP-1	Active			
1.2.0	UO-3	7.01.02	01	00	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	Design analysis passes.	PCP-1	Active			
1.2.0	UO-3	7.01.03	01	00	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for a valid credential.	Design analysis passes.	PCP-1	Active			
1.3.0	UO-3	7.01.04	01	00	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Design analysis passes.	PCP-1	Active			
1.3.0	UO-3	7.01.05	01	00	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Design analysis passes.	PCP-1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	UO-3	7.01.06	01	00	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for an invalid credential.	Design analysis passes.	PCP-1	Active			
		7.02			**Security Boundaries**						
1.3.0	SR-1	7.02.01			Confirm all PACS components (except for the reader and the bearer's credential) are capable of being located on the secure side of perimeter. Confirm with protocol sniffing between secure/attack side.	...all security relevant processing shall be performed inside the secure perimeter. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	PPE-1	Active			
1.3.0	SO-1	7.02.02			Specific waivers to TC-25-001 shall be granted on a per implementation basis of compensating controls. Document all supplemental security devices and check against relevant APLs, FIPS 140-2. Confirm controls are operational through physical inspection, design documentation. Confirm with protocol sniffing between secure/attack side. .	...compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself.	PPE-1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
		7.03			Registering Physical Access Privileges						
1.3.0	UO-3	7.03.01			Shall be able to define populations (validities) such as "guest, visitor, regular access".	Design analysis passes.	PPL-4	Active			
1.3.0	UO-3	7.03.02			shall be able to define: Access points for each population.	Design analysis passes.	PPL-5, PAC-1	Active			
1.3.0	UO-3	7.03.03			shall be able to define: Temporal access rules for each population.	Design analysis passes.	PPL-5, PAC-1	Active			
1.3.0	UO-3	7.03.04			shall be able to define: Authentication mode required to support TC-26-002 and TC-26-003.	Design analysis passes.	PPL-5, PAC-1	Active			
		7.04			PKI Configuration						
1.2.0	SO-1	7.04.01			The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of X.509 constraints and policies.	PIA-5	Active			
1.2.0	SR-1	7.04.02			The solution shall provide the means to select and manage Trust Anchors. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of trust anchors.	PSC-2	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SO-1	7.04.03			The solution may provide configuration options to ignore PKI faults in certificates (end-entity up to trust anchor). This configuration will reflect the customer's PKI relying party policy.	Perform design review of vendor's PKI configuration options. If options are presented to ignore PKI faults, testing shall proceed to 7.4.4.		Active			
1.2.0	SR-2	7.04.04			For every event where a PKI fault is identified, the solution shall check configuration options to ignore the identified fault. If configuration allows the solution to ignore the fault, the solution shall ignore the fault and produce a warning in the audit log and store the certificate in a certificate store of failed certificates. The audit log shall indicate what failed and provide sufficient information to link the log entry to the stored certificate.	Configure system to ignore PKI faults one by one, per capability of solution. Re-run appropriate ICAM card and PKI tests for both time of registration and time of access with the appropriate fault. Inspect logs and the linked certificate store. Confirm failure is properly identified and certificate matches log entry.		Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	7.04.05			If PKI faults are allowed, the solution shall provide a means to generate a report and consolidate failed certificates for transmission to appropriate parties by email. Running the report and sending the email shall be per the customer's PKI relying party policy.	Confirm ability to generate report and certificates to be sent by email.		Active			
1.2.0	SR-1	7.04.06			The system shall check that the issuing certificate authority has not placed the certificate on its certificate revocation list (CRL) within the previous 6 hours.	Confirm solution's ability to set SCVP DPV, CRL and OCSP response caching to 6 hours or less.	Fed 24 hour policy	Active			
		7.05			**Credential Number Specifications**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-2	7.05.01			The solution shall support FICAM conformant 128-bit FASC-N credential numbers as specified in Table 3 for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit FASC-N. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	PAU-2, PAU-3; Table 6-1 row 3	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-1	7.05.02			The solution shall support FICAM conformant 128-bit UUID credential numbers as specified in Table 3 for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit UUID. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	PAU-2, PAU-3; Table 6-1 row 3	Active			
		7.06			**Validation at Time of Access**						
1.2.0	UO-1	7.06.02	01	00	Shall support contactless Card Authentication Key (PKI-CAK).	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.1	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UO-1	7.06.03	Valid card	Common Policy Root	Shall support BIO.	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Active			
1.2.0	UO-1	7.06.04	01	00	Shall support PIV Authentication Key + PIN (PKI-AUTH).	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.2	Active			
1.2.0	UO-1	7.06.05	Valid card	Common Policy Root	Shall support PIV Authentication Key + PIN + BIO (PKI-AUTH+BIO).	Use Authentication Test logs to verify that all good cards with valid PKI-AUTH and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.5	Active			
1.2.0	UO-1	7.06.06	Valid card	Common Policy Root	Shall support Card Authentication Key + PIN + BIO (PKI-CAK+BIO).	Use Authentication Test logs to verify that all good cards with valid PKI-CAK and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.4	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UO-1	7.06.09	01	00	Shall support contact Card Authentication Key (PKI-CAK).	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7	Active			
1.2.0	SR-1	7.06.11			E-PACS portal solutions shall not support legacy technologies when configured for approved FICAM modes.	Verify solution turns off legacy modes when an approved FICAM mode is enabled. With reader set to PKI-AUTH, attempt to use 125KHz, DESFire, iClass, Indala and related legacy technologies. All access attempts with legacy shall be denied.	[E-PACS] §10.1, §10.1.1, §10.1.2, §10.1.3, §10.1.4, §10.1.5, §10.2	Active			
1.3.0	UO-1	7.06.12			Shall support PKI-CAK + PIN to PACS.	Use Authentication Test logs to verify that all good cards with valid PIN were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3, PIA-10, §10.1.3	Active			
		7.07			**Portal Hardware**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	7.07.01			Product shall support Reader to PACS communications using bi-directional technology. This includes a minimum of one of RS-485, Ethernet, secure wireless.	Verify by system design review. Confirmed using protocol sniffing, review of logs produced during authentication testing.	PCM-2, PCM-3	Active			
1.2.0	UO-3	7.07.02			For multi-factor readers, applicant's system must allow an administrator to modify an individual reader's authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			
1.2.0	UO-3	7.07.03			For multi-factor readers, applicant's system must allow an administrator to modify a group of readers' authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UO-3	7.07.04			For multi-factor readers, the site administrator shall not be required to approach and touch each reader to change its authentication mode (authentication factors).	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			
1.2.0	UO-3	7.07.05			For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			
1.2.0	UO-3	7.07.06			For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UO-2	7.07.07			For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			
1.2.0	UO-3	7.07.08			For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UR-2	7.07.09			Contact readers shall support ISO/IEC 7816.	The contact interface of the reader shall be tested for ISO/IEC 7816 conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-3:2010 Sections 4, 7, and 8. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UR-2	7.07.10			Contactless readers shall support ISO/IEC 14443 Type A.	The contactless interface of the reader shall be tested for ISO/IEC 14443 Type A conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-6:2011 Sections 4, 5, 6.1, 7.1 and 8.1, and ISO/IEC 10373-6:2011/Amd.4:2012. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]	Active			
1.2.0	SR-3	7.07.11			ISO/IEC 14443 Type A contactless readers shall not activate and operate with a PIV card beyond 10cm.	Card 1 is presented at 11cm to the reader. All contactless PIV authentication modes shall fail.	[FIPS 201]	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UR-3	7.07.12			ISO/IEC 14443 Type A contactless readers shall provide sufficient field strength to activate and operate with a PIV card at a distance no less than 3.5cm from the reader.	Card 1 is presented at 3.5cm to the reader. All contactless PIV authentication modes shall succeed.	[FIPS 201]	Active			
1.2.0	UO-3	7.07.14			For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered non-compliant.	Verify by system design review	PCM-3	Active			
		7.08			**Auditing and Logging**						
1.2.0	SR-2	7.08.01			Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability.	Verify by review of logs and reports	PAU-1, PAU-2, PAU-7	Active			
1.2.0	SR-1	7.08.02			The product shall provide auditing/logging of all PKI processing to include: - Pass/fail from a Challenge/Response - PDVAL - Disabling credential based on PDVAL, expiration or revocation status.	Verify by review of logs and reports; confirmed by protocol sniffing	PAU-3, PAU-4, PAU-7	Active			
1.2.0	SR-2	7.08.03			The product shall provide auditing/logging of credential number processing and transmission.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7	Active			
1.2.0	SR-2	7.08.04			The product shall provide auditing/logging of all software driven configuration changes.	Verify by review of logs and reports	PAU-6, PAU-7	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-2	7.08.05			The product shall provide auditing/logging of periodic certificate PDVAL and status checking.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7	Active			
1.2.0	SR-2	7.08.06			The product shall provide auditing/logging of Card activity (e.g., 3 days of card activity).	Verify by review of logs and reports	PAU-3, PAU-7	Active			
1.2.0	SR-2	7.08.07			The product shall provide auditing/logging of last known location of a card in system.	Verify by review of logs and reports	PAU-3, PAU-7	Active			
1.2.0	SR-2	7.08.08			The product shall provide auditing/logging of PKI policies for name constraints, path constraints, validity checks.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7	Active			
1.2.0	SR-2	7.08.09			The product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop).	Verify by review of logs and reports	PAU-3, PAU-7	Active			
1.2.0	SR-2	7.08.10			The product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom.	Verify by review of logs and reports	PAU-4, PAU-7	Active			
1.2.0	SR-2	7.08.11			The product shall provide auditing/logging of all readers and their modes.	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7	Active			
1.2.0	SR-2	7.08.12			The product shall provide auditing/logging of configuration download status to system components.	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7	Active			
		7.09			**Security Certification and Accreditation**						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	UR-1	7.09.01			As required by UL 294, relevant components within the solution shall have a UL 294 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2	Active			
1.2.0	UO-3	7.09.02			As required by UL 1076, relevant components within the solution shall have a UL 1076 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2 derived	Active			
1.2.0	UO-3	7.09.03			As required by UL 1981, relevant components within the solution shall have a UL 1981 listing.	Verify UL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-2 derived	Active			
1.2.0	UR-1	7.09.04			When adding a component to an existing system under a given topology, each existing component in the existing system under that topology shall have FIPS 201 Evaluation Program APL status.	Verify APL listing. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-3	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.2.0	SR-1	7.09.05			Each component leveraging cryptography in the system shall have FIPS 140-2 Overall Security Level 1 (or greater) certification. Each component's operating environment must match at least one operating environment, i.e., O/S version and processor type, on a FIPS 140-2 certificate's security policy document. Cryptographic operations must all be performed using only the FIPS 140-2 cryptographic modules as stated on the vendor attestation.	Verify NIST CMVP listing. Must be applied for and in process for certification before any testing can be done. Must be listed before final testing and certification by FIPS 201 Evaluation Program.	PCA-4, [FIPS 201]	Active			
1.3.0	SR-1	7.09.06			Vendors shall self-certify that their products and services are in compliance with [BAA] requirements.	Review Attestation from application.	[BAA]	Active			
1.3.0	SR-1	7.09.07			Vendors shall self-certify that their products and services are in compliance with [TAA] requirements.	Review Attestation from application.	[TAA]	Active			
1.3.3	SR-1	7.09.08			Verify that all PACS and Validation System vendor software executables are signed by an entity whose certificate chain terminates at a well-known trust anchor.	All shared libraries, executables (including .MSI files) have been signed by a trusted source.	[SP800-53]	Active			
		7.10			**Biometric in PACS**						
1.2.0	SR-2	7.10.01			Shall follow PIA-3.4 Detailed Guidance Case 3 to encrypt biometric identifiers leveraged in BIO to PACS.	Verify by system design and inspection of database	PIA-3.4	Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
		7.11			Operational Controls						
1.2.0	SR-2	7.11.01			The system shall have the ability to enforce administrative privilege for configuration management operations.	Verify by use of the system.	PCM-1	Active			
1.2.0	SR-2	7.11.02			Shall authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done using E-Auth LOA-4 credentials.	Verify by use of the system.	PCM-1	Active			
1.2.0	UO-3	7.11.03			The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.	Verify by use of the system.	PCM-2	Active			
1.2.0	UO-3	7.11.04			Each physical component shall be separately defined and addressable within the server user interface.	Verify by setting up of system.	PCM-2	Active			
1.2.0	UO-3	7.11.05			The system shall support configuration downloads to relevant components .	Verify by setting up of system.	PCM-2	Active			
		7.12			Accessibility						

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	UR-2	7.12.01			33. SECTION 508 COMPLIANCE. Offerors are required to self-certify that their products or services are in compliance with Section 508 technical standards. Therefore, the offeror is required to submit with its offer a designated area on its website that outlines the Voluntary Product Accessibility Template (VPAT) or equivalent qualification, which ultimately becomes the Government Product Accessibility Template (GPAT).	Review VPAT from application.	[Sect 508]	Active			
		8.0			Handheld Requirements						
		8.01			Communications						
1.3.0	SR-1	8.01.01			Ensure a secure connection using an encrypted wireless session using a NIST certified encryption method.	Verify within the handheld settings that there is an option to encrypt communications using NIST approved methods.		Active			
1.3.0	SR-1	8.01.02			At a minimum, must have built-in support for Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2).	Verify within the handheld settings that the interface supports a minimum of WPA. WPA-2 is preferred.		Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-1	8.01.03			At a minimum, the system has the ability to communicate using 802.11 a, b, c, g, n.	Verify within the handheld settings that the wireless interface supports one of the listed protocols.		Active			
1.3.0	SR-1	8.01.04			At a minimum, the Handheld must be able to support both 3G and 4G communications for cellular communications.	Verify within the handheld settings that the option for 3G or 4G communications exists.		Active			
1.3.0	SR-1	8.01.05			Handheld must have the ability to demonstrate the option to select a primary communication source and a secondary communication source.	Verify the reader interface allows the devices to be configured for a primary and secondary method of communications.		Active			
1.3.0	SR-1	8.01.06			Handheld must be able to failover from primary to secondary mode to maintain an online state with PACS and Validations system.	Verify that if wireless communications is lost, the reader attempts to connect to secondary mode of communications.		Active			
1.3.0	SR-1	8.01.07			Reader provides a visual indication that the handheld is in an online or offline state. .	Verify the reader provides an indication that the reader is in an offline state.		Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
		8.02			Operational Requirements						
1.3.0	UR-1	8.02.01			The handheld must be capable of supporting contactless, contact, or both modes of authentication. Interfaces can be fully integrated or modular. .			Active			
1.3.0	UR-1	8.02.02			Contactless modes must support a minimum of: CAK+CHUID.			Active			
1.3.0	UR-1	8.02.03			Contact modes must support a minimum of: CAK+CHUID PIV+PIN PIV+PIN+BIO.			Active			
		8.03			Docking Station						
1.3.0	UR-1	8.03.01			The handheld docking station must utilize a hardwired Ethernet port or wireless communications with the Validation System, PACS, or other trusted source.			Active			
1.3.0	SR-1	8.03.02			The handheld docking station provides a mechanism to securely update the handheld while cradled in the device, via hardwired Ethernet or Wireless communications. Updates can be from online validation system, PACS or other trusted source. Secure communication enforced by mutual authentication TLS with PKI.	Design analysis passes.		Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-1	8.03.03			Handheld must automatically logout operator when placed in docking station. .	Design analysis passes.		Active			
		8.04			**FINGERPRINT Verification**						
1.3.0	SO-1	8.04.01			• See Section 2 – Validation at time of Registration • See Section 5 – Validation at time of Access.			Active			
1.3.0	SO-1	8.04.01			• See Section 2 – Validation at time of Registration • See Section 5 – Validation at time of Access.			Active			
		8.05			**Import Function**						
1.3.0	UR-1	8.05.01			Reader must cache CRL information locally on the handheld. This CRL data must include the Certificate PATH information and be supplied by an online Validation System or other trusted source.			Active			
1.3.0	SR-1	8.05.02			Cached information must be protected either by a FIPS140-2 Level 1 software or Level 2 HSM.	Design analysis passes.		Active			
1.3.0	SR-1	8.05.03			The reader must cache authentication and authorization information for all cardholders with access to the Handheld assigned area. This information can be transferred from either an online validations system or other trusted source. .			Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-1	8.05.04			The Handheld device must have the ability to provide a visual indication when locally cached information is over 6 hours old.	Design analysis passes.		Active			
		8.06			**Operational**						
1.3.0	SR-1	8.06.01			System must automatically log the operator out of the handheld after a user defined time of non-use. .	Design analysis passes.		Active			
		8.07			**Online Validation Requirements**						
1.3.0	SR-1	8.07.01			When the Handheld is online communicating with the Validations System, functional requirements defined within the Validation System category apply.			Active			
		8.08			**Online PACS Requirements**						
1.3.0	SR-1	8.08.01			When the Handheld is online communicating with the PACS, the PACS functional requirements defined in the PACS Infrastructure category apply.			Active			
		8.09			**Offline Validation Requirements**						
1.3.0	SR-1	8.09.01			Handheld must use locally cached authentication and authorization data to authenticate and authorize the operator.			Active			
1.3.0	SR-1	8.09.02			Handheld must be able to determine the validity of the cardholder certificates using the locally cached validation data.			Active			

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Status	Category(ies)	Components	Process
1.3.0	SR-1	8.09.03			Handheld must provide the operator with indication that the locally stored data exceeds 6-hour refresh limit.			Active			
1.3.0	SR-1	8.09.04			Handheld must cache PKI Validation decisions to be uploaded to the trusted source for archive and reporting.			Active			
		8.10			**Offline PACS Requirements**						
1.3.0	SR-1	8.10.01			The handheld must provide an indication to the operator that the reader is in offline mode.	Design analysis passes.		Active			
1.3.0	SR-1	8.10.02			The handheld must be able to use locally cached PACS data to verify cardholders access privileges. For example: • Schedule • Shift • Access to areas The operator must be provided a visual indication of access granted or denied. .			Active			
1.3.0	SR-1	8.10.03			While in offline mode the handheld must log all access decisions made at the handheld.			Active			
1.3.0	SR-1	8.10.04			When transitioning from an offline to an online state the handheld must transfer all locally stored access transaction to the PACS solution or other trusted source.	Design analysis passes.		Active			