Physical Access Control Systems (PACS) Functional Requirements and Test Cases (FRTC)

VERSION 1.4.2 Rev. A

FIPS 201 EVALUATION PROGRAM

March 31, 2021

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

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1		Document creation.	Limited
Draft	0.0.2	4/30/2013	Added background and objectives text, normative references.	Limited
Draft	0.1.0	4/30/2013	Full comment resolution version for review.	Limited
Draft	0.1.1	5/1/2013	Release candidate 1.	Limited
Draft	0.1.2	5/2/2013	Revised per May 1, 2013 EPTWG Meeting.	Limited
Draft	0.1.3	5/6/13	Draft Release.	EPTWG
Draft	1.0.0 RC1	7/16/2013	Final review for program release.	Limited
Draft	1.0.1 RC2	7/19/2013	QA updates approved.	Limited
RC1	1.1.2	8/21/2013	Final release.	Public
RC2	1.1.3	8/29/2013	Minor fixes.	Limited
RC3	1.1.4	9/4/2013	CHUID deprecated; Credential # anti-collision specs added; Remove optional technologies.	Limited
RC4	1.1.5	9/12/2013	Requirements for allowing PKI processing to be degraded and logging of failed certificates.	Limited
RC5	1.1.6	9/20/2013	Improved credential processing; added 6-hour CRL requirement; added FICA< mode = no legacy; fixed path names; restored missing path tests 22-35; identified invalid test cases.	Limited
Final	1.2.0	10/23/2013	Updated per initial testing for public release; used Reverse BCD format for 128-bit FASC-N; labeled incorrect tests for future update; identified test cases that will no longer be tested.	Public
Final	1.3.0	3/2/2015	• 3/14/14 – First edit for errata. • 4/16/14 – Second errata edit. Updated document publication schedule. Removed Test Number column. Added Appendix 2, Deprecated Functional Requirements and test Cases. Update for PIV in E-PACS v3.0. Test section numbers static. • 6/2/14 – Fixed cached Public Key test cases; re-worded [Sect508] requirement, added severity level info, re-wrote publication schedule with severities in mind. Added Appendix 3, Severity Levels, to describe the severity level concept. • 7/6/14 – Added Mobile Handheld Requirements. 3/2/15 – Removed deprecated items from the PKI Paths Table and moved them to new Appendix 3, Deprecated ICAM PKI Paths (old Appendix 3 moved to Appendix 4). Deleted tables and other content no longer needed (e.g., date dependent items where the date is now in the past / no longer applicable).	Public

Status	Version	Date	Comment	Audience
Final	1.3.1	7/28/2015	• Added Section 2.1, Addendums • Added PPS entries 30-37 in Table 1 • Added Section 2.19, ISO 7816-3 2006 PPS Protocol Compliance • Added Section 5.18, ISO 7816-3 2006 PPS Protocol Compliance • Reworded 7.7.12 requirements statement	Public
Final	1.3.1	8/18/2015	Fixed test case language for PPS Protocol Compliance.	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
Final	1.3.3 Rev C	1/7/2018	• Replaced all instances of the use of ICAM Test Card #01 with ICAM Test Card 46. • Replaced all instances of the use of ICAM Test Card #02 with ICAM Test Card 54. • Corrected expected Global PIN retry counter, Test Cases 2.18.02 and 5.17.02. • Added ICAM Test Card 55 (Missing Security Object) and Test Case 2.14.03. • Clarified the expected result of Test Cases 2.16.02 and 5.15.02.	Public

Status	Version	Date	Comment	Audience
Final	1.3.3 Rev. D	4/24/2018	• Deprecated Test Cases 2.06.03, 2.06.04, 5.06.03., 5.06.04, and 5.11.01. (and removed Section 5.11). • For time-of-access fault path testing, included instructions as to which golden card must be registered with the PACS. • Activated ICAM Test Card 48 (PPS with LEN value greater than zero). • Corrected bit ordering of last 5 digits of example FASC-N in Credential Identifier Processing in Section 5. • Corrected card type from Card Authentication Certificate to PIV Authentication Certificate in Test Cases 2.06.07 and 5.06.07. • Added "Valid/Invalid" column to card description table. • Verified and updated links to normative references. • Clarified card type (PIV/PIV-I) for test cases 7.05.01 and 7.05.02	Public
Final	1.3.3 Rev. E	6/21/2018	• Deprecated Test Case 5.12.02 • Clarified that Card 7 must be personalized with the tester's biometric. • Removed Fault Paths 37-40 • Deprecated Test Cases 8.01.01-8.10.04 (Handheld)	Public
Final	1.3.3 Rev. F	8/21/2018	• Deprecated Test Cases 2.17.14 and 5.16.14 because RSA 4096 was deprecated by FIPS 186-3 and subsequently SP 800-78-2. • Changed wording of Test Case 5.02.03 to "With ICAM Test Card 46 registered with the PACS, verify product's ability to reject a credential when notAfter date of any certificate in the path is sometime in the past." • Deprecated Test Case 5.02.05 because Test Case 5.02.03 was updated to include all certificates in the path. • Added Test Cases 2.10.8 and 2.10.9 because Paths 3 and 16 can be used to test them.	Public
Final	1.3.3 Rev. G	2/1/2019	• Changed 5.15.04 to "With ICAM Test Card 46" • Deprecated Test Cases 2.04.05 and 5.04.05 (requires SKID to consist of SHA-1 of public key). Going forward, PACS should not enforce this rule. • Replace "CHUID signature" with Card Authentication" in the description for Test Case	Public

Status	Version	Date	Comment	Audience
			5.06.13. We are testing for a Card Authentication certificate policy OID. • The description for Test Case 5.15.04 was changed to, "With ICAM Test Card 46...". • Added Test Cards 57, 58, and 59 and Test Cases 2.09.11, 2.10.10, 5.09.11, and 5.10.1 • Changed Test Case 5.12.05 to " With ICAM Test Card 59 registered...". • Changed Test Case 5.14.05 to ".. To register ICAM Test Card 45...".	
Final	1.4.2 Rev. A	3/31/2021	• Incorporated test cases for Secure Messaging (SM) and On-Card Comparison (OCC). See SM-OCC Companion Paper. • Incorporated test cases for Backend Registration. See Backend Registration Companion Paper. • Consolidated test cases to accommodate FRTC express testing for previously tested solutions. See FRTC Express Companion Paper	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 Change Control

This document is a living document and is expected to be updated over time as new or revised functional requirements are identified. In addition, this document will be updated in accordance with the following schedule:

1. A new version will be published no less than one year from issuance of the current version.
2. If security or infrastructure risks are identified, an interim release may occur.

All new versions are effective immediately. New or revised requirements and their test cases will include an effective date, commensurate with their assigned severity level (see paragraphs 7.1, 7.2, and 7.3.

All approved Physical Access Control Systems (PACS) solutions must pass testing against new and revised requirements before their effective date or be moved to the Removed Products List (RPL).

Notification of changes will be sent to the Evaluation Program Technical Working Group (EPTWG) email list.

3 Objectives

This document identifies the functional requirements that the FIPS 201 Evaluation Program will perform on PACS submitted for evaluation. All requirements are instrumented using a smart card as presented to the system and various Public Key Infrastructure (PKI) paths. The PKI and smart cards test for specific common failures in cards and PKI, as well as Advanced Persistent Threat (APT) issues that impact PACS specifically. The PACS evaluation process is designed to be agnostic to architecture and focuses solely on functional testing using an end-to-end testing methodology.

4 Test Instrumentation

For PACS, the FIPS 201 Evaluation Program relies on fully-defined, instrumented testing. This requires two core elements:

1. ***ICAM Test Cards*** – There are two cards that are completely valid and well formed. In addition, there are cards that have injected faults assuming day-to-day operational errors, and cards emulating a well-funded attacker.
2. ***Test PKI*** – Provides the ability to link golden test cards with PKI faults, which provides the mechanism needed to verify that the system under test honors the PKI.

The full testing regimen, leveraging these test instruments, is described in *7*.

4.1 ICAM Cards Used in Test

The following cards are used in the FIPS 201 Evaluation Program.

- Live PIV and PIV-I Cards from various issuers;
- ICAM Test Cards (detailed in *Table 1*);
- NIST PIV Test Cards; and
- DoD JITC CAC Test Cards.

Table 1 - ICAM Test Cards Used in Test

ICAM Test Card	Valid/In-valid	Description	Threat Type
1	Valid	Golden PIV	None
2	Valid	Golden PIV-I	None
3	Invalid	Deprecated: Substituted keypair in PKI-AUTH certificate (AKID/SKID mismatch)	Manipulated Data
4	Invalid	Tampered CHUID	Manipulated Data
5	Invalid	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Invalid	Tampered PHOTO	Manipulated Data
7	Invalid	Tampered FINGERPRINT	Manipulated Data
8	Invalid	Tampered SECURITY OBJECT	Manipulated Data
9	Invalid	Expired CHUID signer	Invalid Date
10	Invalid	Expired certificate signer	Invalid Date

ICAM Test Card	Valid/In-valid	Description	Threat Type
11	Invalid	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Invalid	Authentication certificates valid in future	Invalid Date
13	Invalid	Expired authentication certificates	Invalid Date
14	Invalid	Expired CHUID	Invalid Date
15	Invalid	Valid CHUID copied from one card to another **(PIV)**	Copied Credential
16	Invalid	Valid Card Authentication Certificate copied from one card to another **(PIV)**	Copied Credential
17	Invalid	Valid PHOTO copied from one card to another **(PIV)**	Copied Credential
18	Invalid	Valid FINGERPRINT copied from one card to another **(PIV)**	Copied Credential
19	Invalid	Valid CHUID copied from one card to another **(PIV-I)**	Copied Credential
20	Invalid	Valid Card Authentication Certificate copied from one card to another **(PIV-I)**	Copied Credential
21	Invalid	Valid PHOTO copied from one card to another **(PIV-I)**	Copied Credential
22	Invalid	Valid FINGERPRINT copied from one card to another **(PIV-I)**	Copied Credential
23	Invalid	Private and Public Key mismatch	Manipulated Keys
24	Invalid	Revoked authentication certificates	Revoked Credential
25	Valid	Discovery object is not present	Only Application PIN is present and shall be used.
26	Valid	Discovery object tag 0x5F2F is present First byte: 0x40, Second byte 0x00	Only Application PIN is present and shall be used.
27	Valid	Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x10	Application and Global PINs are

ICAM Test Card	Valid/In-valid	Description	Threat Type
			present. Application PIN is primary.
28	Valid	Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x20	Application and Global PINs are present. Global PIN is primary.
29	Valid	Deprecated: Discovery object is present and tag 0x5F2F is not populated	Only Application PIN is present and shall be used.
30	Valid	Future: Card with PPS F=372, D=1 (13,440 baud)	ISO Standards Conformance
31	Valid	Future: Card with PPS F=372, D=2 (26,881 baud)	ISO Standards Conformance
32	Valid	Future: Card with PPS F=372, D=4 (53,763 baud)	ISO Standards Conformance
33	Valid	Future: Card with PPS F=372, D=12 (161,290 baud)	ISO Standards Conformance
34	Valid	Future: Card with PPS F=512, D=8 (78,125 baud)	ISO Standards Conformance
35	Valid	Future: Card with PPS F=512, D=16 (156,250 baud)	ISO Standards Conformance
36	Valid	Future: Card with PPS F=512, D=32 (312,500 baud)	ISO Standards Conformance
37	Valid	Card with PPS F=512, D=64 (625,000 baud)	ISO Standards Conformance
38	Invalid	Hash value within the Security Object does not match hash value of its corresponding data group buffer.	Manipulated Data
39	Valid	Federally issued PIV-I card using FASC-N with the agency's Agency Code plus System Code, Credential Number, Credential Series Code, and Issue Code.	Incorrect Identifier
40	Valid	Deprecated (replaced by Card 54): Federally-issued PIV-I. Valid: Federally issued PIV-I card using fourteen 9s.	Incorrect Identifier

ICAM Test Card	Valid/In-valid	Description	Threat Type
41	Invalid	Public key on card does not match public key previously registered to the system.	Copied container
42	Invalid	Certificates on the card refer to an OCSP responder that uses an expired response signing certificate.	Invalid Date
43	Valid	Valid certificates on the card refer to an OCSP responder that uses a response signing certificate that is revoked but contains the *id-pkix-ocsp-nocheck* OID.	Invalid Credential
44	Invalid	Certificates on the card refer to an OCSP responder that uses a response signing certificate that is revoked, and the *id-pkix-ocsp-nocheck* OID is not present.	Invalid Credential
45	Invalid	Certificates on the card refer to an OCSP responder that uses a response signing certificate with an invalid signature.	Manipulated Data
46	Valid	Valid: FIPS 201-2 card with card UUIDs in the SubjectAltName extensions are sequentially after the FASC-Ns (replaces Card 1).	None
47	Valid	Golden FIPS 201-2 PIV card with card UUIDs in the SubjectAltName extensions are sequentially before the FASC-N.	SP 800-73-4 Standards Conformance
48	Valid	Golden FIPS 201-2 PIV card with ISO 7816-compliant PPS Le byte required.	ISO Standards Conformance
49	Invalid	FIPS 201-2 PIV card profile with exception that Cardholder Facial Image CBEFF has expired.	Invalid Date
50	Valid	Golden FIPS 201-2 PIV card profile with exception that Cardholder Facial Image CBEFF will expire before CHUID expiration date.	Invalid Date
51	Invalid	FIPS 201-2 PIV card profile with exception that Cardholder Fingerprints CBEFF has expired.	Invalid Date
52	Valid	Golden FIPS 201-2 PIV card profile with exception that Cardholder Fingerprints CBEFF will expire before CHUID expiration date.	Invalid Date
53	Valid	Golden FIPS 201-2 PIV card profile with slightly larger than recommended Card Authentication Certificate (2160 bytes).	SP 800-73-4 Standards Conformance
54	Valid	Golden FIPS 201-2 Non-Federally Issued PIV-I card (replaces Card 2).	None

ICAM Test Card	Valid/In-valid	Description	Threat Type
55	Valid	FIPS 201-2 PIV card missing its Security Object	Tampered Data
57	Invalid	FIPS 201-2 PIV card with revoked CHUID signing cert	Invalid Credential
58	Invalid	FIPS 201-2 PIV cards with revoked Card Authentication cert	Invalid Credential
59	Valid	Used to register FASC-N for Card 51. After this card is registered, the time of access test case for Card 51 can be run.	Invalid Credential
60	Invalid	PIV-AUTH certificate SKID does not match EE public key in the Auth Certificate.	Tampered Data
61	Invalid	PIV CHUID content signing certificate does not express EKU policy OID id-PIV-content-signing (2.16.840.1.101.3.6.7).	Invalid Credential
62	Invalid	PIV Secure Messaging Certificate Signer content signing certificate does not express EKU policy OID id-PIV-content-signing (2.16.840.1.101.3.6.7).	Invalid Credential
63	Valid	Golden PIV with SM ciphersuite '27', fully configured SM-AUTH, and fully configured OCC-AUTH, intermediate CVC present.	None
64	Valid	Golden PIV-I with SM ciphersuite '27', fully configured SM-AUTH, and fully configured OCC-AUTH, intermediate CVC present.	None
65	Valid	Golden PIV with SM ciphersuite '2E', fully configured SM-AUTH, and fully configured OCC-AUTH, intermediate CVC present.	None
66	Invalid	Based on 65, but PIV Application Property Template Tag '61' does not contain Tag 'AC'.	Invalid Credential
67	Invalid	Based on 65, but PIV Application Property Template Tag '61' contains Tag 'AC' but it does not contain a tag '80' reference of '27' or '2E'.	Invalid Credential
68	Invalid	Based on 65, but Buffer 0x1017 is empty.	Invalid Credential

69	Invalid	Based on 65, but Buffer 0x1017 does not contain tag 0x70.	Invalid Credential
70	Invalid	Based on 65, but Buffer 0x1017 tag 0x70 is empty.	Invalid Credential
71	Invalid	Based on 65, but keyref '04' key is a P-256 key.	Invalid Credential
72	Invalid	Based on 65, but the CVC's issuer identification number does not match the subjectKeyIdentifier in the contentSigning certificate when no intermediate CVC is present.	Invalid Credential
73	Invalid	Based on 65, but the Intermediate CVC's issuer identification number does not match the subjectKeyIdentifier in the contentSigning certificate.	Invalid Credential
74	Invalid	Based on 65, but the CVC's issuer identification number does not match the subjectKeyIdentifier in the intermediate CVC.	Invalid Credential
75	Invalid	Based on 65, but the Secure Messaging Content Signer contentSigning certificate issuance date is set to some date in the past (e.g., 01/01/2020).	Invalid Credential
76	Invalid	Based on 65, but the CRL from crlDP URL within Secure Messaging Content Signer contentSigning certificate states it is revoked.	Invalid Credential
77	Invalid	Based on 65, but the Secure Messaging Certificate Signer contentSigning certificate does not express EKU policy OID 2.16.840.1.101.3.6.7 for content-signers.	Invalid Credential
78	Invalid	Based on 65, but the Secure Messaging Content Signer contentSigning certificate contains policy '1.2.3.4.5.6'.	Invalid Credential
79	Invalid	Based on 65, but buffer 0x1016 is empty.	Invalid Credential
80	Invalid	Based on 65, but buffer 0x1016 contains ‘7F 61 03 02 01 00’.	Invalid Credential
81	Invalid	PIV-AUTH certificate AKID does not match issuer's public key ID.	Invalid Credential

4.2 PKI Used in Test

Table 2 describes the PKI infrastructure used for the FIPS 201 Evaluation Program.

Table 2 - ICAM PKI Path Descriptions

ICAM PKI Path Number	Fault description	Operational Group
1	ICAM Invalid CA Signature	Manipulated Data
2	ICAM Invalid CA *notBefore* Date	Revoked/Date Invalid
3	ICAM Invalid CA *notAfter* Date	Revoked/Date Invalid
4	ICAM Invalid Name Chaining	Standards Conformant Processing
5	ICAM Missing Basic Constraints	Standards Conformant Processing
6	ICAM Invalid CA False Critical	Manipulated Data
7	ICAM Invalid CA False not Critical	Standards Conformant Processing
8	ICAM Invalid Path Length Constraint	Standards Conformant Processing
9	ICAM *keyUsage keyCertSign* False	Standards Conformant Processing
10	ICAM keyUsage Not Critical	Standards Conformant Processing
11	ICAM *keyUsage* Critical *CRLSign* False	Standards Conformant Processing
12	ICAM Invalid *inhibitPolicyMapping*	Standards Conformant Processing
13	ICAM Invalid DN *nameConstraints*	Standards Conformant Processing
14	ICAM Invalid SAN *nameConstraints*	Standards Conformant Processing
15	ICAM Invalid Missing CRL	Standards Conformant Processing
16	ICAM Invalid Revoked CA	Revoked/Date Invalid
17	ICAM Invalid CRL Signature	Manipulated Data
18	ICAM Invalid CRL Issuer Name	Standards Conformant Processing
19	ICAM Invalid Old CRL *nextUpdate*	Revoked/Date Invalid
20	ICAM Invalid CRL *notBefore*	Revoked/Date Invalid
21	ICAM Invalid CRL Distribution Point	Standards Conformant Processing
22	ICAM Valid *requiredExplicitPolicy*	Standards Conformant Processing
23	ICAM Invalid *requiredExplicitPolicy*	Standards Conformant Processing

ICAM PKI Path Number	Fault description	Operational Group
24	ICAM Valid GeneralizedTime	PKI/Crypto Compatibility
25	ICAM Invalid GeneralizedTime	Standards Conformant Processing
32	Deprecated: ICAM Invalid SKID	Standards Conformant Processing
33	ICAM Invalid AKID	Standards Conformant Processing
34	ICAM Invalid CRL format	Standards Conformant Processing
35	Deprecated: ICAM 4096bit RSA key	PKI/Crypto Compatibility
36	ICAM Invalid CRL Signer	Standards Conformant Processing
41	Golden PIV-I path - conforming with SP 800-73-4 data model	Standards Conformant Processing
42	The Signing CA certificate provides a CRL distribution point in its issued certificates, but it does not post a CRL. (no CRL present for EE)	Standards Conformant Processing
43	The Signing CA has been revoked	Revoked/Date Invalid
44	The SCA issued and revoked a CHUID certificate.	Revoked/Date Invalid
45	The Signing CA certificate keyUsage extension is missing keyCertSign and cRLSign, keyUsage is not marked critical	Standards Conformant Processing
46	PIV/PIV-I content signing certificate does not express Policy OID that maps to Federal Common id-fpki-common-piv-contentSigning 2.16.840.1.101.3.2.1.48.86.	Standards Conformant Processing
47	RSA 2-1-1 SCA and RCA	PKI/Crypto Compatibility
48	RSA 2-1-1 SCA and RSA 3-1-1 RCA	PKI/Crypto Compatibility
49	RSA 2-1-256 SCA and RCA	PKI/Crypto Compatibility
50	RSA 2-1-256 SCA and RSA 3-1-256 RCA	PKI/Crypto Compatibility

51	RSA 3-1-256 SCA and RCA	PKI/Crypto Compatibility
52	RSA 4-1-256 SCA and RCA	PKI/Crypto Compatibility
53	RSA 2-1-256 SCA and RCA	PKI/Crypto Compatibility
54	RSA 2-1-256 SCA and RSA 3-1-256 RCA	PKI/Crypto Compatibility
55	P-256-256 SCA and RCA	PKI/Crypto Compatibility
56	P-256-256 SCA and P-384-256 RCA	PKI/Crypto Compatibility
57	P-384-256 SCA and RCA	PKI/Crypto Compatibility
58	P-384-384 SCA and RCA	PKI/Crypto Compatibility

5 Credential Number Processing

Table 3 describes the minimal set of credential number processing rules. All solutions shall use 128-bit (16 byte) credential numbers to provide full protection against credential number collisions and to ensure interoperability between PACS components. These credential numbers shall be processed, transmitted, and stored in binary format. It is strongly recommended that credential numbers not be parsed into separate fields for interoperability, audit, and ease of testing purposes (see Test Cases 7.5.1, 7.5.2, and 7.8.3). If the system parses the numbers into separate fields, they must be stored in such a way that the 128-bit credential can be viewed from the user interface or through reporting in its original 128-bit format. The details of how the credential is parsed shall be provided to the GSA ICAM Lab for testing purposes. The FIPS 201 Evaluation Program anticipates new categories that have direct interaction with E-PACS (e.g., PSIM and PIAM). These new categories are anticipated to require that credential numbers be stored in a single field.

Table 3 – Minimal Set of Credential Number Processing Rules

FASC-N Rule	
PIV and CAC: 128 Bit Output (Reverse BCD) FASC-N ID + CS + ICI + Pers Inden + Org Cat + Org Ind + Pers/Org (parity automatically removed)	Serial Output: 13 41 00 01 98 76 54 11 12 34 56 78 90 11 34 11
	Decoded Wiegand Data: 1 3 4 1 – 0 0 0 1 – 9 8 7 6 0001 0011 0100 0001–0000 0000 0000 0001–1001 1000 0111 0110 5 4 – 1 – 1 – 1 2 3 4 5 6 7 8 0101 0100–0001–0001–0001 0010 0011 0100 0101 0110 0111 1000 9 0 – 1 – 1 3 4 1 – 1 1001 0000–0001–0001 0011 0100 0001–0001
	Translated Card Data: Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1
UUID Rule	
PIV and PIV-I: 128 Bit UUID	16-byte binary representation of the UUID as defined by [RFC 4530].

6 Normative References

[BAA] Buy American Act Certification FAR 52.225-2
https://www.law.cornell.edu/cfr/text/48/52.225-2

[Common] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, September, 2021, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0 March 26, 2014
https://playbooks.idmanagement.gov/assets/pacs/PIV-in-EPACS-v3.pdf

[FBCA] X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), Version 2.35, April, 2019, or as amended
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-fbca.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

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

[ISO 7816-3] Identification cards – Integrated Circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols, International Organization for Standardization, ISO/IEC 7816-3, 2006, as amended
https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-3:ed-3:v1:en

[ISO 14443-4] Cards and security devices for personal identification – Contactless proximity objects – Part 4: Transmission protocol, International Organization for Standardization, ISO/IEC 1443-4, 2018, as amended
https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-4:ed-4:v1:en

[M-19-17] Enabling Mission Delivery through Improved Identity, Credential and Access Management, Office of Management and Budget (OMB) Memorandum M-19-17, May, 2019
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.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] Common Policy X.509 Certificate and Certificate Revocation list (CRL) Profiles, Version 2.1, February, 2021, or as amended https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-common.pdf

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011 https://playbooks.idmanagement.gov/docs/roadmap-ficam.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] Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation, NST Special Publication 800-73-4, May 2015 or as amended https://csrc.nist.gov/publications/detail/sp/800-73/4/final

[SP800-76] Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 2013, or as amended https://csrc.nist.gov/publications/detail/sp/800-76/2/final

[SP800-78] Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST Special Publication 800-87-4, May 2015, or as amended https://csrc.nist.gov/publications/detail/sp/800-78/4/final

[SP800-116] Guidelines for the Use of PIV Credentials in Facility Access, NIST SP 800-116 Revision 1, June 2018, or as amended https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final

[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

7 Functional Requirements and Test Cases

7.1 Severity Levels

If [FRTC] functional requirements are revised due to time-sensitive security threats, noted technology vulnerabilities, or other critical issues, or alternatively, specific problems are discovered in a vendor's product (or class of products) after it has been listed on the APL, the affected vendor(s) will be notified that the identified product(s) must be improved as necessary in order to remain on the APL. A remediation grace period will be granted commensurate with the severity level of the problem.

7.2 APL Listing Requirements

Table 4 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 5* 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 4 - 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	✅

[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 5** below.

Test Level / Classification	Severity 1	Listed on APL	Severity 2	Listed on APL[1]	Severity 3	Listed on APL
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 5 - 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 operations, PACS availability, or other area examined.	90 days
3	The identified problem results in a Low impact to any of security, PACS operations, PACS availability, or other area examined.	1 year

7.3 Classification Codes and Scoring Guidelines

The FRTC's associated 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 6* describes the classification codes.

Table 6 - Classification Codes

Classification Code	**Security/Usability**
S[RO]-[1..3]	**Security** - A control directly impacting security of the system.
U[RO]-[1..3]	**Usability** - A control impacting end user system usability. Does not directly impact security.
Classification Code	**Required/Optional**
[SU]R-[1..3]	**Required** - Must be present. Must work correctly: Red/Green.
[SU]O-[1..3]	**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**

Table 7 - Impact Guidelines

	High	Moderate	Low
Security	Could lead to incorrect access to exclusion areas (see [SP 800-116])	Could lead to incorrect access to limited areas (see [SP 800-116])	Could lead to incorrect access to controlled areas (see [SP 800-116])
Operations	Unable to manage or use the PACS to the extent that PACS use is severely diminished, inconvenient, or unreliable	Unable to manage or use the PACS to the extent that PACS use is seriously diminished, inconvenient, or unreliable	Unable to manage or use the PACS to the extent that PACS use is slightly diminished or inconvenient
Availability	The PACS is down for significant lengths of time, precluding entry into facilities/areas during that time	The PACS is down frequently for limited lengths of time, precluding entry into facilities/areas during those somewhat frequent times	The PACS is down infrequently for limited lengths of time, precluding entry into facilities/areas during those times

8 Functional Requirements and Test Cases Matrix

Table 8 - Functional Requirements and Test Cases Matrix

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
	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		
SR-1	2.01.01	46	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
SR-1	2.01.02	54	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
SR-1	2.01.03	46	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
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
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
	2.02			Certificate Validity Periods		
SR-3	2.02.01	46	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
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
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
SR-1	2.02.04	46	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
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
	2.03			Name Chaining		
SR-1	2.03.01	46	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	Registration fails.	PIA-3.2, PIA-5

				match common name portion of subject's name in the previous intermediate certificate.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
	2.04			**Basic Constraints**		
SR-1	2.04.01	46	05	Verify product's ability to recognize when the intermediate CA certificate is missing Basic Constraints extension.	Registration fails.	PIA-3.2, PIA-5
SR-3	2.04.02	46	06	Verify product's ability to recognize when the Basic Constraints extension is present and critical in the intermediate CA certificate but the cA component is false.	Registration fails.	PIA-3.2, PIA-5
SR-3	2.04.03	46	07	Verify product's ability to recognize when the Basic Constraints extension is present and not critical in the intermediate CA certificate but the cA component is false.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.04.04	46	08	Verify product's ability to recognize when the first certificate in the path includes Basic Constraints 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
SR-3	2.04.06	81	33	Verify product's ability to detect a mismatched AKID with the authority (issuer) public key in the Auth certificate.	Registration fails.	PIA-3.2, PIA-5
SR-3	2.04.07	60	62	Verify product's ability to detect a mismatched SKID with the EE public key in the Auth Certificate.	Registration fails.	PIA-3.2, PIA-5
	2.05			**Key Usage Verification**		
SR-1	2.05.01	46	09	Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which *keyCertSign* is false.	Registration fails.	PIA-3.2, PIA-5
SR-3	2.05.02	46	10	Verify product's ability to recognize when the intermediate certificate includes a non-critical Key Usage extension and rejects the path because a CA's Key Usage extension must always be marked critical.	Registration fails.	PIA-3.2, PIA-5, [PROF] Worksheet 3
SR-1	2.05.03	46	11	Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which *crlSign* is false.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.05.04	46	NEW	Verify product's ability to recognize when intermediate certificate includes Key Usage extension *keyCertSign* and *crlSign* false, and Key Usage not critical.	Registration fails.	
SR-1	2.05.05	61	00	Verify product's ability to recognize when the PIV CHUID content signing certificate does not express EKU policy OID *id-PIV-content-signing* (2.16.840.1.101.3.6.7).	Registration fails.	[Common], PIA-3.2, PIA-5

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	2.05.06	62	00	Verify product's ability to recognize when the Secure Messaging Certificate Signer content signing certificate does not express EKU policy OID *id-PIV-content-signing* (2.16.840.1.101.3.6.7).	Registration fails.	[Common], PIA-3.2, PIA-5
	2.06			**Certificate Policies**		
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
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
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
SR-2	2.06.06	46	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
SR-1	2.06.07	46	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 the PIV 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
SR-1	2.06.08	46	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	Registration succeeds.	PIA-3.2, PIA-5

				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.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-1	2.06.09	46	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-contentSigning* (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5
SR-1	2.06.10	46	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
SR-1	2.06.11	46	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
SR-1	2.06.12	54	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 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
SR-1	2.06.13	54	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-cardAuth* (2.16.840.1.101.3.2.1.48.79) by the relying party solution.	Registration succeeds.	PIA-3.2, PIA-5
SR-1	2.06.14	54	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	Registration succeeds.	PIA-3.2, PIA-5

				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.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-1	2.06.15	54	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
SR-1	2.06.16	54	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
SR-1	2.06.17	54	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
SR-1	2.06.18	54	00	With trust anchor set to ICAM Test Card PIV Root CA, and the following policies are required: __*id-fpki-common-authentication* (2.16.840.1.101.3.2.1.3.13) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17) __*id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.3.39) and a valid PIV-I is presented.	Registration fails.	
SR-1	2.06.19	54	00	With trust anchor set to ICAM Test Card PIV-I Root CA, and the following policies are required: __*id-fpki-common-pivi-authentication* (2.16.840.1.101.3.2.1.48.83) __*id-fpki-common-pivi-cardAuth* (2.16.840.1.101.3.2.1.48.84) __*id-fpki-common-pivi-contentSigning* (1.2.3.4) and a PIV-I is presented.	Registration fails.	
	2.07			**Generalized Time**		

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-3	2.07.01	46	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
SR-3	2.07.02	46	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
	2.08			**Name Constraints**		
SR-1	2.08.01	46	00	The system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Registration succeeds.	PIA-3.2, PIA-5
SR-1	2.08.02	46	13	The system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.08.03	46	14	The system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree.	Registration fails.	PIA-3.2, PIA-5
	2.09			**Certificate Revocation Tests (CRL)**		
SR-1	2.09.01	46	15	The system recognizes when no revocation information is available for the End Entity certificate.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.02	46	16	The system recognizes when a second intermediate CA certificate is revoked.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.03	24	00	The system recognizes when the End Entity certificate is revoked.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.04	46	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
SR-1	2.09.05	46	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
SR-3	2.09.06	46	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
SR-1	2.09.07	46	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
SR-1	2.09.08	46	17	The system recognizes when the CRL has an invalid signature.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-2	2.09.09	46	34	The system recognizes when an incorrectly formatted CRL is present in the path.	Registration fails.	PIA-3.5, PIA-5, PIA-7

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	2.09.10	46	36	The system recognizes when an invalid CRL signer is in the path.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.11	58	00	The system recognizes when the Card Authentication Certificate is revoked.	Registration fails.	[SP 800-73], PIA-3, PIA-3.2
SR-1	2.09.12	58	00	The system recognizes when: 1. the end-entity PIV Authentication Certificate is not expired or revoked 2. the end-entity Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available.	Registration fails.	[SP 800-73], PIA-3, PIA-3.2
	2.10			**CHUID Verification**		
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
SR-2	2.10.02	09	00	The system recognizes when the CHUID signer certificate is expired.	Registration fails.	PIA-3.6, PIA-5
SR-1	2.10.03	14	00	The system recognizes when the CHUID is expired.	Registration fails.	PIA-3.6
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
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
SR-1	2.10.06	11	00	The system recognizes when the PIV-AUTH certificate expires after the CHUID expiration date.	Registration fails.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	2.10.08	46	03	The system recognizes when an intermediate certificate in the CHUID signer certificate path is expired.	Registration fails.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	2.10.09	46	16	The system recognizes when an intermediate certificate in the CHUID signer certificate path is revoked.	Registration fails.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	2.10.10	57	0	The system recognizes when the CHUID signer certificate is revoked.	Registration fails.	PIA-3, PIA-3.2
	2.11			**Facial Image Verification**		
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
SR-2	2.11.02	49	00	The system recognizes when the Facial Image CBEFF is expired.	Registration fails.	[SP 800-76]
UO-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]

	2.12			Copied Containers		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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
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
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
SR-1	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
	2.13			Fingerprint Verification		
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
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
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
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
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
SR-2	2.13.07	51	00	The system recognizes when the Cardholder Fingerprints CBEFF is expired.	Registration fails.	[SP 800-76]
UO-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]
	2.14			Security Object Verification		
SR-2	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
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
SR-1	2.14.03	55	00	The system recognizes when a credential is missing the Security Object or the length of the Security Object is zero.	Registration fails.	[SP800-73] Part 1
	2.15			OCSP Response Checking		

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	2.15.01	46	00	The system successfully validates a good credential using an OCSP response with a good signature.	Registration succeeds.	PIA-3.2, PIA-3.5
SR-2	2.15.02	42	00	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
SR-3	2.15.03	43	00	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
SR-2	2.15.04	44	00	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
SR-1	2.15.05	45	00	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
SR-1	2.15.06	45	00	The system recognizes when: 1. the end-entity PIV Authentication Certificate is not expired or revoked 2. the Card Authentication Certificate is not expired but is revoked; AIA to OCSP is available and crlDP to CRL is not available.	Registration fails.	PIA-3.2, PIA-4
	2.16			**Interoperability Testing**		
SR-1	2.16.01	Valid PIV and PIV-I	Common Policy Root	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.	Registration succeeds.	PIA-6
SR-1	2.16.02	39	37	The system recognizes a Federally-issued PIV-I card with a FASC-N that does not begin with fourteen 9s and treats the credential as a PIV-I throughout the system. The primary identifier for the cards is the CHUID GUID.	Registration succeeds.	PIA-6
SR-1	2.16.03	54	00	The system recognizes a Federally-issued PIV-I card with a FASC-N that begins with fourteen 9s.	Registration succeeds.	PIA-6
SR-3	2.16.04	46	00	The system recognizes when the Extended Key Usage extension keyPurposeId OID *id-PIV-content-signing* (2.16.840.1.101.3.6.7) is present in the content signing certificate.	Registration succeeds.	[FIPS 201]
SR-3	2.16.05	46	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-PIV-content-signing* (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Registration fails.	[FIPS 201]
SR-3	2.16.06	54	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.	Registration succeeds.	[FIPS 201]
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**

SR-3	2.16.07	54	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-fpki-pivi-content-signing* (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.	Registration fails.	[FIPS 201]
SR-3	2.16.08	46	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.	Registration succeeds.	[FIPS 201]
SR-3	2.16.09	46	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-PIV-cardAuth* (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Registration fails.	[FIPS 201]
SR-3	2.16.10	54	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.	Registration succeeds.	[FIPS 201]
SR-3	2.16.11	54	00	The system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-PIV-cardAuth* (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Registration fails.	[FIPS 201]
SR-1	2.16.13	47	00	A FIPS 201-2 card can be registered with the *pivFASC-N* positioned after the *entryUUID* in the *GeneralNames* sequence within the Subject Alternative Names extension of the PIV Authentication certificate.	Registration succeeds.	[FIPS 201]
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]]
SR-1	2.16.15	Valid PIV	Common Policy Root	Various valid PIV cards can be individually registered. Trust anchor set to Common Policy Test Root, and the following policies are required: __id-fpki-common-authentication (2.16.840.1.101.3.2.1.48.11) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.48.13) __id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86)	Registration succeeds.	PIA-6
SR-1	2.16.16	Valid CAC	Common Policy Root	Various valid CAC cards can be individually registered. Trust anchor set to Common Policy Root, and the following policies are required: __*id-fpki-common-authentication* (2.16.840.1.101.3.2.1.3.13) __*id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.3.39) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17) (When applicable)	Registration succeeds.	PIA-6
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**

SR-1	2.16.17	Valid PIV-I	Common Policy Root	Various valid PIV-I cards can be individually registered. Trust anchor set to Common Policy Test Bridge, and the following policies are required: __id-fpki-common-pivi-authentication (2.16.840.1.101.3.2.1.48.78) __id-fpki-certpcy-pivi-cardAuth (2.16.840.1.101.3.2.1.48.79) __id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.48.80)	Registration succeeds.	PIA-6
SR-1	2.16.18	63	Common Policy Root	Various valid PIV cards can be individually registered. SM-AUTH present OCC-AUTH present Trust anchor set to Common Policy Test Root, and the following policies are required: __id-fpki-common-authentication (2.16.840.1.101.3.2.1.48.11) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.48.13) __id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86)	Registration succeeds.	PIA-6
SR-1	2.16.19	Valid Test CAC	Common Policy Root	Various valid CAC cards can be individually registered. SM-AUTH present OCC-AUTH present Trust anchor set to Common Policy Root, and the following policies are required: __id-fpki-common-authentication (2.16.840.1.101.3.2.1.3.13) __id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.3.39) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17) (When applicable)	Registration succeeds.	PIA-6
SR-1	2.16.20	64	Common Policy Root	Various valid PIV-I cards can be individually registered. SM-AUTH present OCC-AUTH present Trust anchor set to Common Policy Test Bridge, and the following policies are required: __id-fpki-common-pivi-authentication (2.16.840.1.101.3.2.1.48.78) __id-fpki-certpcy-pivi-cardAuth (2.16.840.1.101.3.2.1.48.79) __id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.48.80)	Registration succeeds.	PIA-6

	2.17			Cryptography Testing		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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 3-3; [Common] §6.1.5
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
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
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
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
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
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
	2.18			**Discovery Object and PIN Usage Policy**		
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
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 10. (E-PACS is using the Application PIN).	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1
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
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
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**

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
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
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
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
	2.20			**SM and OCC-AUTH**		
	4.0			**Requirements for Automated Provisioning, Deprovisioning, and Modifications, In Accordance With [E-PACS] PIA-8**		
UR-2	4.01.01			The E-PACS shall accept automated provisioning using APL data model 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
UR-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
UR-2	4.01.03			The E-PACS shall accept automated record modifications (e.g., certificates) using APL data model 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
SR-1	4.01.04			The E-PACS shall support a secure channel (e.g., mutual-auth over TLS) for all transactions with the trusted source.	Design analysis passes.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94
	5.0			**Authentication at Time of Access Test Cases**		
	5.01			**Signature Verification**		

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.01.01	46	00	With ICAM Test Card 46 registered with the PACS, 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
SO-1	5.01.02	54	00	With ICAM Test Card 54 registered with the PACS, 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
SR-1	5.01.03	46	01	With ICAM Test Card 46 registered with the PACS, 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
SR-1	5.01.04	05	00	With ICAM Test Card 01 registered with the PACS, 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
SR-1	5.01.05	23	00	With ICAM Test Card 01 registered with the PACS, verify product's ability to recognize certificate/private key mismatch.	Access denied.	PAI-3.2, PIA-3.4, PIA-4
SR-1	5.01.06	41	00	With ICAM Test Card 46 registered with the PACS, 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
	5.02			**Certificate Validity Periods**		
SR-3	5.02.01	46	02	With ICAM Test Card 46 registered with the PACS, verify product's ability to reject a credential when the *notBefore* date of the intermediate CA certificate is sometime in the future.	Access denied.	PIA-3.5, PIA-5
SR-2	5.02.02	12	00	With ICAM Test Card 01 registered with the PACS, 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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.02.03	46	03	With ICAM Test Card 46 registered with the PACS, verify product's ability to reject a credential when notAfter date of *any* certificate in the path is sometime in the past.	Access denied.	PIA-3.5, PIA-5
SR-1	5.02.04	13	00	With ICAM Test Card 01 registered with the PACS, 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
	5.03			**Name Chaining**		
SR-1	5.03.01	46	04	With ICAM Test Card 46 registered with the PACS, 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
	5.04			**Basic Constraints**		
SR-1	5.04.01	46	05	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the intermediate CA certificate is missing the Basic Constraints extension.	Access denied.	PIA-3.2, PIA-5
SR-3	5.04.02	46	06	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the Basic Constraints extension is present and critical in the intermediate CA certificate but the *cA* component is false.	Access denied.	PIA-3.2, PIA-5
SR-3	5.04.03	46	07	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the Basic Constraints extension is present and not critical in the intermediate CA certificate but the *cA* component is false.	Access denied.	PIA-3.2, PIA-5
SR-1	5.04.04	46	08	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the first certificate in the path includes Basic Constraints 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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-3	5.04.06	46	33	With ICAM Test Card 46 registered with the PACS, 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
	5.05			**Key Usage Verification**		
SR-1	5.05.01	46	09	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which keyCertSign is false.	Access denied.	PIA-3.2, PIA-5
SR-3	5.05.02	46	10	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the intermediate certificate includes a non-critical Key Usage extension and rejects the path because a CA's Key Usage extension must always be marked critical.	Access denied.	PIA-3.2, PIA-5, [PROF] Worksheet 3
SR-1	5.05.03	46	11	With ICAM Test Card 46 registered with the PACS, verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which crlSign is false.	Access denied.	PIA-3.2, PIA-5
SR-1	5.05.04	46	NEW	Verify product's ability to recognize when intermediate certificate includes Key Usage extension *keyCertSign* and *crlSign* false, and Key Usage not critical.	Access denied.	PIA-3.2, PIA-5
	5.06			**Certificate Policies**		
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
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
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	Access denied.	PIA-3.2, PIA-5

				does not map to the end entity certificate such as *id-fpki-common-High* (2.16.840.1.101.3.2.1.3.16).		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-2	5.06.06	46	12	With ICAM Test Card 46 registered with the PACS, and 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
SR-1	5.06.07	46	00	With ICAM Test Card 46 registered with the PACS, and 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 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
SR-1	5.06.08	46	00	With ICAM Test Card 46 registered with the PACS, and 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
SR-1	5.06.09	46	00	With ICAM Test Card 46 registered with the PACS, and 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-contentSigning* (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.10	46	00	With ICAM Test Card 46 registered with the PACS, and 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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.06.11	46	00	With ICAM Test Card 46 registered with the PACS, and 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
SR-1	5.06.12	54	00	With ICAM Test Card 54 registered with the PACS, and 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 Authentication Certificates will be set to the CITE test OID for *id-fpki-common-pivi-authentication* (2.16.840.1.101.3.2.1.48.83) by the relying party solution.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.13	54	00	With ICAM Test Card 54 registered with the PACS, and 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-common-pivi-cardAuth* (2.16.840.1.101.3.2.1.48.84) by the relying party solution.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.14	54	00	With ICAM Test Card 54 registered with the PACS, and 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-common-pivi-contentSigning* (2.16.840.1.101.3.2.1.48.85) by the relying party solution.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.15	54	00	With ICAM Test Card 54 registered with the PACS, and 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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.06.16	54	00	With ICAM Test Card 54 registered with the PACS, and 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
SR-1	5.06.17	54	00	With ICAM Test Card 54 registered with the PACS, and 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
SR-1	5.06.18	54, 39	00	With trust anchor set to ICAM Test Card PIV Root CA, and the following policies are required: __*id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11) __*id-fpki-common-cardAuth* (2.16.840.1.101.3.2.1.48.13) __*id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.48.86) and a valid PIV-I is presented.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.19	54	00	With trust anchor set to ICAM Test Card PIV-I Root CA, and the following policies are required: __*id-fpki-common-pivi-authentication* (2.16.840.1.101.3.2.1.48.83) __*id-fpki-common-pivi-cardAuth* (2.16.840.1.101.3.2.1.48.84) __*id-fpki-common-pivi-contentSigning* (2.16.840.1.101.3.*1.2.3.4*) and a PIV-I is presented.	Access denied.	PIA-3.2, PIA-5
	5.07			**Generalized Time**		
SR-3	5.07.01	46	24	With ICAM Test Card 46 registered with the PACS, verify product's ability to process valid use of generalized time post year 2049 in the path.	Access granted.	PIA-3.2, PIA-5
SR-3	5.07.02	46	25	With ICAM Test Card 46 registered with the PACS, verify product's ability to process invalid use of generalized time before year 2049 in the path.	Access denied.	PIA-3.2, PIA-5
	5.08			**Name Constraints**		
SR-1	5.08.01	46	00	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the intermediate certificate includes a Name	Access granted.	PIA-3.2, PIA-5

				Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-1	5.08.02	46	13	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Access denied.	PIA-3.2, PIA-5
SR-1	5.08.03	46	14	The system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree.	Access denied.	PIA-3.2, PIA-5
	5.09			**Certificate Revocation Tests (CRL)**		
SR-1	5.09.01	46	15	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when no revocation information is available for the End Entity certificate.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.02	46	16	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when a second intermediate CA certificate is revoked.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.03	24	00	The system recognizes when the End Entity certificate is revoked.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.04	46	17	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the CRL has an invalid signature.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.05	46	18	With ICAM Test Card 46 registered with the PACS, verify 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
SR-1	5.09.06	46	19	With ICAM Test Card 46 registered with the PACS, verify 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
SR-3	5.09.07	46	20	With ICAM Test Card 46 registered with the PACS, verify 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
SR-1	5.09.08	46	21	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when a certificate in the path has an incorrect CRL distribution point.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.09	46	34	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when an incorrectly formatted CRL is present in the path.	Access denied.	PIA-3.5, PIA-5, PIA-7

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.09.10	46	36	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when an invalid CRL signer is in the path.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.11	58	00	The system recognizes when the Card Authentication Certificate is revoked.	Access denied.	[SP 800-73], PIA-3, PIA-3.2
SR-1	5.09.12	58	00	The system recognizes when: 1. the end-entity PIV Authentication Certificate is not expired or revoked 2. the end-entity Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available.	Access denied.	[SP 800-73], PIA-3, PIA-3.2
	5.10			**Content Signer Verification**		
SR-1	5.10.1	57	00	The system recognizes when the CHUID signer certificate is revoked. Access method: PKI-AUTH	Access denied.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
	5.12			**Fingerprint Verification**		
SR-1	5.12.01	07	00	With ICAM Test Card 07 personalized with the tester's fingerprints and ICAM Test Card 01 registered with the PACS, the system recognizes when the Fingerprint signature is invalid and does not verify.	Access denied.	PIA-3, PIA-3.2, PIA-3.3, PIA-4
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
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
	5.14			**OCSP Response Checking**		
SR-1	5.14.01	46	00	With ICAM Test Card 46 registered with the PACS, verify the system successfully validates a good credential using an OCSP response with a good signature.	Access granted.	PIA-3.2, PIA-3.5
SR-2	5.14.02	42	00	With ICAM Test Card 42 registered with the PACS, verify that 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
SR-3	5.14.03	43	00	With ICAM Test Card 43 registered with the PACS, verify that validation succeeds using an OCSP Responder with a revoked signature certificate for a good credential with PKIX_OCSP_NOCHECK present.	Access granted.	PIA-3.2, PIA-3.5
SR-2	5.14.04	44	00	With ICAM Test Card 44 registered with the PACS, verify that validation fails using an OCSP Responder with a revoked signature	Access denied.	PIA-3.2, PIA-3.5, PIA-3.6

				certificate for a good credential without PKIX_OCSP_NOCHECK present.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-1	5.14.05	45	00	With ICAM Test Card 45 registered with the PACS, verify that validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good credential.	Access denied.	PIA-3.2, PIA-4
SR-1	5.14.05	45	00	The system recognizes when: 1. the end-entity PIV Authentication Certificate is not expired or revoked 2. the Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available.	Access denied.	PIA-3.2, PIA-4
	5.15			**Interoperability Testing**		
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
SR-1	5.15.02	39	37	With ICAM Test Card 39 registered with the PACS, verify the system recognizes a Federally-issued PIV-I card with a FASC-N that does not begin with fourteen 9s and treats the credential as a PIV-I throughout the system. The primary identifier for the cards is the CHUID GUID.	Access granted.	PIA-6
SR-1	5.15.03	54	00	With ICAM Test Card 54 registered with the PACS, verify the system recognizes a Federally-issued PIV-I card with a FASC-N that begins with fourteen 9s.	Access granted.	PIA-6
SR-3	5.15.04	46	00	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the Extended Key Usage extension *keyPurposeId* OID *id-PIV-content-signing* (2.16.840.1.101.3.6.7) is present in the content signing certificate.	Access granted.	[FIPS 201]
SR-3	5.15.05	46	00	With ICAM Test Card 46 registered with the PACS, verify 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]
SR-3	5.15.06	54	00	With ICAM Test Card 54 registered with the PACS, verify 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]
SR-3	5.15.07	54	00	With ICAM Test Card 54 registered with the PACS, verify the system recognizes when an explicit Extended Key Usage extension	Access denied.	[FIPS 201]

				keyPurposeId OID (e.g., 1.2.3.4.5.6.7) is not present in the content signing certificate.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-3	5.15.08	46	00	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the Extended Key Usage extension *keyPurposeId* OID (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Access granted.	[FIPS 201]
SR-3	5.15.09	46	00	With ICAM Test Card 46 registered with the PACS, verify 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]
SR-3	5.15.10	54	00	With ICAM Test Card 54 registered with the PACS, verify 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]
SR-3	5.15.11	54	00	With ICAM Test Card 54 registered with the PACS, verify the system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-PIV-cardAuth* (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate.	Access denied.	[FIPS 201]
SR-1	5.15.13	47	00	With ICAM Test Card 47 registered with the PACS, FIPS 201-2 card results in an access granted decision using PKI-AUTH method with the *pivFASC-N* positioned after the *entryUUID* in the *GeneralNames* sequence within the Subject Alternative Names extension of the PIV Authentication certificate.	Access granted.	[FIPS 201]
SR-1	5.15.14	53	00	With ICAM Test Card 53 registered with the PACS, verify the system successfully handles cards with a slightly larger than recommended Card Authentication Certificate (2160 bytes).	Access granted.	[SP800-73]
SR-1	5.15.15	63	Common Policy Root	Various valid PIV cards support use of PKI-CAK, PKI-AUTH, PKI-CAK+BIO, PKI-AUTH+BIO, SM-AUTH (Cipher suite '27' and '2E'), OCC-AUTH. Trust anchor set to Common Policy Test Root, and the following policies are required: __id-fpki-common-authentication (2.16.840.1.101.3.2.1.48.11) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.48.13) __id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86)	Access granted.	PIA-6

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.15.16	Valid Test CAC	Common Policy Root	Various valid CAC cards support use of PKI-CAK, PKI-AUTH, PKI-CAK+BIO, PKI-AUTH+BIO, SM-AUTH (Cipher suite '27' and '2E'), OCC-AUTH. Trust anchor set to Common Policy Root, and the following policies are required: __id-fpki-common-authentication (2.16.840.1.101.3.2.1.3.13) __id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.3.39) __id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17) (When applicable)	Access granted.	PIA-6
SR-1	5.15.17	64	Common Policy Root	Various valid PIV-I cards support use of PKI-CAK, PKI-AUTH, PKI-CAK+BIO, PKI-AUTH+BIO, SM-AUTH (Cipher suite '27' and '2E'), OCC-AUTH. Trust anchor set to Common Policy Test Bridge, and the following policies are required: __id-fpki-common-pivi-authentication (2.16.840.1.101.3.2.1.48.78) __id-fpki-certpcy-pivi-cardAuth (2.16.840.1.101.3.2.1.48.79) __id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.48.80)	Access granted.	PIA-6
SR-1	5.16.02	NIST #1	NIST Root	With NIST Test Card #1 registered with the PACS, verify Product's ability to validate signatures using SHA-256 and RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
SO-3	5.16.05	NIST #2	NIST Root	With NIST Test Card #2registered with the PACS, 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
SR-1	5.16.07	NIST #4	NIST Root	With NIST Test Card #4 registered with the PACS, 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
SO-3	5.16.08	NIST #5	NIST Root	With NIST Test Card #5 registered with the PACS, 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
SR-1	5.16.10	NIST #1	NIST Root	With NIST Test Card #1 registered with the PACS, verify Product's ability to validate signatures using SHA-256.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5
SO-3	5.16.11	NIST #5	NIST Root	With NIST Test Card #5 registered with the PACS, verify Product's ability to validate signatures using SHA-384.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.16.12	NIST #1	NIST Root	With NIST Test Card #1 registered with the PACS, verify Product's ability to validate signatures using SHA-256 and RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	Access granted.	[SP800-78] Table 3-2
	5.17			**Discovery Object and PIN Usage Policy**		
SR-2	5.17.01	25	00	Register ICAM Test Card 25 (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
SR-2	5.17.02	25	00	Register ICAM Test Card 25 (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 10. (E-PACS is using the Application PIN).	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.17.03	26	00	Register ICAM Test Card 26 (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
SR-2	5.17.04	26	00	Register ICAM Test Card 26 (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
SR-2	5.17.05	27	00	Register ICAM Test Card 27 (Discovery object is present and 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
SR-2	5.17.07	27	00	Register ICAM Test Card 27 (Discovery object is present and PIV App 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
SR-2	5.17.10	28	00	Register ICAM Test Card 28 (Discovery object is present and PIV App and Global PINs are available, and 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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-2	5.17.15	28	00	Register ICAM Test Card 28 (Discovery object is present and PIV App and Global PINs are available, and 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
	5.18			**ISO 7816-3 2006 PPS Protocol Compliance**		
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]
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]
	5.19			**SM and OCC-AUTH**		
SR-1	5.19.1	63	00	Reader set to SM-AUTH mode. Verify Product's ability to verify SM-AUTH using ciphersuite '27'. The explicit policy for Secure Messaging Content Signer contentSigning certificate will be set to the CITE test OID for id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access granted.	[800-73] Part2, PIA-6
SR-1	5.19.10	72	00	Reader set to SM-AUTH mode. Verify product's ability to reject a credential when the CVC's issuer identification number does not match the subjectKeyIdentifier in the contentSigning certificate when no intermediate CVC is present.	Access denied.	[800-73] Part2
SR-1	5.19.11	73	00	Reader set to SM-AUTH mode. Verify product's ability to reject a credential when the Intermediate CVC's issuer identification number does not match the subjectKeyIdentifier in the contentSigning certificate.	Access denied.	[800-73] Part2
SR-1	5.19.12	74	00	Reader set to SM-AUTH mode. Verify product's ability to reject a credential when the CVC's issuer identification number does not match the subjectKeyIdentifier in the intermediate CVC.	Access denied.	[800-73] Part2
SR-1	5.19.13	75	00	Reader set to SM-AUTH mode.	Access denied.	PIA-6

				Verify product's ability to reject credential when Secure Messaging Content Signer contentSigning certificate is expired. The explicit policy for Secure Messaging Content Signer contentSigning certificate will be set to the CITE test OID for id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86) by the relying party solution.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
SR-1	5.19.14	76	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when Secure Messaging Content Signer contentSigning certificate is revoked. The explicit policy for Secure Messaging Content Signer contentSigning certificate will be set to the CITE test OID for id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access denied.	PIA-6
SR-1	5.19.15	77	00	Reader set to SM-AUTH mode. Verify product's ability to recognize when the Secure Messaging Certificate Signer contentSigning certificate does not express EKU policy OID 2.16.840.1.101.3.6.7 for content-signers.	Access denied.	PIA-6
SR-1	5.19.16	78	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when Secure Messaging Content Signer contentSigning certificate contains policy '1.2.3.4.5.6'. The explicit policy for Secure Messaging Content Signer contentSigning certificate will be set to the CITE test OID for *id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access denied.	PIA-6
SR-1	5.19.17	79	00	Reader set to OCC-AUTH mode (requires SM). Verify product's ability to reject credential when Biometric Information Templates Group Template (buffer 0x1016) is empty.	Access denied.	[800-73] Part1
SR-1	5.19.18	80	00	Reader set to OCC-AUTH mode (requires SM). Verify product's ability to reject credential when Biometric Information Templates Group Template (buffer 0x1016) contains '7F 61 03 02 01 00'.	Access denied.	[800-73] Part2

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.19.19	65	00	Reader set to OCC-AUTH mode (requires SM). Verify Product's ability to accept a OCC fingerprint matching either fingerprint keyref tags '96' or '97'.	Access granted.	[800-73] Part2
SR-1	5.19.2	65	00	Reader set to SM-AUTH mode. Verify Product's ability to verify SM-AUTH using ciphersuite '2E'. The explicit policy for Secure Messaging Content Signer contentSigning certificate will be set to the CITE test OID for id-fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.48.86) by the relying party solution.	Access granted.	[800-73] Part2, PIA-6
SR-1	5.19.20	65	00	Reader set to OCC-AUTH mode (requires SM). Verify Product's ability to reject a valid credential when non-matching OCC fingerprint is presented for fingerprint keyref tags '96' and '97'.	Access denied.	[800-73] Part2
SR-1	5.19.3	66	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when PIV Application Property Template Tag '61' does not contain Tag 'AC'.	Access denied.	[800-73] Part2
SR-1	5.19.4	67	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when PIV Application Property Template Tag '61' contains Tag 'AC' but it does not contain a tag '80' reference of '27' or '2E'.	Access denied.	[800-73] Part2
SR-1	5.19.5	1	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when buffer 0x1017 is not present.	Access denied.	[800-73] Part1
SR-1	5.19.6	68	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when buffer 0x1017 is empty.	Access denied.	[800-73] Part1
SR-1	5.19.7	69	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when buffer 0x1017 does not contain tag 0x70.	Access denied.	[800-73] Part1
SR-1	5.19.8	70	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when buffer 0x1017 tag 0x70 is empty.	Access denied.	[800-73] Part1

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
SR-1	5.19.9	71	00	Reader set to SM-AUTH mode. Verify product's ability to reject credential when Secure Messaging General Authenticate against keyref '04' using ciphersuite '2E' does not result in final SW1='90'.	Access denied.	[800-73] Part2
	7.0			**PACS Design Use Cases**		
	7.01			**Continuity of Operations Testing**		
UO-3	7.01.01	46	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
UO-3	7.01.02	46	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
UO-3	7.01.03	46	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
UO-3	7.01.04	5	01	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
UO-3	7.01.05	5	01	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
UO-3	7.01.06	5	01	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
UO-3	7.01.07	23	00	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a cloned credential.	Design analysis passes.	PCP-1
	7.02			**Security Boundaries**		

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
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
SO-1	7.02.02			Specific waivers to TC# 7.02.01 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
	7.03			**Registering Physical Access Privileges**		
UO-3	7.03.01			Shall be able to define populations (validities) such as "guest, visitor, regular access".	Design analysis passes.	PPL-4
UO-3	7.03.02			Shall be able to define: Access points for each population.	Design analysis passes.	PPL-5, PAC-1
UO-3	7.03.03			Shall be able to define: Temporal access rules for each population.	Design analysis passes.	PPL-5, PAC-1
UO-3	7.03.04			Shall be able to define: Authentication mode required to support 7.03.02 and 7.03.03.	Design analysis passes.	PPL-5, PAC-1
	7.04			**PKI Configuration**		
SO-1	7.04.01			The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name	Verify configurability of	PIA-5

				constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	X.509 constraints and policies.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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
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.	
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.	
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.	

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
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
	7.05			**Credential Number Specifications**		
UO-3	7.05.01	46		The solution should 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
UO-3	7.05.02	54		The solution should 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,	PAU-2, PAU-3; Table 6-1 row 3

					the details shall be provided to the GSA ICAM Lab for testing purposes.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
	7.06			**Validation at Time of Access**		
UO-1	7.06.02	46	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
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
UO-1	7.06.04	46	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
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
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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
UO-1	7.06.09	46	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
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
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
	7.07			**Portal Hardware**		
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	PCM-2, PCM-3

					authentication testing.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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
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
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
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	PCM-3

					Test card 1: PIV Golden for access according to mode.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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
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
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	PCM-3

					Golden for access according to mode.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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]
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	[FIPS 201]

					review and approval.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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]
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]
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
	7.08			**Auditing and Logging**		
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
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
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
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
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
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

Classifi-cation	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source
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
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
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
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
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
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
	7.09			**Security Certification and Accreditation**		
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
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
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
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	PCA-3

					FIPS 201 Evaluation Program.	
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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]
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]
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]
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]
	7.10			**Biometric in PACS**		
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
	7.11			**Operational Controls**		
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
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
UO-3	7.11.03			The system shall have the ability to manage the system through software controlled configuration management methods. Initial	Verify by use of the system.	PCM-2

				configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.		
Classifi-cation	**TC#**	**Card #**	**Path #**	**Description/Test Case Procedure**	**Expected Result**	**Requirement Source**
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
UO-3	7.11.05			The system shall support configuration downloads to relevant components.	Verify by setting up of system.	PCM-2
	7.12			**Accessibility**		
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]

9 Deprecated Test Cases

The table below lists test cases that have been deprecated from the FRTC in 1.3.3 Rev. G. These tests have become obsolete. Some have been replaced with another test case. Test cases for a particular security risk may have been mitigated by another technology or standard. Note that these are not cumulative. Refer to previous versions of the FRTC for other deprecated test cases.

Table 9 – Test Cases Deprecated in FRTC 1.3.3 Rev. G

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
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	Because some agencies use a different hashing method for computing SKIDs, SHA-1 can no longer be required.
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	This is an unrealistic scenario that will never occur in the real world.

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
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	This is an unrealistic scenario that will never occur in the real world.
SR-1	2.17.14	46	35	Verify product's ability to validate signatures using RSA 4096 in the path.	Registration succeeds.	Derived from [SP800-78] Table 3-2	RSA 4096 was deprecated by FIPS 186-3 and subsequently SP 800-78-2.
SR-1	2.18.06	27	00	Discovery object is present. PIV App and Global PINs are available. PIV Application PIN is primary. Enter invalid Global PIN (e.g., 999999). Confirm PIV Application PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (4).	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Application PIN is primary, then the E-PACS should use the Application PIN. Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
SR-2	2.18.08	27	00	Enter valid Global PIN. Confirm PIV Application PIN retry counter remains 5. Confirm Global PIN retry counter is reset to 5.	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Application PIN is primary, then the E-PACS should use the Application PIN and the tester will observe that the E-PACS is using the PIV Application PIN. Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.
SR-2	2.18.09	28	00	Enter invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (4). Confirm Global PIN retry counter remains at 5.	Registration fails.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If the Global PIN is primary, then the E-PACS will fail to register not because the PIV Application PIN is incorrect, but because the Global PIN is incorrect, which means that the Global PIN retry counter will be decremented rather than the PIV Application PIN retry counter. Discovery object is present. PIV App and Global PINs

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
							are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.
SR-2	2.18.11	28	00	Enter valid PIV Application PIN. Confirm PIV Application PIN retry counter is reset to 5. Confirm Global PIN retry counter remains at 4.	Registration succeeds.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Global PIN is primary, then the E-PACS will use the Global PIN and the tester should confirm that the E-PACS is using the Global PIN. Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.
SR-1	5.02.05	10	00	With ICAM Test Card 01 registered with the PACS, 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	

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
SR-3	5.04.05	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	Because some agencies use a different hashing method for computing SKIDs, SHA-1 can no longer be required.
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.	Registration succeeds.	PIA-3.2, PIA-5	This is an unrealistic scenario that will never occur in the real world.
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.	Registration fails.	PIA-3.2, PIA-5	This is an unrealistic scenario that will never occur in the real world.

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
UO-1	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	No PACS or validation system is currently required to verify facial image signatures at time-of-access.
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	Not feasible to tamper with a valid PIV card.
SR-3	5.13.01	08	00	The system recognizes when the Security Object signature is invalid and does not verify.	Access denied.	PIA-3.4, PIA-4, PIA-5	Deprecated in 1.3.3. Access control decisions at time of access are based on signed objects on the card. A security object signature verification at time of access adds no value. Security object signature can be valid while containers can be manipulated.
SR-1	5.16.14	46	35	Verify product's ability to validate signatures using RSA 4096 in the path.	Access granted.	Derived from [SP800-78] Table 3-2	RSA 4096 was deprecated by FIPS 186-3 and subsequently SP 800-78-2.

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
SO-2	5.17.06	27	00	Enter invalid Global PIN (e.g., 999999). Confirm PIV App PIN retry counter remains at 4. Confirm Global PIN retry counter is decremented by one (4).	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Application PIN is primary, then the E-PACS should use the Application PIN. Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.
SO-2	5.17.08	27	00	Enter valid Global PIN. Confirm PIV App PIN retry counter remains 5. Confirm Global PIN retry counter is reset to 5.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Application PIN is primary, then the E-PACS should use the Application PIN and the tester will observe that the E-PACS is using the PIV Application PIN. Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
SR-2	5.17.09	28	00	Enter invalid PIV App PIN (e.g., 999999). Confirm PIV App PIN retry counter is decremented by one (4). Confirm Global PIN retry counter remains at 5.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If the Global PIN is primary, then the E-PACS will fail to register not because the PIV Application PIN is incorrect, but because the Global PIN is incorrect, which means that the Global PIN retry counter will be decremented rather than the PIV Application PIN retry counter. Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.
SR-1	5.17.11	28	00	Enter valid PIV App PIN. Confirm PIV App PIN retry counter is reset to 5. Confirm Global PIN retry counter remains at 4.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. The Pass/Fail criteria is incorrect. If both PINs are available, and the Global PIN is primary, then the E-PACS will use the Global PIN and the tester should confirm that the E-PACS is using the Global PIN. Discovery object is present. PIV App and Global PINs are available. Global PIN is

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
							primary. Confirm E-PACS is using the Application PIN.
SO-2	5.17.12	29	00	Enter invalid PIV App PIN (e.g., 999999). Confirm PIV App PIN retry counter is decremented to 4. Confirm Global PIN retry counter remains at 5.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. Impossible to create card with unpopulated 0x5F2F. PIV applet requires that tag 0x5F2F is populated. Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using the Application PIN.
SO-2	5.17.13	29	00	Enter valid Global PIN. Confirm PIV App PIN retry counter is decremented to 3. Confirm Global PIN retry counter remains at 5.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. Impossible to create card with unpopulated 0x5F2F. PIV applet requires that tag 0x5F2F is populated. Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using the Application PIN.
SO-2	5.17.14	29	00	Enter valid PIV App PIN. Confirm PIV App PIN retry counter is reset to 5. Confirm Global PIN remains at 5.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1	Deprecated in 1.3.3. Impossible to create card with unpopulated 0x5F2F. PIV applet requires that tag

Classification	TC#	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Comments
							0x5F2F is populated. Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using the Application PIN.
UO-1	7.06.07	01	00	Shall support PKI-CAK + BIO to PACS.	Use Authentication Test logs to verify that all good cards with valid BIO 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	NIST and OMB state that BIO to PACS is not a valid authentication factor.
UO-1	7.06.08	01	00	Shall support PKI-AUTH + BIO to PACS.	Use Authentication Test logs to verify that all good cards with valid BIO 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	NIST and OMB state that BIO to PACS is not a valid authentication factor.