

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



VERSION 1.4.2 Rev. D

---

**FIPS 201 EVALUATION PROGRAM**

---

August 21, 2025

Office of Government-wide Policy  
Office of Technology Strategy  
Identity Management Division  
Washington, DC 2040

## 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	<ul style="list-style-type: none"> <li>● 3/14/14 – First edit for errata.</li> <li>● 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.</li> <li>● 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.</li> <li>● 7/6/14 – Added Mobile Handheld Requirements.</li> </ul> <p>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).</p>	Public

Status	Version	Date	Comment	Audience
Final	1.3.1	7/28/2015	<ul style="list-style-type: none"> <li>Added Section 2.1, Addendums</li> <li>Added PPS entries 30-37 in Table 1</li> <li>Added Section 2.19, ISO 7816-3 2006 PPS Protocol Compliance</li> <li>Added Section 5.18, ISO 7816-3 2006 PPS Protocol Compliance</li> <li>Reworded 7.7.12 requirements statement</li> </ul>	Public
Final	1.3.1	8/18/2015	Fixed test case language for PPS Protocol Compliance.	Public
Final	1.3.3	9/8/2017	<ul style="list-style-type: none"> <li>Revised to synch with PACS FRTC v1.3.3.</li> <li>Updated links to online normative references.</li> <li>Added security classifications, severity level definitions, APL listing requirements.</li> <li>Reactivated 12 previously deprecated test cases, clarified 16, added 58, and deprecated 14 test cases.</li> <li>Biometric verification of cardholder is required at time of registration.</li> <li>Security Object verification is mandatory at time of registration.</li> </ul>	Public
Final	1.3.3 Rev A	9/18/2017	<ul style="list-style-type: none"> <li>Corrected typos.</li> <li>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.</li> <li>Added one (1) missing certificate policy test case for PIV Authentication at time of access.</li> </ul>	Public
Final	1.3.3 Rev B	11/3/2017	<ul style="list-style-type: none"> <li>Updated normative policy references for Federal Common Policy, FBCA, SSP, and PIV-I.</li> <li>Updated Discovery Object tests to reflect that max retries of test cards are set to 10, not 5.</li> <li>Added ICAM Test Card 54 (NFI PIV-I).</li> </ul>	Public
Final	1.3.3 Rev C	1/7/2018	<ul style="list-style-type: none"> <li>Replaced all instances of the use of ICAM Test Card #01 with ICAM Test Card 46.</li> <li>Replaced all instances of the use of ICAM Test Card #02 with ICAM Test Card 54.</li> <li>Corrected expected Global PIN retry counter, Test Cases 2.18.02 and 5.17.02.</li> <li>Added ICAM Test Card 55 (Missing Security Object) and Test Case 2.14.03.</li> <li>Clarified the expected result of Test Cases 2.16.02 and 5.15.02.</li> </ul>	Public

Status	Version	Date	Comment	Audience
Final	1.3.3 Rev. D	4/24/2018	<ul style="list-style-type: none"> <li>• Deprecated Test Cases 2.06.03, 2.06.04, 5.06.03., 5.06.04, and 5.11.01. (and removed Section 5.11).</li> <li>• For time-of-access fault path testing, included instructions as to which golden card must be registered with the PACS.</li> <li>• Activated ICAM Test Card 48 (PPS with LEN value greater than zero).</li> <li>• Corrected bit ordering of last 5 digits of example FASC-N in Credential Identifier Processing in Section 5.</li> <li>• Corrected card type from Card Authentication Certificate to PIV Authentication Certificate in Test Cases 2.06.07 and 5.06.07.</li> <li>• Added "Valid/Invalid" column to card description table.</li> <li>• Verified and updated links to normative references.</li> <li>• Clarified card type (PIV/PIV-I) for test cases 7.05.01 and 7.05.02</li> </ul>	Public
Final	1.3.3 Rev. E	6/21/2018	<ul style="list-style-type: none"> <li>• Deprecated Test Case 5.12.02</li> <li>• Clarified that Card 7 must be personalized with the testers biometric.</li> <li>• Removed Fault Paths 37-40</li> <li>• Deprecated Test Cases 8.01.01-8.10.04 (Handheld)</li> </ul>	Public
Final	1.3.3 Rev. F	8/21/2018	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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."</li> <li>• Deprecated Test Case 5.02.05 because Test Case 5.02.03 was updated to include all certificates in the path.</li> <li>• Added Test Cases 2.10.8 and 2.10.9 because Paths 3 and 16 can be used to test them.</li> </ul>	Public
Final	1.3.3 Rev. G	2/1/2019	<ul style="list-style-type: none"> <li>• Changed 5.15.04 to "With ICAM Test Card 46"</li> <li>• 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.</li> <li>• Replace "CHUID signature" with Card Authentication" in the description for Test Case</li> </ul>	Public

Status	Version	Date	Comment	Audience
			<p>5.06.13. We are testing for a Card Authentication certificate policy OID.</p> <ul style="list-style-type: none"> <li>• The description for Test Case 5.15.04 was changed to, "With ICAM Test Card 46...".</li> <li>• Added Test Cards 57, 58, and 59 and Test Cases 2.09.11, 2.10.10, 5.09.11, and 5.10.1</li> <li>• Changed Test Case 5.12.05 to " With ICAM Test Card 59 registered...".</li> <li>• Changed Test Case 5.14.05 to ".. To register ICAM Test Card 45...".</li> </ul>	
Final	1.4.2 Rev. A	3/31/2021	<ul style="list-style-type: none"> <li>• Incorporated test cases for Secure Messaging (SM) and On-Card Comparison (OCC). See SM-OCC Companion Paper.</li> <li>• Incorporated test cases for Backend Registration. See Backend Registration Companion Paper.</li> <li>• Consolidated test cases to accommodate FRTC express testing for previously tested solutions. See FRTC Express Companion Paper</li> </ul>	Public
Final	1.4.2 Rev B	10/15/2021	<ul style="list-style-type: none"> <li>• Reinstate section 8 test cases</li> <li>• Corrections of test case descriptions</li> <li>• Corrections of PKI paths used in testing</li> </ul>	Public
Final	1.4.2 Rev C	11/30/2023	<ul style="list-style-type: none"> <li>• Updated the document name to indicate "Guidance Document" for clarity and updates to Section 2, Tables 2, 4, 5, 6, 7, and 8.</li> </ul>	Public
Final	1.4.2 Rev D	08/21/2025	<ul style="list-style-type: none"> <li>• This is to add the updated FRTC workbook to this document.</li> <li>• The FRTC workbook as added deprecated and future test case tabs, along with giving each test case area their own tab.</li> <li>• Alignment of test case numbers between 2.0 and 5.0</li> </ul>	Public

## Table of Contents

1	Background .....	6
2	Change Control.....	6
3	Objectives.....	6
4	Test Instrumentation.....	7
4.1	ICAM Cards Used in Test.....	7
	Table 1 - ICAM Test Cards Used in Test.....	7
4.2	PKI Used in Test.....	12
	Table 2 - ICAM PKI Path Descriptions .....	12
5	Credential Number Processing.....	15
6	Normative References .....	16
7	Functional Requirements and Test Cases.....	19
7.1	Severity Levels.....	19
7.2	APL Listing Requirements .....	19
	Table 4 - APL listing based on Test Level and Classification .....	19
	Table 5 - Severity Remediation Timeframes .....	20
7.3	Classification Codes and Scoring Guidelines.....	20
	Table 6 - Classification Codes.....	20
	Table 7 - Impact Guidelines .....	21
	Table 8 – Possible Test Results.....	21
8	Functional Requirements and Test Cases Matrix.....	22
	Table 9 - Functional Requirements and Test Cases Matrix .....	22

## 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 across the Federal Government. As part of this responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program (EP) and its FIPS 201 Approved Products List (APL), along with services for Federal ICAM (FICAM) conformance and compliance.

## 2 Change Control

This document is a living document and will be updated over time as new or revised functional requirements are identified. Additionally, this document will be updated according to the following schedule:

1. A new version of the [PACS FRTC Topology Mapping Workbook.xlsx](#) will be published on IDManagement.gov if the existing test cases are updated and/or new test cases are added to ensure FICAM conformance and compliance.
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 that matches their assigned severity level (see Sections 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 published under [Program Announcements](#) on IDManagement.gov.

## 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 tests identify 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

The FIPS 201 Evaluation Program for PACS relies on fully defined, instrumented testing. This requires two core elements:

1. **ICAM Test Cards** – Two cards are entirely valid and well-formed test data. In addition, some cards 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 whole testing regimen, leveraging these test instruments, is described in Section 7.

### 4.1 ICAM Cards Used in Test

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

- Production 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/Invalid	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

ICAM Test Card	Valid/Invalid	Description	Threat Type
10	Invalid	Expired certificate signer	Invalid Date
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 <b>(PIV)</b>	Copied Credential
16	Invalid	Valid Card Authentication Certificate copied from one card to another <b>(PIV)</b>	Copied Credential
17	Invalid	Valid PHOTO copied from one card to another <b>(PIV)</b>	Copied Credential
18	Invalid	Valid FINGERPRINT copied from one card to another <b>(PIV)</b>	Copied Credential
19	Invalid	Valid CHUID copied from one card to another <b>(PIV-I)</b>	Copied Credential
20	Invalid	Valid Card Authentication Certificate copied from one card to another <b>(PIV-I)</b>	Copied Credential
21	Invalid	Valid PHOTO copied from one card to another <b>(PIV-I)</b>	Copied Credential
22	Invalid	Valid FINGERPRINT copied from one card to another <b>(PIV-I)</b>	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
28	Valid	Discovery object tag 0x5F2F is present First byte: 0x60, Second byte: 0x20	Application and Global PINs are present. Global PIN is

ICAM Test Card	Valid/Invalid	Description	Threat Type
			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
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 <i>id-pkix-ocsp-nocheck</i> 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 <i>id-pkix-ocsp-nocheck</i> 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

ICAM Test Card	Valid/ Invalid	Description	Threat Type
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
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

ICAM Test Card	Valid/Invalid	Description	Threat Type
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 crIDP 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 ECU 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
0	ICAM Valid Path	No Faults
1	ICAM Invalid CA Signature	Manipulated Data
2	ICAM Invalid CA <i>notBefore</i> Date	Revoked/Date Invalid
3	ICAM Invalid CA <i>notAfter</i> 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 <i>keyUsage keyCertSign</i> False	Standards Conformant Processing
10	ICAM <i>keyUsage</i> Not Critical	Standards Conformant Processing
11	ICAM <i>keyUsage</i> Critical <i>CRLSign</i> False	Standards Conformant Processing
12	ICAM Invalid <i>inhibitPolicyMapping</i>	Standards Conformant Processing
13	ICAM Invalid DN <i>nameConstraints</i>	Standards Conformant Processing
14	ICAM Invalid SAN <i>nameConstraints</i>	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 <i>nextUpdate</i>	Revoked/Date Invalid
20	ICAM Invalid CRL <i>notBefore</i>	Revoked/Date Invalid
21	ICAM Invalid CRL Distribution Point	Standards Conformant Processing
22	ICAM Valid <i>requiredExplicitPolicy</i>	Standards Conformant Processing

ICAM PKI Path Number	Fault description	Operational Group
23	ICAM Invalid <i>requiredExplicitPolicy</i>	Standards Conformant Processing
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

<b>ICAM PKI Path Number</b>	<b>Fault description</b>	<b>Operational Group</b>
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. Credential numbers are strongly advised not to 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.

**Table 3 – Minimal Set of Credential Number Processing Rules**

FASC-N Rule											
<b><u>PIV and CAC:</u></b>  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:  <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">1</td> <td style="width: 10%;">3</td> <td style="width: 10%;">4</td> <td style="width: 10%;">1 - 0</td> <td style="width: 10%;">0</td> <td style="width: 10%;">0</td> <td style="width: 10%;">1 - 9</td> <td style="width: 10%;">8</td> <td style="width: 10%;">7</td> <td style="width: 10%;">6</td> </tr> </table> 0001 0011 0100 0001-0000 0000 0000 0001-1001 1000 0111 0110	1	3	4	1 - 0	0	0	1 - 9	8	7	6
	1	3	4	1 - 0	0	0	1 - 9	8	7	6	
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">5</td> <td style="width: 10%;">4 - 1 - 1 - 1</td> <td style="width: 10%;">2</td> <td style="width: 10%;">3</td> <td style="width: 10%;">4</td> <td style="width: 10%;">5</td> <td style="width: 10%;">6</td> <td style="width: 10%;">7</td> <td style="width: 10%;">8</td> </tr> </table> 0101 0100-0001-0001-0001 0010 0011 0100 0101 0110 0111 1000	5	4 - 1 - 1 - 1	2	3	4	5	6	7	8		
5	4 - 1 - 1 - 1	2	3	4	5	6	7	8			
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											
<b><u>PIV and PIV-I:</u></b>  128 Bit UUID	16-byte binary representation of the UUID as defined by [RFC 4530].										

## 6 Normative References

- [ARCH] Federal Identity, Credential, and Access Management (FICAM) Architecture  
<https://www.idmanagement.gov/playbooks/>
- [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, or as amended,  
<fpki-x509-cert-policy-common.pdf> (idmanagement.gov)
- [E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0, March 26, 2014.  
<https://www.idmanagement.gov/docs/pacs-piv-epacs.pdf> (PIV in ePACS)
- [FBCA] X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), or as amended,  
[X.509 Certificate Policy For The Federal Bridge Certification Authority \(FBCA\) \(idmanagement.gov\)](X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) (idmanagement.gov))
- [FIPS 201] Federal Information Processing Standard 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors  
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf>
- [FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases  
<https://www.idmanagement.gov/docs/fips201ep-pacsfrtc.pdf>
- [HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004,  
<https://www.dhs.gov/homeland-security-presidential-directive-12>
- [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/wp-content/uploads/2019/05/M-19-17.pdf>
- [PIV-I] Personal Identity Verification Interoperable 101  
[Personal Identity Verification Interoperable 101 \(idmanagement.gov\)](Personal Identity Verification Interoperable 101 (idmanagement.gov))

- [PROF] Common Policy X.509 Certificate and Certificate Revocation list (CRL) Profiles, or as amended,  
<https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf>
- [RPL] Removed Process List (RPL) Process Document, v1.0.2, April 8, 2022  
<https://www.idmanagement.gov/docs/fips201ep-rplprocess.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, NIST Special Publication 800-73-5, July 2024 or as amended,  
<https://csrc.nist.gov/pubs/sp/800/73/pt1/5/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 800-78-5, July 2024, or as amended  
<https://csrc.nist.gov/pubs/sp/800/78/5/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  
<https://www.acquisition.gov/far/52.225-6>
- [UL 294] The Standard of Safety for Access Control System Units, UL Edition Number 8, May 24, 2023, Type ULSTD  
<https://www.shopulstandards.com/ProductDetail.aspx?productId=UL294>
- [UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number 6, April 6, 2018, and revised February 16, 2021, Type ULSTD, SUPERCEDED BY UL 2610 on July 9, 2025.  
<https://www.shopulstandards.com/ProductDetail.aspx?productId=UL1076>

- [UL 1981] The Standard for Central-Station Automation Systems UL Edition Number 3, Date October 10, 2014. Last revised March 29, 2023. Type ULSTD  
<https://www.shopulstandards.com/ProductDetail.aspx?productId=UL1981>
- [UL 2610] Commercial Premises Security Alarm Units and Systems Edition Number 2, Published April 7, 2021. Last revision January 31, 2023. Type ULSTD SUPERCEDED UL 1076 on July 9, 2025.  
[https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2610\\_2\\_S\\_20210407](https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2610_2_S_20210407)
- [VPAT] Voluntary Product Accessibility Template Version 2.4 Rev 508 – the U.S. Federal accessibility standard, March 2022  
[VPAT 2.4Rev 508 \(March 2022\)](#)

## 7 Functional Requirements and Test Cases

### 7.1 Severity Levels

If this document is 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 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 the classification of the test case and its severity level. For example, the program will not list a product that has a Severity 1 test case that failed.

In making an APL listing decision, the same evaluation criteria are used for required and vendor-supported optional functionality. **Note:** the vendor designates in their PACS Lab Application which test cases their product does not support.

**Table 4 - APL listing based on Test Level and Classification**

Test Level / Classification	Severity 1	List on APL?	Severity 2	List on APL?	Severity 3	List on APL?
<i>Security</i>	Pass	✓	Pass	✓	Pass	✓
	Fail	✗	Fail	✗	Fail	✓
<i>Usability</i>	Pass	✓	Pass	✓	Pass	✓
	Fail	✗	Fail	✗	Fail	✓

Table 5 specifies the remediation timeframes for each severity level. Products that fail to remediate within the specified timeframes are moved to the RPL. The cited impacts (High, Moderate, Low) are summarized in the table below.

**Table 5 - Severity Remediation Timeframes**

<i>Severity Level</i>	<i>Severity Description</i>	<i>New Product Remediation Timeframe</i>	<i>Existing Product Remediation Timeframe</i>
1	The identified problem has a <b>High Impact</b> on the security, PACS operations, PACS availability, or other area examined.		30 days
2	The identified problem results in a <b>Moderate Impact</b> on security, PACS operations, PACS availability, or other area examined.		90 days
3	The identified problem results in a <b>Low Impact</b> on the security, PACS operations, PACS availability, or other area examined.	1 year	1 year

**7.3 Classification Codes and Scoring Guidelines**

The FRTC includes a classification code for each test case. The classification code indicates that the test type for the requirement is *Security* or *Usability*. The Usability classification does not directly impact security. There is an additional classification code for whether the condition is *Required* or *Optional*. Table 6 describes the classification codes.

**Table 6 - Classification Codes**

<b>Classification Code</b>	<b>Description</b>
S	<b>Security</b> - A control directly impacting PACS security.
U	<b>Usability</b> - A control impacting PACS operations and availability.
R	<b>Required</b> - Must be present. Must work correctly.
O	<b>Optional</b> - May be present. If present, it must work correctly.
<i>Examples</i>	
Example: SR-2	<b>Security Required, Severity Level 2</b>
Example: UO-3	<b>Usability Optional, Severity Level 3</b>

**Table 7 - Impact Guidelines**

	<b>High Impact</b>	<b>Moderate Impact</b>	<b>Low Impact</b>
<b>Security</b>	Could lead to incorrect access to limited or exclusion areas (see [SP800-116])	Could lead to incorrect access to controlled areas (see [SP800-116])	Deny Access to controlled areas when it should be granted (see [SP800-116])
<b>Operations</b>	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
<b>Availability</b>	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

Each test case in *Table 9* must be accounted for in a Test Results Report. *Table 8* describes the possible test results each test case may have.

**Table 8 – Possible Test Results**

<b><i>Test Result</i></b>	<b><i>Description</i></b>
Pass	A test case whose actual results match expected results. Color coded <b>Green</b> in the Test Results Report.
Fail	A test case whose actual results do not match expected results. Color coded <b>Red</b> in the Test Results Report.
Not Supported	A test case the vendor has indicated is not supported. Color coded <b>Yellow</b> in the Test Results Report.
Not Tested	A test case the GSA PACS Lab has decided not to perform. Color coded <b>Yellow</b> in the Test Results Report.

## 8 Functional Requirements and Test Cases Matrix

Table 9 - Functional Requirements and Test Cases Matrix

Classification	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			<b>Signature Verification</b>		
SR-1	2.01.01	46	00	Verify the product’s ability to validate signatures in the certificates found in the certification path for card 46/Test PIV.	Registration succeeds.	PIA-2 thru PIA-7
SR-1	2.01.02	54	37	Verify the product’s ability to validate signatures in the certificates found in the certification path for card 54/Test PIV-I.	Registration succeeds.	PIA-2 thru PIA-7
SR-1	2.01.03	46	01	Verify the product’s ability to validate signatures in the certificates found in the certification path for a PIV credential.	Registration fails.	PIA-3.2, PIA-3.4, PIA-4, PIA-5
SR-1	2.01.04	05	00	Verify the product’s ability to recognize an 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 the product’s ability to recognize certificate/private key mismatch.	Registration fails.	PIA-3.2, PIA-3.4, PIA-4
	2.02			<b>Certificate Validity Periods</b>		
SR-3	2.02.01	46	02	Verify the 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 the 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 the 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 the 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

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.02.05	13	00	Verify the 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
	<b>2.03</b>			<b>Name Chaining</b>		
SR-1	2.03.01	46	04	Verify the product's ability to reject a credential when the common name portion of the issuer's name in the End Entity certificate does not match the common name portion of the subject's name in the previous intermediate certificate.	Registration fails.	PIA-3.2, PIA-5
	<b>2.04</b>			<b>Basic Constraints</b>		
SR-1	2.04.01	46	05	Verify the product's ability to recognize when the intermediate CA certificate lacks the Basic Constraints extension.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.04.04	46	08	Verify the product's ability to recognize when the first certificate in the path includes a 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
	<b>2.05</b>			<b>Key Usage Verification</b>		
SR-1	2.05.01	46	09	Verify the product's ability to recognize when the intermediate certificate includes a Key Usage extension in which <i>keyCertSign</i> is false.	Registration fails.	PIA-3.2, PIA-5
SR-3	2.05.02	46	10	Verify the 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 the product's ability to recognize when the intermediate certificate includes a Key Usage extension in which <i>crlSign</i> is false.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.05.04	46	42	Verify the product's ability to recognize when an intermediate certificate includes the Key Usage extension <i>keyCertSign</i> and <i>crlSign</i> false, and Key Usage not critical.	Registration fails.	
	<b>2.06</b>			<b>Certificate Policies</b>		
SR-1	2.06.01	Production PIV	Common Policy Root	With the trust anchor set to Common Policy, check if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for PIV Authentication Certificates to <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13).	Registration succeeds.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.06.02	Production PIV	Common Policy Root	With the trust anchor set to Common Policy, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the PIV Authentication Certificate path. The relying party solution will set the explicit policy for PIV Authentication Certificates to <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.06.05	Production PIV	Common Policy Root	With the Common Policy anchor, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the certificate; however, it is present somewhere in the certificate path. The relying party solution will set the explicit policy to a value that is present in the certificate path but does not map to the end entity certificate, such as <i>id-fpki-common-High</i> (2.16.840.1.101.3.2.1.3.16), by the relying party solution. The relying party solution will set the explicit policy to a value that is present in the certificate path but does not map to the PIV Authentication Certificate.	Registration fails.	PIA-3.2, PIA-5
SR-2	2.06.06	46	12	With the required policy set to the CITE test OID for <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11), verify the product's ability to process a path that includes a <i>policyConstraints</i> extension with <i>inhibitPolicyMapping</i> 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 if the validation software can 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 <i>id-fpki-common-authentication</i> (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 if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Card Authentication Certificates to the CITE test OID for <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13).	Registration succeeds.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.06.09	46	00	With the trust anchor set to ICAM Test Card PIV Root CA, check if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for CHUID signature certificates to the CITE test OID for <i>id-fpki-common-piv-contentSigning</i> (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 can recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The relying party solution will set the explicit policy for <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	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 can recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The relying party solution will set the explicit policy for <i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.06.12	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, check if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Authentication Certificates to the CITE test OID for <i>id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.2.1.48.78) by the relying party solution. This TC also verifies the products' ability to use policy mappings. The PIV Auth OID is (2.16.840.1.101.3.2.1.48.248) and is mapped to OID (2.16.840.1.101.3.2.1.48.78) in the intermediate certificate.	Registration succeeds.	PIA-3.2, PIA-5
SR-1	2.06.13	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, check if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Card Authentication certificates to the CITE test OID for <i>id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.2.1.48.79) by the relying party solution. This TC also verifies the products' ability to use policy mappings. The PIV cardAuth OID is	Registration succeeds.	PIA-3.2, PIA-5

PACS Functional Requirements and Test Cases

v1.4.2 Rev. D

				(2.16.840.1.101.3.2.1.48.249) and is mapped to OID (2.16.840.1.101.3.2.1.48.79) in the intermediate certificate.		
SR-1	2.06.14	54	37	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 <i>id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.2.1.48.80) by the relying party solution. This TC also verifies the products ability to use policy mappings. The OID in the PIV contentSigning is (2.16.840.1.101.3.2.1.48.252) and is mapped to OID (2.16.840.1.101.3.2.1.48.80) in the intermediate certificate.	Registration succeeds.	PIA-3.2, PIA-5
SR-1	2.06.15	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the Authentication Certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.06.16	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5
SR-1	2.06.17	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.06.18	54	00	With the trust anchor set to ICAM Test Card PIV Root CA, the following policies are required: <i>_id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11) <i>_id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13) <i>_id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.48.86) and a Test PIV-I is presented.	Registration fails.	
SR-1	2.06.19	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, the following policies are required: <i>_id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.2.1.48.78) <i>_id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.2.1.48.79) <i>_id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.1.2.3.4) - not valid. And a Test PIV-I is presented.	Registration fails.	
SR-1	2.06.20	46	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the PIV Authentication certificate path. The relying party solution will set the explicit policy for <i>_id-fpki-common-authentication</i> (2.16.840.1.101.3.1.2.3.4) to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Registration fails.	PIA-3.2, PIA-5

	<b>2.07</b>			<b>Generalized Time</b>		
SR-3	2.07.01	46	24	Verify the 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 the product's ability to process invalid use of generalized time before the year 2049 in the path.	Registration fails.	PIA-3.2, PIA-5
	<b>2.08</b>			<b>Name Constraints</b>		
	<b>2.09</b>			<b>Certificate Revocation Tests (CRL)</b>		
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	17	The system recognizes when the CRL has an invalid signature.	Registration fails.	PIA-3.5, PIA-5, PIA-7

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.09.05	46	18	The system recognizes when a certificate in the path links to a CRL issued by a CA other than the one that issued the cert.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.06	46	19	The system recognizes when a certificate in the path points to a CRL with an expired <i>nextUpdate</i> value (an expired CRL).	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-3	2.09.07	46	20	The system recognizes when a certificate in the path points to a CRL with a <i>notBefore</i> Date in the future.	Registration fails.	PIA-3.5, PIA-5, PIA-7
SR-1	2.09.08	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-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
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
SO-1	2.09.12	58	00	1. The system recognizes when: 1. The end-entity PIV Authentication Certificate is neither expired nor revoked. 2. The end-entity Card Authentication Certificate is not expired but has been revoked; AIA to OCSP is unavailable, while crlDP to CRL is available.	Registration fails.	[SP 800-73], PIA-3, PIA-3.2
	<b>2.10</b>			<b>CHUID Verification</b>		
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 has expired.	Registration fails.	PIA-3.6, PIA-5
SR-1	2.10.03	14	00	The system recognizes when the CHUID has 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)

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.10.08	46	03	The system recognizes when an intermediate certificate in the CHUID signer certificate path has 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	00	The system recognizes when the CHUID signer certificate is revoked.	Registration fails.	PIA-3, PIA-3.2
	<b>2.11</b>			<b>Facial Image Verification</b>		
SR-1	2.11.01	06	00	The system recognizes when the facial image signature is invalid.	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]
	<b>2.12</b>			<b>Copied Containers</b>		
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	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	2.12.03	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	2.12.04	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
	<b>2.13</b>			<b>Fingerprint Verification</b>		
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	Production PIV	Common Policy Root	Verify the Product's ability to accept a valid credential with a matching fingerprint.	Registration succeeds.	PIA-9
SR-1	2.13.04	Production PIV	Common Policy Root	Verify the Product's ability to reject a valid credential with a non-matching fingerprint.	Registration fails.	PIA-9

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

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]
SR-1	2.13.09	Production NFI PIV-I	Common Policy Root	Verify the Product's ability to accept a valid credential with a matching fingerprint.	Registration succeeds.	PIA-9
SR-1	2.13.10	Production NFI PIV-I	Common Policy Root	Verify the Product's ability to reject a valid credential with a non-matching fingerprint.	Registration fails.	PIA-9
SR-1	2.13.11	Production FI PIV-I	Common Policy Root	Verify the Product's ability to accept a valid credential with a matching fingerprint.	Registration succeeds.	PIA-9
SR-1	2.13.12	Production FI PIV-I	Common Policy Root	Verify the Product's ability to reject a valid credential with a non-matching fingerprint.	Registration fails.	PIA-9
SR-1	2.13.13	Production CAC	Common Policy Root	Verify the Product's ability to accept a valid credential with a matching fingerprint.	Registration succeeds.	PIA-9
SR-1	2.13.14	Production CAC	Common Policy Root	Verify the Product's ability to reject a valid credential with a non-matching fingerprint.	Registration fails.	PIA-9
	<b>2.14</b>			<b>Security Object Verification</b>		
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
	<b>2.15</b>			<b>OCSP Response Checking</b>		

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.15.01	46	00	The system validates a valid credential using an OCSP response with a valid signature.	Registration succeeds.	PIA-3.2, PIA-3.5
SR-2	2.15.02	42	00	Validation fails when an OCSP Responder has an expired signature certificate for a test 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 test 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 test 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
SO-1	2.15.06	58	00	1. 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 revoked; AIA to OCSP is available, and crlDP to CRL is unavailable.	Registration fails.	PIA-3.2, PIA-4
	<b>2.16</b>			<b>Interoperability Testing</b>		
SR-1	2.16.01	Production PIV	Common Policy Root	Production PIV cards can be registered.	Registration succeeds.	PIA-6
SR-1	2.16.02	39	37	The system recognizes a Federally-issued PIV-I card with an 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	37	The system recognizes a Federally-issued PIV-I card with an 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 (EKU) extension keyPurposeId OID <i>id-PIV-content-signing</i> (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 (EKU) extension <i>keyPurposeId</i> OID <i>id-PIV-content-signing</i> (2.16.840.1.101.1.2.3) is absent in the content signing certificate.	Registration fails.	[FIPS 201]

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-3	2.16.06	54	37	The system recognizes when the Extended Key Usage (EKU) extension keyPurposeId OID <i>id-fpki-pivi-content-signing</i> (2.16.840.1.101.3.8.7) is present in the content signing certificate.	Registration succeeds.	[FIPS 201]
SR-3	2.16.07	54	37	The system recognizes when an explicit Extended Key Usage (EKU) extension keyPurposeId OID <i>id-fpki-pivi-content-signing</i> (2.16.840.1.101.1.2.3) is absent in the content signing certificate.	Registration fails.	[FIPS 201]
SR-3	2.16.08	46	00	The system recognizes when the Extended Key Usage (EKU) extension keyPurposeId OID <i>id-PIV-cardAuth</i> (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 (EKU) extension keyPurposeId OID <i>id-PIV-cardAuth</i> (2.16.840.1.101.1.2.3) is absent in the Card Authentication certificate.	Registration fails.	[FIPS 201]
SR-3	2.16.10	54	37	The system recognizes when the Extended Key Usage (EKU) extension keyPurposeId OID <i>id-PIV-cardAuth</i> (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	37	The system recognizes when an explicit Extended Key Usage (EKU) extension keyPurposeId OID <i>id-PIV-cardAuth</i> (2.16.840.1.101.1.2.3) is absent 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 <i>entryUUID</i> in the <i>GeneralNames</i> sequence within the Subject Alternative Names extension of the PIV Authentication and Card Authentication certificate.	Registration succeeds.	[FIPS 201]
SR-1	2.16.14	53	00	The system manages cards with a Card Authentication Certificate that is slightly larger than the recommended size (2160 bytes).	Registration succeeds.	[[SP800-73]]
SR-1	2.16.15	Production PIV	Common Policy Root	PIV cards can be individually registered.  Trust anchor set to Common Policy Root, and the following policies are required: <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13) <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17) <i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.3.39)	Registration succeeds.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.16.16	Production CAC	Common Policy Root	<p>CAC cards can be individually registered.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:</p> <ul style="list-style-type: none"> <li><u>id-fpki-common-authentication</u> (2.16.840.1.101.3.2.1.3.13)</li> <li><u>id-fpki-common-cardAuth</u> (2.16.840.1.101.3.2.1.3.17)</li> <li><u>id-fpki-common-piv-contentSigning</u> (2.16.840.1.101.3.2.1.3.39)</li> </ul>	Registration succeeds.	PIA-6
SR-1	2.16.17	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I cards can be individually registered.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:</p> <ul style="list-style-type: none"> <li><u>id-fpki-common-pivi-authentication</u> (2.16.840.1.101.3.2.1.3.45)</li> <li><u>id-fpki-common-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.46)</li> <li><u>id-fpki-common-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.47)</li> </ul>	Registration succeeds.	PIA-6
SR-1	2.16.18	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I cards can be individually registered.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:</p> <ul style="list-style-type: none"> <li><u>id-fpki-certpcy-pivi-hardware</u> (2.16.840.1.101.3.2.1.3.18)</li> <li><u>id-fpki-certpcy-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.19)</li> <li><u>id-fpki-certpcy-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.20)</li> </ul>	Registration succeeds.	PIA-6
SR-1	2.16.19	Test CAC - Gemalto	CAC Test Path	<p>DOD Test CAC cards can be individually registered.</p> <p>Trust anchor set to DOD CAC Test-Path, and the following policies are required:</p> <ul style="list-style-type: none"> <li><u>id-fpki-common-authentication</u> (2.16.840.1.101.3.2.1.48.11)</li> <li><u>id-fpki-common-cardAuth</u> (2.16.840.1.101.3.2.1.48.13)</li> <li><u>id-fpki-common-piv-contentSigning</u> (2.16.840.1.101.3.2.1.48.86)</li> </ul>	Registration succeeds.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	2.16.20	Test CAC - IDEMIA	CAC Test Path	DOD Test CAC cards can be individually registered.  Trust anchor set to DOD CAC Test-Path, and the following policies are required: <i>_id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11) <i>_id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13) <i>_id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.48.86)	Registration succeeds.	PIA-6
SR-1	2.16.21	Test CAC - G + D	CAC Test Path	DOD Test CAC cards can be individually registered.  Trust anchor set to DOD CAC Test-Path, and the following policies are required: <i>_id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11) <i>_id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13) <i>_id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.48.86)	Registration succeeds.	PIA-6
	<b>2.17</b>			<b>Cryptography Testing</b>		
SR-1	2.17.02	NIST #1	NIST Root	Verify the 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 the 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 the 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 the 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 the 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 the 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 the Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) with an exponent of 65,537.	Registration succeeds.	[SP800-78] Table 3-2

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

2.18				Discovery Object and PIN Usage Policy		
SR-2	2.18.01	25	00	Discovery object not present. Enter an 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 a valid PIV Application PIN. Confirm that the PIV Application PIN retry counter is reset to 10. Confirm that the 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	The discovery object is present and set for PIV Application PIN only. Enter an 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	The discovery object is present and set for PIV Application PIN only. Enter a valid PIV Application PIN. Confirm that the 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
SR-1	2.18.05	27	00	The discovery object is present. PIV App and Global PINs are available. PIV Application PIN is primary. Enter an invalid PIV Application PIN (e.g., 999999). Confirm PIV Application PIN retry counter is decremented by one (9). Confirm that the 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	The discovery object is present. PIV Application and Global PINs are available. PIV Application PIN is primary. Enter a valid PIV Application PIN. Confirm that the 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	The discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Enter an invalid Global PIN (e.g., 999999). Confirm that the PIV Application PIN retry counter remains at 10. Confirm that the 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	2.18.15	28	00	The discovery object is present. PIV Application and Global PINs are available. Global PIN is primary. Enter a valid Global PIN. Confirm that the 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
<b>2.19</b>				<b>ISO 7816-3 2006 PPS Protocol Compliance</b>		
<b>2.20</b>				<b>SM and OCC-AUTH</b>		
SO-1	2.20.02	Production PIV	Common Policy	Production PIV cards can be individually registered.	Registration succeeds.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

			Root	<p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i>                      (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i>                      (2.16.840.1.101.3.2.1.3.39)</p>		
SO-1	2.20.03	Production PIV	Common Policy Root	<p>Production PIV cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i>                      (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i>                      (2.16.840.1.101.3.2.1.3.39)</p>	Registration succeeds.	PIA-6
SO-1	2.20.04	Production CAC	Common Policy Root	<p>Production CAC cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i>                      (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i>                      (2.16.840.1.101.3.2.1.3.39)</p>	Registration succeeds.	PIA-6
SO-1	2.20.05	Production CAC	Common Policy Root	<p>Production CAC cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i>                      (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i></p>	Registration succeeds.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

				(2.16.840.1.101.3.2.1.3.39)		
SO-1	2.20.06	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <i>__id-fpki-common-pivi-authentication</i>                      (2.16.840.1.101.3.2.1.3.45)  <i>__id-fpki-common-pivi-cardAuth</i>                      (2.16.840.1.101.3.2.1.3.46)  <i>__id-fpki-common-pivi-contentSigning</i>                      (2.16.840.1.101.3.2.1.3.47)</p>	Registration succeeds.	PIA-6
SO-1	2.20.07	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <i>__id-fpki-common-pivi-authentication</i>                      (2.16.840.1.101.3.2.1.3.45)  <i>__id-fpki-common-pivi-cardAuth</i>                      (2.16.840.1.101.3.2.1.3.46)  <i>__id-fpki-common-pivi-contentSigning</i>                      (2.16.840.1.101.3.2.1.3.47)</p>	Registration succeeds.	PIA-6
SO-1	2.20.08	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <i>__id-fpki-certpcy-pivi-hardware</i>                      (2.16.840.1.101.3.2.1.3.18)  <i>__id-fpki-certpcy-pivi-cardAuth</i>                      (2.16.840.1.101.3.2.1.3.19)  <i>__id-fpki-certpcy-pivi-contentSigning</i></p>	Registration succeeds.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

				(2.16.840.1.101.3.2.1.3.20)		
SO-1	2.20.09	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:</p> <p><i>__id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.2.1.3.18)</p> <p><i>__id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.2.1.3.19)</p> <p><i>__id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.2.1.3.20)</p>	Registration succeeds.	PIA-6

	<b>4.0</b>			<b>Requirements for Automated Provisioning, Deprovisioning, and Modifications, In Accordance With [E-PACS] PIA-8</b>		
	<b>4.01</b>			<b>Provisioning</b>		
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
	<b>5.0</b>			<b>Authentication at Time of Access Test Cases</b>		
	<b>5.01</b>			<b>Signature Verification</b>		
SR-1	5.01.01	46	00	With ICAM Test Card 46 registered with the PACS, verify the product’s ability to validate signatures in the certificates found in the certification path for a test PIV credential.	Access granted.	PIA-2 thru PIA-7

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SO-1	5.01.02	54	37	With ICAM Test Card 54 registered with the PACS, verify the product's ability to validate signatures in the certificates found in the certification path for a test 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 the product's ability to recognize an invalid signature on an intermediate CA in the certification path.	Access denied.	PAI-3.2, PIA-3.4, PIA-4, PIA-5
SR-1	5.01.05	01, 23	00	With ICAM Test Card 01 registered with the PACS, verify the product's ability to recognize certificate/private key mismatch.	Access denied.	PAI-3.2, PIA-3.4, PIA-4
	<b>5.02</b>			<b>Certificate Validity Periods</b>		
SR-3	5.02.01	46	00, 02	With ICAM Test Card 46 registered with the PACS, verify the product's ability to reject a credential when the <i>notBefore</i> date of the intermediate CA certificate is sometime in the future.	Access denied.	PIA-3.5, PIA-5
SR-1	5.02.04	46	00, 03	With ICAM Test Card 46 registered with the PACS, verify the product's ability to reject a credential when <i>notAfter</i> date of <i>any</i> certificate in the path is sometime in the past.	Access denied.	PIA-3.5, PIA-5
	<b>5.03</b>			<b>Name Chaining</b>		
SR-1	5.03.01	46	00, 04	With ICAM Test Card 46 registered with the PACS, verify the product's ability to reject a credential when the common name portion of the issuer's name in the End Entity certificate does not match the common name portion of the subject's name in the previous intermediate certificate.	Access denied.	PIA-3.2, PIA-5
	<b>5.04</b>			<b>Basic Constraints</b>		
SR-1	5.04.01	46	00, 05	With ICAM Test Card 46 registered with the PACS, verify the product's ability to recognize when the intermediate CA certificate is missing the Basic Constraints extension.	Access denied.	PIA-3.2, PIA-5
SR-1	5.04.04	46	00, 08	With ICAM Test Card 46 registered with the PACS, verify the product's ability to recognize when the first certificate in the path includes a Basic Constraints extension with a <i>pathLenConstraint</i> 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

PACS Functional Requirements and Test Cases

v1.4.2 Rev. D

5.05				Key Usage Verification		
SR-1	5.05.01	46	00, 09	With ICAM Test Card 46 registered with the PACS, verify the product's ability to recognize when the intermediate certificate includes a Key Usage extension in which <i>keyCertSign</i> is false.	Access denied.	PIA-3.2, PIA-5
SR-3	5.05.02	46	00, 10	With ICAM Test Card 46 registered with the PACS, verify the 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	00, 11	With ICAM Test Card 46 registered with the PACS, verify the product's ability to recognize when the intermediate certificate includes a Key Usage extension in which <i>crI</i> is false.	Access denied.	PIA-3.2, PIA-5
SR-1	5.05.04	46	42	Verify the product's ability to recognize when the intermediate certificate includes Key Usage extension <i>keyCertSign</i> , <i>crI</i> false, and Key Usage not critical.	Access denied.	PIA-3.2, PIA-5
5.06				Certificate Policies		
SR-2	5.06.01	Production PIV	Common Policy Root	With the trust anchor set to Common Policy, check if the validation software can recognize when an explicit certificate policy is required and present in the PIV Authentication certificate path. The relying party solution will set the explicit policy to <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13).	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.02	Production PIV	Common Policy Root	With the trust anchor set to Common Policy, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the certificate path. The relying party solution will set the explicit policy for PIV Authentication Certificates to <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.05	Production PIV	Common Policy Root	With the Common Policy anchor, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the certificate; however, it is present somewhere in the certificate path. The relying party solution will set the explicit policy to a value that is present in the certificate path but does not map to the end entity certificate, such as <i>id-fpki-common-High</i> (2.16.840.1.101.3.2.1.3.16), by the relying party solution. The relying party solution will set the explicit policy to a value that is present in the certificate path but does not map to the PIV Authentication Certificate.	Access denied.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-2	5.06.06	46	00, 12	With ICAM Test Card 46 registered with the PACS, and with required policy set to the CITE test OID for <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11), verify the product's ability to process a path that includes a <i>policyConstraints</i> extension with <i>inhibitPolicyMapping</i> 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 the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Authentication Certificates to the CITE test OID for <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11).	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.08	46	00	With ICAM Test Card 46 registered with the PACS and the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Card Authentication Certificates to the CITE test OID for <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13).	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.09	46	00	With ICAM Test Card 46 registered with the PACS and the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for CHUID signature certificates to the CITE test OID for <i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.48.86).	Access granted.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.06.10	46	00	After registering ICAM Test Card 46 with the PACS and setting the trust anchor to ICAM Test Card PIV Root CA, verify whether the validation software can identify when an explicit certificate policy is required but absent from the Card Authentication certificate path. The relying party solution will establish the explicit policy for <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.1.2.3.4). This explicit policy will be set to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.11	46	00	With ICAM Test Card 46 registered with the PACS and the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The relying party solution will set the explicit policy for <i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.1.2.3.4) to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.12	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Authentication Certificates to the CITE test OID for <i>id-fpki-certscy-pivi-hardware</i> (2.16.840.1.101.3.2.1.48.78). This TC also verifies the products' ability to use policy mappings. The OID in the PIV Auth is (2.16.840.1.101.3.2.1.48.248) and is mapped to OID (2.16.840.1.101.3.2.1.48.78) in the intermediate certificate.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.13	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for Card Authentication certificates to the CITE test OID for <i>id-fpki-certscy-pivi-cardAuth</i> (2.16.840.1.101.3.2.1.48.79). This TC also verifies the products' ability to use policy mappings. The OID in the Card Auth is (2.16.840.1.101.3.2.1.48.249) and is mapped to OID (2.16.840.1.101.3.2.1.48.79) in the intermediate certificate.	Access granted.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.06.14	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and present in the certificate path. The relying party solution will set the explicit policy for CHUID signature certificates to the CITE test OID for <i>id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.2.1.48.80). This TC also verifies the products' ability to use policy mappings. The OID in the CHUID/contentSigning is (2.16.840.1.101.3.2.1.48.252) and is mapped to OID (2.16.840.1.101.3.2.1.48.80) in the intermediate certificate.	Access granted.	PIA-3.2, PIA-5
SR-1	5.06.15	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the Authentication Certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.16	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.17	54	37	With ICAM Test Card 54 registered with the PACS and the trust anchor set to ICAM Test Card PIV-I Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The relying party solution will set the explicit policy for <i>id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.1.2.3.4). The explicit policy will be to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	PIA-3.2, PIA-5

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.06.18	54	37, 00	With the trust anchor set to ICAM Test Card PIV Root CA, the following policies are required: <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.48.11) <i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.48.13) <i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.48.86) A Test PIV-I is presented.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.19	54	37	With the trust anchor set to ICAM Test Card PIV-I Root CA, the following policies are required: <i>id-fpki-certpcy-pivi-hardware</i> (2.16.840.1.101.3.2.1.48.78) <i>id-fpki-certpcy-pivi-cardAuth</i> (2.16.840.1.101.3.2.1.48.79) <i>id-fpki-certpcy-pivi-contentSigning</i> (2.16.840.1.101.3.1.2.3.4) - <b>invalid</b> . A Test PIV-I is presented.	Access denied.	PIA-3.2, PIA-5
SR-1	5.06.20	46	00	With the trust anchor set to ICAM Test Card PIV Root CA, check to see if the validation software can recognize when an explicit certificate policy is required and not present in the PIV Authentication certificate path. The relying party solution will set the explicit policy for <i>id-fpki-common-authentication</i> (2.16.840.1.101.3.1.2.3.4) to an arbitrary ( <b>invalid</b> ) value not present in the certificate path.	Access denied.	
	<b>5.07</b>			<b>Generalized Time</b>		
SR-3	5.07.01	46	24	With ICAM Test Card 46 registered with the PACS, verify the 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	00, 25	With ICAM Test Card 46 registered with the PACS, verify the product's ability to process invalid use of generalized time before the year 2049 in the path.	Access denied.	PIA-3.2, PIA-5
	<b>5.08</b>			<b>Name Constraints</b>		
	<b>5.09</b>			<b>Certificate Revocation Tests (CRL)</b>		
SR-1	5.09.02	46	00, 16	With the ICAM Test Card 46 registered with the PACS, confirm that the system recognizes when a second intermediate CA certificate is revoked.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.04	46	00, 17	With ICAM Test Card 46 registered in the PACS, confirm that 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	00, 18	With the ICAM Test Card 46 registered in the PACS, confirm that the system recognizes when a certificate in the	Access denied.	PIA-3.5, PIA-5, PIA-7

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

				path links to a CRL issued by a CA other than the one that issued the certificate.		
SR-1	5.09.06	46	00, 19	With ICAM Test Card 46 registered with the PACS, confirm that the system recognizes when a certificate in the path has an expired <i>nextUpdate</i> value, indicating an expired CRL.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-3	5.09.07	46	00, 20	With the ICAM Test Card 46 registered in the PACS, confirm that the system recognizes when a certificate in the path refers to a CRL with a notBefore date set in the future.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.08	46	00, 21	With ICAM Test Card 46 registered with the PACS, confirm that the system detects when a certificate in the path has an incorrect CRL distribution point.	Access denied.	PIA-3.5, PIA-5, PIA-7
SR-1	5.09.11	58	00	The system detects when the Card Authentication Certificate is revoked.	Access denied.	
SO-1	5.09.12	58	00	The system recognizes when: 1. The end-entity PIV Authentication Certificate is neither expired nor revoked. 2. The end-entity Card Authentication Certificate is not expired but has been revoked; AIA to OCSP is unavailable, while crlDP to CRL is available.	Access denied.	[SP 800-73], PIA-3, PIA-3.2
	<b>5.10</b>			<b>Content Signer Verification</b>		

SO-1	5.10.01	01, 04	00	The system detects when the CHUID signature is invalid.	Access denied.	PIA-3.2, PIA-4
SO-2	5.10.02	01, 09	00	The system detects when the CHUID signer certificate has expired.	Access denied.	PIA-3.6, PIA-5
SO-1	5.10.03	01, 14	00	The system detects when the CHUID has expired.	Access denied.	PIA-3.6
SR-2	5.10.04	01, 15	00	The system detects when the FASC-N in the CHUID does not match the FASC-N in the PIV Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.1.2

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-2	5.10.05	01, 19	00	The system detects when the UUID in the CHUID does not match the UUID in the PIV-I Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.3
SR-1	5.10.06	01, 11	00	The system detects when the PIV-AUTH certificate expires after the CHUID expiration date.	Access denied.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	5.10.08	46	00, 03	The system detects when an intermediate certificate in the CHUID signer certificate path has expired.	Access denied.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	5.10.09	46	00, 16	The system detects when an intermediate certificate in the CHUID signer certificate path is revoked.	Access denied.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
SR-1	5.10.10	57	00	The system detects when the CHUID signer certificate is revoked.	Access denied.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
	<b>5.11</b>			<b>Facial Image Verification</b>		
SR-1	5.11.01	01, 06	00	With ICAM Test Card 1 registered with the PACS, the system identifies when the Facial Image signature is invalid.	Access denied.	PIA-3, PIA-3.2, PIA-3.3, PIA-4
SO-2	5.11.02	46, 49	00	The system detects when the Facial Image CBEFF has expired.	Access denied.	[SP 800-76]
SO-1	5.11.03	Production PIV	Common Policy Root	Confirm the product's ability to accept valid credentials with matching facial authentication.	Access granted.	PIA-3 thru PIA-7
SO-1	5.11.04	Production PIV	Common Policy Root	Confirm that the product can reject a valid credential using non-matching facial authentication.	Access denied.	PIA-3.3
SO-1	5.11.09	Production NFI PIV-I	Common Policy Root	Confirm the product's capability to accept a valid credential with matching facial authentication.	Access granted.	PIA-9
SO-1	5.11.10	Production NFI PIV-I	Common Policy Root	Confirm that the product can reject a valid credential using non-matching facial authentication.	Access denied.	PIA-9
SO-1	5.11.11	Production FI PIV-I	Common Policy Root	Confirm the product's capability to accept a valid credential with matching facial authentication.	Access granted.	PIA-9
SO-1	5.11.12	Production FI PIV-I	Common Policy Root	Confirm that the product can reject a valid credential using non-matching facial authentication.	Access denied.	PIA-9

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SO-1	5.11.13	Production CAC	Common Policy Root	Confirm the product's capability to accept a valid credential with matching facial authentication.	Access granted.	PIA-9
SO-1	5.11.14	Production CAC	Common Policy Root	Confirm that the product can reject a valid credential using non-matching facial authentication.	Access denied.	PIA-9
	<b>5.12</b>			<b>Copied Containers</b>		
SR-1	5.12.01	01, 16	00	The system identifies when the FASC-N in the PKI-CAK certificate does not match the FASC-N in the PIV Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.1.2
SR-1	5.12.02	01, 17	00	The system detects when the FASC-N in the Facial Image does not match the FASC-N in the PIV Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.1.2
SR-1	5.12.03	01, 20	00	The system detects when the UUID in the PKI-CAK certificate does not match the UUID in the PIV-I Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.1.2
SO-1	5.12.04	01, 21	00	The system detects when the UUID in the facial image does not match the UUID in the PIV-I Auth Certificate.	Access denied.	PIA-3.2; [SP800-73], Part 1, §3.1.2
	<b>5.13</b>			<b>Fingerprint Verification</b>		
SR-1	5.13.01	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 identifies when the fingerprint signature is invalid.	Access denied.	PIA-3, PIA-3.2, PIA-3.3, PIA-4
SR-1	5.13.03	Production PIV	Common Policy Root	Confirm that the product can accept a valid credential with a matching fingerprint.	Access granted.	PIA-3 thru PIA-7
SR-1	5.13.04	Production PIV	Common Policy Root	Confirm that the product can reject a valid credential with a non-matching fingerprint.	Access denied.	PIA-3.3
SR-1	5.13.05	01, 18	00	The system identifies when the FASC-N in the fingerprint does not match the FASC-N in the PIV Auth Certificate.	Access denied.	
SR-3	5.13.06	01, 22	00	The system identifies when the UUID in the fingerprint does not match the UUID in the PIV-I Auth Certificate.	Access denied.	
SR-2	5.13.07	46, 51	00	The system detects when the Cardholder's CBEFF fingerprints have expired.	Access denied.	
UO-3	5.13.08	46, 52	00	The system detects when the Cardholder's CBEFF fingerprints are set to expire before the CHUID expiration date.	Access granted.	

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.13.09	Production NFI PIV-I	Common Policy Root	Confirm that the product can accept a valid credential with a matching fingerprint.	Access granted.	PIA-9
SR-1	5.13.10	Production NFI PIV-I	Common Policy Root	Confirm that the product can reject a valid credential with a non-matching fingerprint.	Access denied.	PIA-9
SR-1	5.13.11	Production FI PIV-I	Common Policy Root	Confirm that the product can accept a valid credential with a matching fingerprint.	Access granted.	PIA-9
SR-1	5.13.12	Production FI PIV-I	Common Policy Root	Confirm that the product can reject a valid credential with a non-matching fingerprint.	Access denied.	PIA-9
SR-1	5.13.13	Production CAC	Common Policy Root	Confirm that the product can accept a valid credential with a matching fingerprint.	Access granted.	PIA-9
SR-1	5.13.14	Production CAC	Common Policy Root	Confirm that the product can reject a valid credential with a non-matching fingerprint.	Access denied.	PIA-9
	<b>5.14</b>			<b>Security Object Verification</b>		
	<b>5.15</b>			<b>OCSP Response Checking</b>		
SR-1	5.15.01	46	00	With ICAM Test Card 46 registered in the PACS, confirm that the system validates a valid credential using an OCSP response with a valid signature.	Access granted.	PIA-3.2, PIA-3.5
SR-2	5.15.02	42	00	With ICAM Test Card 42 registered with the PACS, confirm that validation fails when using an OCSP Responder that has an expired signature certificate for a valid card.	Access denied.	PIA-3.2, PIA-3.5, PIA-3.6
SR-3	5.15.03	43	00	With ICAM Test Card 43 registered with the PACS, confirm that validation is successful using an OCSP Responder with a revoked signature certificate for a valid credential with PKIX_OCSP_NOCHECK present.	Access granted.	PIA-3.2, PIA-3.5
SR-2	5.15.04	44	00	With ICAM Test Card 44 registered with the PACS, confirm that validation fails when using an OCSP Responder with a revoked signature certificate for a valid credential without PKIX_OCSP_NOCHECK present.	Access denied.	PIA-3.2, PIA-3.5, PIA-3.6
SR-1	5.15.05	45	00	With the ICAM Test Card 45 registered with the PACS, confirm that validation fails when using an OCSP Responder that has a signature certificate containing an invalid signature for a valid credential.	Access denied.	PIA-3.2, PIA-4

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SO-1	5.15.06	58	00	1. 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 revoked; AIA to OCSP is available, and crlDP to CRL is unavailable.	Access denied.	PIA-3.2, PIA-4
	<b>5.16</b>			<b>Interoperability Testing</b>		
SR-1	5.16.01	Production PIV	Common Policy Root	Production PIV cards are granted access using the PKI-AUTH method.	Access granted.	PIA-6
SR-1	5.16.02	39	37	With ICAM Test Card 39 registered with the PACS, confirm that the system recognizes a federally issued PIV-I card with an FASC-N that does not start 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	5.16.03	54	37	With ICAM Test Card 54 registered in the PACS, confirm that the system identifies a federally issued PIV-I card with an FASC-N starting with fourteen 9s.	Access granted.	PIA-6
SR-3	5.16.04	46	00	With the ICAM Test Card 46 registered with the PACS, confirm that the system recognizes the Extended Key Usage (EKU) extension keyPurposeId OID <i>id-PIV-content-signing</i> (2.16.840.1.101.3.6.7) in the content signing certificate.	Access granted.	[FIPS 201]
SR-3	5.16.05	46	00	With ICAM Test Card 46 registered with the PACS, confirm that the system recognizes when an explicit Extended Key Usage (EKU) extension keyPurposeId OID <i>id-PIV-content-signing</i> (2.16.840.1.101.1.2.3) is absent from the content signing certificate.	Access denied.	[FIPS 201]
SR-3	5.16.06	54	37	With ICAM Test Card 54 registered in the PACS, the system recognizes the presence of the Extended Key Usage (EKU) extension keyPurposeId OID <i>id-fpki-pivi-content-signing</i> (2.16.840.1.101.3.8.7) in the content signing certificate.	Access granted.	[FIPS 201]
SR-3	5.16.07	54	37	With ICAM Test Card 54 registered with the PACS, confirm that the system detects when the explicit Extended Key Usage (EKU) extension keyPurposeId OID <i>id-fpki-pivi-content-signing</i> (2.16.840.1.101.1.2.3) is absent from the content signing certificate.	Access denied.	[FIPS 201]

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-3	5.16.08	46	00	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when the Extended Key Usage extension <i>keyPurposeId</i> OID <i>id-PIV-cardAuth</i> (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Access granted.	[FIPS 201]
SR-3	5.16.09	46	00	With ICAM Test Card 46 registered with the PACS, verify the system recognizes when an explicit Extended Key Usage extension <i>keyPurposeId</i> OID <i>id-PIV-cardAuth</i> (1.16.840.1.101.1.2.3) is not present in the Card Authentication certificate.	Access denied.	[FIPS 201]
SR-3	5.16.10	54	37	With ICAM Test Card 54 registered with the PACS, verify the system recognizes when the Extended Key Usage extension <i>keyPurposeId</i> OID <i>id-PIV-cardAuth</i> (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate.	Access granted.	[FIPS 201]
SR-3	5.16.11	54	37	With ICAM Test Card 54 registered with the PACS, verify the system recognizes when an explicit Extended Key Usage extension <i>keyPurposeId</i> OID <i>id-PIV-cardAuth</i> (1.16.840.1.101.1.2.3) is not present in the Card Authentication certificate.	Access denied.	[FIPS 201]
SR-1	5.16.13	47	00	With ICAM Test Card 47 registered with the PACS, FIPS 201-2 card results in an access granted decision with the <i>pivFASC-N</i> positioned after the <i>entryUUID</i> in the <i>GeneralNames</i> sequence within the Subject Alternative Names extension of the PIV Authentication certificate.	Access granted.	[FIPS 201]
SR-1	5.16.14	53	00	With ICAM Test Card 53 registered with the PACS, the system manages cards with a Card Authentication Certificate that is slightly larger than the recommended size (2160 bytes).	Access granted.	[SP800-73]
SR-1	5.16.15	Production PIV	Common Policy Root	PIV card can complete Time of Access for all supported authentication types.  Trust anchor set to Common Policy Root, and the following policies are required: <ul style="list-style-type: none"> <li>___<i>id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13)</li> <li>___<i>id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)</li> <li>___<i>id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.3.39)</li> </ul>	Access granted.	PIA-6

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.16.16	Production CAC	Common Policy Root	<p>CAC card can complete Time of Access for all supported authentication types.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <u>id-fpki-common-authentication</u> (2.16.840.1.101.3.2.1.3.13)  <u>id-fpki-common-cardAuth</u> (2.16.840.1.101.3.2.1.3.17)  <u>id-fpki-common-piv-contentSigning</u> (2.16.840.1.101.3.2.1.3.39)</p>	Access granted.	PIA-6
SR-1	5.16.17	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I card can complete Time of Access for all support authentication types.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-common-pivi-authentication</u> (2.16.840.1.101.3.2.1.3.45)  <u>id-fpki-common-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.46)  <u>id-fpki-common-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.47)</p>	Access granted.	PIA-6
SR-1	5.16.18	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I card can complete Time of Access for all support authentication types.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-certpcy-pivi-hardware</u> (2.16.840.1.101.3.2.1.3.18)  <u>id-fpki-certpcy-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.19)  <u>id-fpki-certpcy-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.20)</p>	Access granted.	PIA-6
SR-1	5.16.19	Test CAC - Gemalto	CAC Test Path	<p>DOD Test CAC cards can complete Time of Access for all support authentication types.</p> <p>Trust anchor set to DOD CAC Test Path, and the following policies are required:  <u>id-fpki-common-authentication</u> (2.16.840.1.101.3.2.1.48.11)  <u>id-fpki-common-cardAuth</u> (2.16.840.1.101.3.2.1.48.13)  <u>id-fpki-common-piv-contentSigning</u> (2.16.840.1.101.3.2.1.48.86)</p>	Access granted.	

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	5.16.20	Test CAC - IDEMIA	CAC Test Path	DOD Test CAC cards can complete Time of Access for all support authentication types.  Trust anchor set to DOD CAC Test Path, 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.	
SR-1	5.16.21	Test CAC - G + D	CAC Test Path	DOD Test CAC cards can complete Time of Access for all support authentication types.  Trust anchor set to DOD CAC Test Path, 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.	
	<b>5.17</b>			<b>Cryptography Testing</b>		
SR-1	5.17.02	NIST #1	NIST Root	With NIST Test Card #1 registered with the PACS, confirm the product's capability to validate signatures using SHA-256 and RSA PKCS#1 v1.5 (2048) with an exponent of 65,537.	Access granted.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
SO-3	5.17.05	NIST #2	NIST Root	With NIST Test Card #2 registered in the PACS, confirm the product's capability 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	5.17.07	NIST #4	NIST Root	With NIST Test Card #4 registered in the PACS, confirm the product's capability 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	5.17.08	NIST #5	NIST Root	With NIST Test Card #5 registered in the PACS, confirm the product's capability 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	5.17.10	NIST #1	NIST Root	With NIST Test Card #1 registered in the PACS, confirm the product's capability to validate signatures using SHA-256.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5
SO-3	5.17.11	NIST #5	NIST Root	With NIST Test Card #5 registered in the PACS, confirm the product's capability to validate signatures using SHA-384.	Access granted.	[SP800-78] Table 3-7; [Common] §6.1.5
SR-1	5.17.12	NIST #1	NIST Root	With NIST Test Card #1 registered in the PACS, confirm the product's capability to validate signatures using SHA-256 and RSA PKCS#1 v1.5 (2048) with an exponent of 65,537.	Access granted.	[SP800-78] Table 3-2

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

5.18				Discovery Object and PIN Usage Policy		
SR-2	5.18.01	25	00	Register the ICAM Test Card 25; the Discovery object is missing. Enter an invalid PIV Application PIN (e.g., 999999). Confirm that the PIV Application PIN retry counter decreases by one to 9. E-PACS is using the Application PIN.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.18.02	25	00	Register the ICAM Test Card 25; the Discovery object is missing. Enter a valid PIV Application PIN. Confirm that the PIV Application PIN retry counter is reset to 10. Confirm that the 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	5.18.03	26	00	Register ICAM Test Card 26; the Discovery object is available and configured for PIV Application PIN only. Enter an invalid PIV Application PIN (e.g., 999999). Confirm that the PIV Application PIN retry counter decreases by one to 9. E-PACS is utilizing the Application PIN.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.18.04	26	00	Register the ICAM Test Card 26; the Discovery object is present and configured for the PIV Application PIN only. Enter a valid PIV Application PIN. Confirm that the PIV Application PIN retry counter resets to 10. E-PACS is using the Application PIN.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.18.05	27	00	Register ICAM Test Card 27; the Discovery object is present, and the PIV App and Global PINs are available. The PIV Application PIN is primary. Enter an invalid PIV Application PIN (e.g., 999999). Confirm that the PIV Application PIN retry counter is decremented by one to 9. Confirm that the 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	5.18.07	27	00	Register the ICAM Test Card 27; the Discovery object is present, and the PIV App and Global PINs are accessible. The PIV Application PIN is primary. Please enter a valid PIV Application PIN. Confirm that the PIV Application and Global PINs are ten (10) digits long. E-PACS is utilizing the Application PIN.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.18.10	28	00	Register the ICAM Test Card 28. The Discovery object is present, and the PIV application, along with the Global PINs, is available, with the Global PIN being primary. Enter an invalid Global PIN (e.g., 999999). Confirm that the PIV application PIN retry counter remains at 10 and verify that the Global PIN retry counter is reduced by 1 to 9.	Access denied.	[SP800-73] Part 1, §3.2.6, §5.1
SR-2	5.18.15	28	00	Register ICAM Test Card 28; the Discovery object is available, and the PIV App and Global PINs are present, with the Global PIN being primary. Enter a valid Global PIN. Confirm that the PIV Application and Global PINs are 10. E-PACS uses the Global PIN.	Access granted.	[SP800-73] Part 1, §3.2.6, §5.1

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

	5.19			ISO 7816-3 2006 PPS Protocol Compliance		
	5.20			SM and OCC-AUTH		
SR-1	5.20.01	01	00	<p>The reader is set to SM-AUTH mode.</p> <p>Confirm the product's capability to reject credentials when buffer 0x1017 is missing.</p>	Access denied.	[800-73] Part1
SO-1	5.20.02	Production PIV	Common Policy Root	<p>Production PIV cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.3.39)</p>	Access granted.	
SO-1	5.20.03	Production PIV	Common Policy Root	<p>Production PIV cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.3.39)</p>	Access granted.	
SO-1	5.20.04	Production CAC	Common Policy Root	<p>Production CAC cards can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Root, and the following policies are required:  <i>__id-fpki-common-authentication</i> (2.16.840.1.101.3.2.1.3.13)  <i>__id-fpki-common-cardAuth</i> (2.16.840.1.101.3.2.1.3.17)  <i>__id-fpki-common-piv-contentSigning</i> (2.16.840.1.101.3.2.1.3.39)</p>	Access granted.	

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SO-1	5.20.06	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I card can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-common-pivi-authentication</u> (2.16.840.1.101.3.2.1.3.45)  <u>id-fpki-common-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.46)  <u>id-fpki-common-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.47)</p>	Access granted.	
SO-1	5.20.07	Production FI PIV-I	Common Policy Root	<p>Production Federal Issued (FI) PIV-I card can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-common-pivi-authentication</u> (2.16.840.1.101.3.2.1.3.45)  <u>id-fpki-common-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.46)  <u>id-fpki-common-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.47)</p>	Access granted.	
SO-1	5.20.08	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I card can be individually registered.</p> <p>SM-AUTH present using cipher suite '27'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-certpcy-pivi-hardware</u> (2.16.840.1.101.3.2.1.3.18)  <u>id-fpki-certpcy-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.19)  <u>id-fpki-certpcy-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.20)</p>	Access granted.	

SO-1	5.20.09	Production NFI PIV-I	Common Policy Root	<p>Production Non-Federal Issued (NFI) PIV-I card can be individually registered.</p> <p>SM-AUTH present using cipher suite '2E'.</p> <p>Trust anchor set to Common Policy Bridge, and the following policies are required:  <u>id-fpki-certpcy-pivi-hardware</u> (2.16.840.1.101.3.2.1.3.18)  <u>id-fpki-certpcy-pivi-cardAuth</u> (2.16.840.1.101.3.2.1.3.19)  <u>id-fpki-certpcy-pivi-contentSigning</u> (2.16.840.1.101.3.2.1.3.20)</p>	Access granted.	
------	---------	----------------------	--------------------	---	-----------------	--

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

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 and sequentially. 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 one at a time in order. 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 sequentially removed and immediately restored to individual components within the solution. The solution shall recover and uphold the requirements for authentication factors and authorizations for a valid credential.	Design analysis passes.	PCP-1
UO-3	7.01.04	05	00	The network connection is dropped to individual components within the solution one at a Time. The degraded mode shall honor requirements for authentication factors and authorizations for invalid credentials.	Design analysis passes.	PCP-1
UO-3	7.01.05	05	00	Individual component services within the solution are stopped one at a time, in sequence. The degraded mode shall honor requirements for authentication factors and authorizations for invalid credentials.	Design analysis passes.	PCP-1
UO-3	7.01.06	05	00	Power is sequentially removed and then immediately restored to individual components within the solution. The solution shall recover and uphold 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 sequentially, one at a time. The degraded mode shall honor the requirements for authentication factors and authorizations for a cloned credential.	Design analysis passes.	PCP-1
7.02		Security Boundaries				
SR-1	7.02.01			Confirm that all PACS components (excluding the reader and the bearer's credentials) can be located on the secure side of the perimeter. Confirm with protocol sniffing between the secure and attack sides.	...all security-related processing shall be conducted within the secure perimeter. No security-related decisions shall be made by system components that do not belong to the cardholder's credential when positioned on the attack side of the door.	PPE-1

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

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 verify them against relevant APLs and FIPS 140-3. Ensure that controls are operational through physical inspections and design documentation. Validate with protocol sniffing between the secure side and the attack side.	...compensating controls are applied, including tamper switches and FIPS 140-3 certified cryptographic processing within the reader.	PPE-1
	<b>7.03</b>			<b>Registering Physical Access Privileges</b>		
UO-3	7.03.01			The solution shall be able to define populations (validities) such as guests, visitors, and regular access.	Design analysis passes.	PPL-4
UO-3	7.03.02			The solution shall be able to define access points for each population.	Design analysis passes.	PPL-5, PAC-1
UO-3	7.03.03			The solution shall be able to define temporary access rules for each group.	Design analysis passes.	PPL-5, PAC-1
UO-3	7.03.04			The solution shall be able to define the authentication mode required to support 7.03.02 and 7.03.03.	Design analysis passes.	PPL-5, PAC-1
	<b>7.04</b>			<b>PKI Configuration</b>		
SO-1	7.04.01			The solution shall provide the ability to select which X.509 constraints are evaluated, including policy constraints, name constraints, and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify the configurability of X.509 constraints and policies.	PIA-5
SR-1	7.04.02			The solution shall provide the selection and management of Trust Anchors. This setup will align with the customer's PKI relying party policy.	Verify the configurability of trust anchors.	PSC-2
SO-1	7.04.03			The solution shall provide configuration options to disregard certificate PKI faults and end-entity to the trust anchor. This configuration will align with the customer's PKI relying party policy.	Conduct a design review of the vendor's PKI configuration options. If options are presented to ignore PKI faults, testing will advance to 7.04.04.	

SR-2	7.04.04			For every event where a PKI fault is identified, the solution will check the configuration options to ignore the identified fault. If the configuration allows the solution to bypass the fault, it will disregard the fault and produce a warning in the audit log, storing the certificate in a repository of failed certificates. The audit log will indicate what failed and provide sufficient information to link the log entry to the stored certificate.	Configure the system to ignore PKI faults individually, based on the solution's capabilities. Re-run the relevant ICAM card and PKI tests for both the registration time and the access time with the corresponding fault. Check logs and the associated certificate store. Ensure that the failure is accurately identified and that the certificate matches the log	
------	---------	--	--	--	---	--

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

					entry.	
SR-2	7.04.05			If PKI faults are permitted, the solution shall provide a way to generate a report and consolidate failed certificates for email transmission to relevant parties. Running the report and sending the email will be conducted in accordance with the customer’s PKI relying party policy.	Confirm the ability to generate reports and certificates to be sent by email.	
SR-1	7.04.06			The system shall check that the issuing certificate authority has not added the certificate to its certificate revocation list, using CRL or OSCP, within the previous 6 hours.	Confirm the solution can set CRL and OSCP response caching to 6 hours or less.	Fed 24-hour policy
	<b>7.05</b>			<b>Credential Number Specifications</b>		
UO-3	7.05.01	46	00	The solution should support a minimum of FICAM-conformant 128-bit FASC-N credential numbers, as specified in Table 3 for Time of Registration, Time of Access, and Automated Provisioning.	Configure the system for 128-bit FASC-N. Review the transactional test logs for registration and access. Confirm that all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into individual fields, the details will be sent to the GSA ICAM Lab for testing.	PAU-2, PAU-3; Table 6-1 row 3
UO-3	7.05.02	54	37	The solution should support a minimum of FICAM-conformant 128-bit UUID credential numbers, as specified in Table 3 for Time of Registration, Time of Access, and Automated Provisioning.	Configure the system for a 128-bit UUID. Review the transactional test logs for registration and access. Ensure that all operational usage is 128-bits and not parsed into separate fields. If the system parses the numbers into individual fields, the details will be provided to the GSA ICAM Lab for testing.	PAU-2, PAU-3; Table 6-1 row 3
	<b>7.06</b>			<b>Validation at Time of Access</b>		

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

7.07				Portal Hardware		
SR-1	7.07.01			The product shall support reader-to-PACS communication using bidirectional technology. This includes at least one RS-485 or Ethernet connection.	Verify through a system design review. Confirmation accomplished via protocol sniffing and an analysis of logs generated during authentication testing.	PCM-2, PCM-3
UR-3	7.07.02			For multi-factor readers, the applicant's system must enable an administrator to change the authentication mode (authentication factors) of an individual reader from either the server or a client/workstation to the server.	Verify through a system design review. Confirm by configuring multi-factor reader authentication modes while using Test Card 1: PIV Golden for access based on the selected mode.	PCM-3
UO-3	7.07.03			For multi-factor readers, the applicant's system must enable an administrator to modify a group of readers' authentication modes (authentication factors) from the server or from a client/workstation to the server.	Verify through a system design review. Confirm by configuring multi-factor reader authentication modes while using Test Card 1: PIV Golden for access based on the selected mode.	PCM-3
UR-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 through a system design review. Confirm by configuring multi-factor reader authentication modes while using Test Card 1: PIV Golden for access based on the selected mode.	PCM-3
UO-3	7.07.05			The system shall support the dynamic assignment of an individual reader's authentication mode (authentication factors) based on a time-based schedule for multi-factor readers.	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-3	7.07.06			The system shall support the dynamic assignment of a group of readers' authentication modes (authentication factors) based on a time-based schedule for multi-factor readers.	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

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

UO-2	7.07.07			For multi-factor readers, the system shall support dynamic assignment of each reader's authentication mode (authentication factors) according to a Threat Condition, Force Protection Condition, maritime security level, or other similar structured emergency response protocol.	Verify through a system design review. Confirm by setting the emergency response protocol level for multi-factor reader authentication modes and using Test Card 1: PIV Golden for access according to the mode.	PCM-3
UO-3	7.07.08			The system shall support the dynamic assignment of a group of readers' authentication modes (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocols for multi-factor readers.	Verify through a system design review. Confirm by setting the emergency response protocol level for multi-factor reader authentication modes and using Test Card 1: PIV Golden for access according to the mode.	PCM-3

UR-2	7.07.09			Contact readers shall support ISO/IEC 7816.	The reader's contact interface shall be tested for ISO/IEC 7816 conformance. The vendor is required to test with the most recent version of ISO/IEC 10373-3, which is 10373-3:2018. The vendor shall either provide a test data report documenting conformance or the Vendor Self-Attestation Form for ISO/IEC Test Reports for review and approval.	[FIPS 201]
UR-2	7.07.10			Contactless readers shall support ISO/IEC 14443 Type A.	The reader's contactless interface shall be tested for ISO/IEC 14443 Type A conformance. The vendor is required to test with the most recent version of ISO/IEC 10373-6, which is ISO/IEC 10373-6:2020 and ISO/IEC 10373-6:2020/Amd.1:2022. The vendor shall either provide a test data report documenting conformance or the Vendor Self-Attestation Form for ISO/IEC Test Reports for review and approval.	[FIPS 201]

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-3	7.07.11	Production PIV		ISO/IEC 14443 Type A contactless readers shall not activate or operate with a PIV card beyond 10 cm.	The Production PIV Card is presented to the reader at 11 cm. All contactless PIV authentication modes will not succeed.	[FIPS 201]
UR-3	7.07.12	Production PIV		ISO/IEC 14443 Type A contactless readers shall provide adequate field strength to activate and operate with a PIV card from a distance of at least 3.5 cm from the reader.	The Production PIV Card is presented to the reader at a size of 3.5 cm. All contactless PIV authentication modes will be successful.	[FIPS 201]
SO-3	7.07.13			The System shall safeguard communications between readers and the PACS by utilizing a cryptographically secure protocol.	If OSDP is utilized, it must be a secure OSDP (AES-128 or greater). Other approved federal encryption protocols are permitted.	PSC-1
UO-3	7.07.14			For multi-factor readers, a time delay exceeding 120 seconds for a reader to change modes will also be deemed non-compliant.	Verify by system design review	PCM-3
SR-1	7.07.15	Valid PIV	Common Policy Root	For readers that support two-factor authentication, configure the reader for one-factor and two-factor authentication simultaneously. Then, verify that it fails one-factor authentication.	Access denied.	
SR-1	7.07.16	Valid PIV	Common Policy Root	For readers that support three authentication factors, configure the reader to allow for one, two, and three factors simultaneously. Then, ensure it fails when attempting one-factor authentication.	Access denied.	
SR-1	7.07.17	Valid PIV	Common Policy Root	For readers that support three factors of authentication, configure the reader for one factor, two factors, and three factors simultaneously. Verify that it fails at two factors of authentication.	Access denied.	
	<b>7.08</b>			<b>Auditing and Logging</b>		
SR-2	7.08.01			Auditing records shall be granularly applied to the card and individual transactions. They 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, OMB M 21-31, and M 22-09
SR-1	7.08.02			- The product shall provide auditing and logging for all PKI processing, including: - Pass/fail results from a Challenge/Response - PDVAL - Disabling credentials based on PDVAL, expiration, or revocation	Verify by review of logs and reports; confirm by protocol sniffing	PAU-3, PAU-4, PAU-7, OMB M 21-31, and M 22-09

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

				status.		
SR-2	7.08.03			The product shall provide auditing and logging for the processing and transmission of credential numbers.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.04			The product shall provide auditing and logging for all software-driven configuration changes.	Verify by review of logs and reports	PAU-6, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.05			The product shall provide auditing and logging of periodic certificate PDVAL and status checks.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.06			The product shall provide auditing and logging of card activity (e.g., three days of card activity).	Verify by review of logs and reports	PAU-3, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.07			The product shall provide auditing and logging of the last known location of a card in the system.	Verify by review of logs and reports	PAU-3, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.08			The product shall provide auditing and logging of PKI policies regarding name constraints, path constraints, and validity checks.	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.09			The product shall provide auditing and logging of individual and group alarm reporting (e.g., door force, and door prop).	Verify by review of logs and reports	PAU-3, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.10			The product shall provide auditing and logging of the dates when individuals were provisioned or de-provisioned, along with the names of those responsible.	Verify by review of logs and reports	PAU-4, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.11			The product shall provide auditing and logging of all readers and their modes.	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7, OMB M 21-31, and M 22-09
SR-2	7.08.12			The product shall provide auditing and logging of the configuration download status to system components.	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7, OMB M 21-31, and M 22-09
	<b>7.09</b>			<b>Security Certification and Accreditation</b>		
UR-1	7.09.01			As specified by UL 294, the pertinent components in the solution must possess a UL 294 listing.	Verify the UL listing; it must be listed prior to final testing and certification by the FIPS 201 Evaluation Program.	PCA-2
UO-3	7.09.02			As specified by UL 1076 or UL 2610, which superseded UL 1076 on July 9, 2025, the relevant components within the solution must have a UL 1076 or UL 2610 listing	Verify the UL listing; it must be listed prior to final testing and certification by the FIPS 201 Evaluation Program.	PCA-2 derived

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

UO-3	7.09.03			As specified by UL 1981, applicable components within the solution must possess a UL 1981 listing.	Verify the UL listing; it must be listed prior to final testing and certification by the FIPS 201 Evaluation Program.	PCA-2 derived
UR-1	7.09.04			When adding a component to an existing system within a given topology, each current component in the system under that topology must have FIPS 201 Evaluation Program APL status.	Verify the APL listing, as it must be completed before the final testing and certification by the FIPS 201 Evaluation Program.	PCA-3
SR-1	7.09.05			Each component using cryptography in the system shall have FIPS 140-3 Overall Security Level 1 (or higher) certification. The operating environment for each component must correspond with at least one operating environment, such as the O/S version and processor type, found in a FIPS 140-2 certificate's security policy document. All cryptographic operations must be conducted exclusively with the FIPS 140-3 cryptographic modules as specified in the vendor attestation.	Verify the NIST CMVP listing. It must be applied for and in process for certification before any testing occurs. The listing must be finalized before the final testing and certification by the FIPS 201 Evaluation Program.	PCA-4, [FIPS 201]
SR-1	7.09.08			Ensure that all PACS and Validation System vendor software executables are signed by an entity whose certificate chain ends with a recognized public trust anchor.	All shared libraries and executables, including .MSI files, have been signed by a trusted source. At a minimum, these include all applications that the lab must launch or run to test the application against the FRTC.	[SP800-53]
	<b>7.10</b>			<b>Biometric in PACS</b>		
SR-2	7.10.01			Shall adhere to PIA-3.4 Detailed Guidance Case 3 for encrypting biometric identifiers used in BIO for PACS.	Ensure compliance through system design and database inspection. All PII and CUI information for cardholders must be safeguarded according to current federal standards for both data in transit and data at rest.	PIA-3.4
	<b>7.11</b>			<b>Operational Controls</b>		
SR-2	7.11.01			The system must be able to enforce administrative privileges for configuration management operations.	Check using the system.	PCM-1
SR-2	7.11.02			Administrators shall be authenticated using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done with credentials complying with NIST SP 800-63.	Check using the system.	PCM-1

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

UO-3	7.11.03			The system shall be able to be managed through software-controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only, not for management of the hardware tree.	Check using the system.	PCM-2
UO-3	7.11.04			Each physical component shall be clearly defined and accessible within the server user interface.	Check by configuring the system.	PCM-2
UO-3	7.11.05			The system shall support configuration downloads to the appropriate components.	Check by configuring the system.	PCM-2
	<b>7.12</b>			<b>Accessibility</b>		
UR-2	7.12.01			SECTION 508 COMPLIANCE. Offerors must self-certify that their products or services comply with Section 508 technical standards. Consequently, the offeror must submit with its offer a designated area on its website that outlines the Voluntary Product Accessibility Template (VPAT) or an equivalent qualification, which ultimately becomes the Government Product Accessibility Template (GPAT).	Review VPAT from application.	[Sect 508]

	<b>8.0</b>			<b>Handheld Requirements</b>		
	<b>8.01</b>			<b>Communications</b>		
SR-1	8.01.01			Ensure the handheld uses a secure connection using an encrypted wireless session using a FIPS 140-2/140-3 level 2 certified encryption method.	Verify within the handheld settings that there is an option to encrypt communications using NIST approved methods.	
SR-1	8.01.02			At a minimum, must have built-in support for Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2).	Verify within the handheld settings that the interface supports a minimum of WPA. WPA-2 is preferred.	
SR-1	8.01.03			At a minimum, the system has the ability to communicate using Wi-Fi 5	Verify within the handheld settings that the wireless interface supports one of the listed protocols.	
SR-1	8.01.04			The Handheld must be able to support at minimum 3G or 4G LTE communications is operating under cellular communications.	Verify within the handheld settings that the option for 3G or 4G communications exists.	

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	8.01.05			Handheld must have the ability to demonstrate the option to select a primary communication source and a secondary communication source.	Verify the reader interface allows the devices to be configured for a primary and secondary method of communications.	
SR-1	8.01.06			Handheld must be able to failover from primary to secondary mode to maintain an online state with PACS and Validations system.	Verify that if wireless communications are lost, the reader attempts to connect to secondary mode of communications.	

SR-1	8.01.07			Reader provides a visual indication that the handheld is in an online or offline state. .	Verify the reader provides an indication that the reader is in an offline state.	
------	---------	--	--	---	--	--

	<b>8.02</b>			<b>Operational Requirements</b>		
--	-------------	--	--	---------------------------------	--	--

UR-1	8.02.01			The handheld is capable of supporting contactless, contact, or both modes of authentication. Interfaces can be fully integrated or modular.		
UR-1	8.02.02			Contactless modes must support a minimum of: PKI-CAK.		
UR-1	8.02.03			Contact modes must support a minimum of: PKI-CAK.		
UR-1	8.02.05			Contact modes must support a minimum of: PIV-Auth + PIN.		
UR-1	8.02.06			Contact modes must support a minimum of: PIV-Auth + PIN + Fingerprint.		
UR-1	8.02.07			Contact modes must support a minimum of: PIV-Auth + PIN + Facial Authentication.		

	<b>8.03</b>			<b>Docking Station</b>		
--	-------------	--	--	------------------------	--	--

UR-1	8.03.01			The handheld docking station must utilize a hardwired Ethernet port or wireless communications with the Validation System, PACS, or other trusted source.		
------	---------	--	--	---	--	--

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	8.03.02			<p>The handheld docking station provides a mechanism to securely update the handheld while cradled in the device, via hardwired Ethernet or Wireless communications.</p> <p>Updates can be from online validation system, PACS or other trusted source.</p> <p>Secure communication enforced by mutual authentication TLS with PKI.</p>	Design analysis passes.	
SR-1	8.03.03			Handheld must automatically logout operator when placed in docking station.	Design analysis passes.	
SR-1	8.03.04			Ensure the docking station uses a secure connection using an encrypted wireless session using a FIPS 140-2 level 2 certified encryption method.		

SR-1	8.03.05			The docking station must be able to support at minimum 3G or 4G LTE communications is operating under cellular communications.		
	<b>8.04</b>			<b>FINGERPRINT Verification</b>		
SO-1	8.04.01			<ul style="list-style-type: none"> <li>• See Section 2 – Validation at time of Registration</li> <li>• See Section 5 – Validation at time of Access.</li> </ul>		
SO-1	8.04.01			<ul style="list-style-type: none"> <li>• See Section 2 – Validation at time of Registration</li> <li>• See Section 5 – Validation at time of Access.</li> </ul>		
	<b>8.05</b>			<b>Import Function</b>		
UR-1	8.05.01			<p>Reader must cache CRL information locally on the handheld.</p> <p>This CRL data must include the Certificate PATH information and be supplied by an online Validation System or other trusted source.</p>		
SR-1	8.05.02			Cached information must be protected either by a FIPS140-2/140-3 Level 1 software or Level 2 HSM.	Design analysis passes.	
SR-1	8.05.03			The reader must cache authentication and authorization information for all cardholders with access to the Handheld assigned area. This information can be transferred from either an online validations system or other trusted source. .		
SR-1	8.05.04			The Handheld device must have the ability to provide a visual indication when locally cached information is over 6 hours old.	Design analysis passes.	

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

	<b>8.06</b>			<b>Operational</b>		
SR-1	8.06.01			System must automatically log the operator out of the handheld after a user defined time of non-use.	Design analysis passes.	
	<b>8.07</b>			<b>Online Validation Requirements</b>		
SR-1	8.07.01			When the Handheld is online communicating with the Validations System, functional requirements defined within the Validation System category apply.		
	<b>8.08</b>			<b>Online PACS Integration Requirements</b>		
SR-1	8.08.01			When the Handheld is online communicating with the PACS, the PACS functional requirements defined in the PACS Infrastructure category apply.		
	<b>8.09</b>			<b>Offline Validation Requirements</b>		
SR-1	8.09.01			Handheld must use locally cached authentication and authorization data to authenticate and authorize the operator.		
SR-1	8.09.02			Handheld must be able to determine the validity of the cardholder certificates using the locally cached validation data.		
SR-1	8.09.03			Handheld must provide the operator with indication that the locally stored data exceeds 6-hour refresh limit.		
SR-1	8.09.04			Handheld must cache PKI Validation decisions to be uploaded to the trusted source for archive and reporting.		
	<b>8.10</b>			<b>Offline PACS Integration Requirements</b>		
SR-1	8.10.01			The handheld must provide an indication to the operator that the reader is in offline mode.	Design analysis passes.	
SR-1	8.10.02			The handheld must be able to use locally cached PACS data to verify cardholders access privileges. For example: <ul style="list-style-type: none"> <li>• Schedule</li> <li>• Shift</li> <li>• Access to areas</li> </ul> The operator must be provided a visual indication of access granted or denied.		
SR-1	8.10.03			While in offline mode the handheld must log all access decisions made at the handheld.		

**PACS Functional Requirements and Test Cases**

**v1.4.2 Rev. D**

SR-1	8.10.04			When transitioning from an offline to an online state the handheld must transfer all locally stored access transaction to the PACS solution or other trusted source.	Design analysis passes.	
------	---------	--	--	--	-------------------------	--