# Functional Requirements and Test Cases (FRTC) for Physical Access Control Systems (PACS) Alternative Authenticators

VERSION 1.0


## FIPS 201 EVALUATION PROGRAM

**September 26, 2023**

Office of Government-Wide Policy
Office of Technology Policy
Identity Assurance and Trusted Access Division
Washington, DC 20405

# Document History

| Status | Version | Date | Comment | Audience |
|---|---|---|---|---|
| Draft | 0.1.0 | 5/22/23 | Document creation. Draft test cases based on using only the Card Authentication Key (CAK) relying on the contactless interface of the Alternative PIV Token. | Limited |
| Draft | 1.0 | 07/28/23 | Updated document to reflect comments from reviewers | Limited |
| Final | 1.0 | 09/26/2023 | Publish to IDManagement.gov for review and comments. | Public |

# Table of Contents

1 Background and Introduction 3
1.1 Test Assumptions 3
1.2 Definitions 3
2 Change Control 4
3 Objectives 4
4 Functional Testing 5
4.1 ICAM Card Data Used for Testing 5
4.2 PKI Used in Test 6
4.3 Alternative Authenticators Used for Testing 7
5 Credential Number Processing 7
6 Functional Requirements and Test Cases 9
6.1 Severity Levels 9
6.2 APL Listing Requirements 9
6.3 Classification Codes and Scoring Guidelines 10
6.4 Test Results 11
7 Topics for Further Cosideration 12
7.1 Time of Registration/Enrollment 12
7.2 Time of Access 12
7.3 Mobile Phones 12
7.4 Other Authenticators Considerations 12
8 Normative References 13
9 Functional Requirements and Test Cases Matrix 15

# List of Tables

Table 1 – ICAM Test Card Data Used for Testing 5
Table 2 – ICAM PKI Path Descriptions 6
Table 3 – Vendor/Model of Alternative PIV Tokens Used for Testing 7
Table 4 – Minimal Set of Credential Number Processing Rules 8
Table 5 – APL Listing Based on Test Level and Classification 9
Table 6 – Severity Remediation Timeframes 10
Table 7 – Classification Codes 10
Table 8 – Impact Guidelines 11
Table 9 – Possible Test Results 11
Table 10 – Functional Requirements and Test Cases Matrix 15

# 1 Background and Introduction

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

This document specifies the functional tests the FIPS 201 Evaluation Program performs on a Physical Access Control System (PACS) submitted for compliance evaluation – a precursor to being added to the APL.

All tests use Alternative Authenticators that support ISO 14443, the PIV Applet, and various Public Key Infrastructure (PKI) paths.

The PKI and Alternative Authenticators are tested for specific common failures in tokens, PKI, and issues that impact PACS specifically.

PACS evaluation focuses solely on functional testing using an end-to-end testing methodology. There is no evaluation of the PACS topology/architecture itself.

## *1.1 Test Assumptions*

1. Alternative Authenticators use the PIV Applet – not the Derived PIV Applet.
2. The only authenticator on Alternative Authenticators is PKI-CAK.
3. Alternative Authenticators comply with the ISO 14443 Near Field Communication (NFC) standard.
4. Mobile phones are out of scope for this Alternative Authenticators testing version.
5. Test Cases based solely on form factor type are out of scope.

## *1.2 Definitions*

| Term | Definition |
|---|---|
| Alternative Authenticator | FIPS 140 certified token that can import a PKCS #12 file (.p12 file extension) that supports ISO 7816 and ISO 14443 (NFC) as well as the PIV Applet. |
| No-fault Alternative Authenticator | Entirely valid and well-formed Alternative test authenticator. |
| Functional Testing | Test cases for testing application functionality (black box testing). Uses elements put in place to emulate a real-world environment and specific operational scenarios. Expected results are tested against actual results |
| PKI Path | Required trust path for the test case. |
| No-fault PKI Path | PKI path conforming with NIST SP 800-73-4 data model. |

# 2 Change Control

This document will be updated over time as new, revised, and deprecated functional requirements are identified, and the associated test cases are added, updated, or deleted. In addition, this document will be updated if security or infrastructure risks are identified, and an interim release may occur.

All new versions of this document are effective immediately. Solutions currently being tested in the lab must meet the updated requirements during testing. Systems already on the Approved Products List (APL) must meet the updated requirements within the remediation timeframe commensurate with their assigned severity level (see Section 6) or be moved to the Removed Products List (RPL). See [RPL] for process details.

# 3 Objectives

The objective of this document is to specify the Alternative Authenticator vendors/models that may be used for testing[1] and the functional requirements and test cases needed to ensure PACS compliance.

[1] NIST NPIVP Test Facility has no method to approve alternative PIV form factors.

# 4 Functional Testing

PACS evaluation relies on fully defined functional requirements. This requires two core elements:

1. ***ICAM Test Alternative Authenticators*** – Tokens configured to provide a mixture of positive and negative test cases. Tokens are injected with either valid operational scenarios reflecting day-to-day operational errors or invalid scenarios (faults) reflecting a well-funded attacker. Currently, Alternative Authenticators are solely hardware-based.
2. ***ICAM Test PKI Paths*** – Provides the ability to link Alternative Authenticators with PKI faults, which provides the mechanism needed to verify that the system under test performs path discovery and validation (PD-VAL) of the PKI.

The test cases described in Section 8 are based on these functional requirements.

## *4.1 ICAM Card Data Used for Testing*

The data provisioned onto the test Alternative Authenticators is from the *ICAM Test Card Signer and Data Populator* published on the GSA Github Repository. *Table 1* describes the ICAM card data provisioned onto the test tokens used for the FIPS 201 Evaluation Program.

*Table 1 – ICAM Test Card Data Used for Testing*

| ***Source ICAM Test Card*** | ***Data Description*** | ***Fault Type*** |
|---|---|---|
| 05 | Tampered PIV and Card Authentication Certificates. | Manipulated Data |
| 10 | Expired certificate signer. | Invalid Date |
| 12 | Card Authentication certificate not valid until a future date. | Invalid Date |
| 13 | Expired Card Authentication certificate. | Invalid Date |
| 16 | Valid Card Authentication Certificate copied from one card to another (PIV). | Copied Credential |
| 23 | Card Authentication Certificate Private and Public Key mismatch. | Manipulated Keys |
| 37 | No-fault Card Authentication certificate with a valid PPS F=512, D=64 (625,000 baud), ECC Card Auth Cert. | No Fault |
| 41 | Public key does not match public key previously registered to the system. | Copied Container |
| 42 | Card Authentication certificate refers to an OCSP responder that uses an expired response signing certificate. | Invalid Date |
| 43 | Card Authentication certificate refers to an OCSP responder that uses a response signing certificate that is revoked but contains the *id-pkix-ocsp-nocheck* OID. | Invalid Credential |

| *Source ICAM Test Card* | *Data Description* | *Fault Type* |
|---|---|---|
| 44 | Card Authentication certificate refers to an OCSP responder that uses a response signing certificate that is revoked, and the *id-pkix-ocsp-nocheck* OID is not present. | Invalid Credential |
| 45 | Card Authentication certificate refers to an OCSP responder that uses a response signing certificate with an invalid signature. | Manipulated Data |
| 46 | No-fault Card Authentication certificate with card UUIDs in the SubjectAltName extensions are sequentially after the FASC-N (replaces Card 1). | None |
| 47 | No-fault Card Authentication certificate with card UUIDs in the SubjectAltName extensions are sequentially before the FASC-N. | No Fault |
| 53 | No-fault Card Authentication certificate profile with a slightly larger than recommended Card Authentication Certificate (2160 bytes). | No Fault |
| 58 | Card Authentication certificate with a revoked Card Authentication certificate. | 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 #* | *Fault Description* |
|---|---|
| 00 | No fault PKI path conforming with NIST SP 800-73-4 data model |
| 01 | ICAM Invalid CA Signature |
| 02 | ICAM Invalid CA *notBefore* Date |
| 03 | ICAM Invalid CA *notAfter* Date |
| 04 | ICAM Invalid Name Chaining |
| 05 | ICAM Missing Basic Constraints |
| 06 | ICAM Invalid CA False Critical |
| 07 | ICAM Invalid CA False not Critical |
| 08 | ICAM Invalid Path Length Constraint |
| 09 | ICAM *keyUsage keyCertSign* False |
| 10 | ICAM keyUsage Not Critical |
| 11 | ICAM *keyUsage* Critical *CRLSign* False |
| 12 | ICAM Invalid *inhibitPolicyMapping* |
| 13 | ICAM Invalid DN *nameConstraints* |

| ICAM PKI Path # | Fault Description |
|---|---|
| 14 | ICAM Invalid SAN *nameConstraints* |
| 15 | ICAM Invalid Missing CRL |
| 16 | ICAM Invalid Revoked CA |
| 17 | ICAM Invalid CRL Signature |
| 18 | ICAM Invalid CRL Issuer Name |
| 19 | ICAM Invalid Old CRL *nextUpdate* |
| 20 | ICAM Invalid CRL *notBefore* |
| 21 | ICAM Invalid CRL Distribution Point |
| 24 | ICAM Valid GeneralizedTime |
| 25 | ICAM Invalid GeneralizedTime |
| 33 | ICAM Invalid AKID |
| 34 | ICAM Invalid CRL format |
| 36 | ICAM Invalid CRL Signer |

### 4.3 Alternative Authenticators Used for Testing

Any token that meets the Alternative Authenticator definition specified in *Section 1.2, Definitions* may be used for PACS testing. *Table 3* is the list of Alternative Authenticator vendors/models currently used for testing.

*Table 3 – Vendor/Model of Alternative Authenticators Used for Testing*

| Vendor | Model | Description |
|---|---|---|
| Yubico | YubiKey 5 NFC FIPS | FIPS 140-2 validated (Overall Level 2, Physical Security Level 3) and meets authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance (Government Certified). Has a USB-A connector and can communicate wirelessly via Near Field Communication (NFC). |
| Yubico | YubiKey 5C NFC FIPS | FIPS 140-2 validated (Overall Level 2, Physical Security Level 3) and meets authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance (Government Certified). Has a USB-C connector and can communicate wirelessly via Near Field Communication (NFC). |

# 5 Credential Number Processing

*Table 4* describes the minimal set of credential number processing rules. All solutions shall use 128-bit (16 bytes) credential numbers to provide complete protection against credential number collisions and 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 Case 7.05.01). If the system parses the numbers into separate fields, they must be stored for the 128-bit credential to 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 4 – Minimal Set of Credential Number Processing Rules*

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

# 6 Functional Requirements and Test Cases

## 6.1 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.

## 6.2 APL Listing Requirements

*Table 5* 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 with a Severity 1 or Severity 2 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 5 – 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? |
|---|---|---|---|---|---|---|
| ***Security*** | Pass | ✔ | Pass | ✔ | Pass | ✔ |
| | Fail | ✘ | Fail | ✘ | Fail | ✔ |
| ***Usability*** | Pass | ✔ | Pass | ✔ | Pass | ✔ |
| | Fail | ✘ | Fail | ✘ | Fail | ✔ |

*Table 6* 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 *Table 8*.

*Table 6 – Severity Remediation Timeframes*

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

## 6.3 Classification Codes and Scoring Guidelines

The FRTC includes a classification code for each test case. The classification code indicates 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 7* describes the classification codes.

*Table 7 – Classification Codes*

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

*Table 8 – Impact Guidelines*

| | High Impact | Moderate Impact | Low Impact |
|---|---|---|---|
| **Security** | 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]) |
| **Operations** | Unable to manage or use the PACS to the extent that PACS use is severely diminished, inconvenient, or unreliable | Unable to manage or use the PACS to the extent that PACS use is seriously diminished, inconvenient, or unreliable | Unable to manage or use the PACS to the extent that PACS use is slightly diminished or inconvenient |
| **Availability** | The PACS is down for significant lengths of time, precluding entry into facilities/areas during that time | The PACS is down frequently for limited lengths of time, precluding entry into facilities/areas during those somewhat frequent times | The PACS is down infrequently for limited lengths of time, precluding entry into facilities/areas during those times |

## 6.4 Test Results

Each test case in *Table 10* must be accounted for in a Test Results Report. *Table 9* describes the possible test results each test case may have.

*Table 9 – Possible Test Results*

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

# 7 Topics for Further Cosideration

## 7.1 Time of Registration/Enrollment

Does your PACS registration/enrollment system have a different credential registration that would either:

1. Register/Enroll the PACS alternative (non-PIV with PKI) authenticator independently
2. Register/Enroll the PACS alternative (non-PIV with PKI) authenticator as an additional credential to an existing PACS user

## 7.2 Time of Access

1. What additional authenticator objects would a PACS reader require, beyond what is required for Registration/Enrollment?

## 7.3 Mobile Phones

1. Would a mobile phone solution require that it emulate a smart card?
2. Would this require a container like a virtual smart card respond to card edge commands vs. logical access that only requires a certificate to authenticate?

## 7.4 Other Authenticators Considerations

1. Besides the PKI-CAK, would this PACS alternative authenticator need a properly formed and digitally signed CHUID?
2. Would any of the fields in the CHUID need to match any previously registered PIV cards?
3. Would the CCC container be required?
4. Would the Discovery Object be required?
5. Is the printed information data object (container) required for the population of the user account fields at registration/enrollment? If not required, is the recommended because it provides trusted source of user information between the issuer and the authenticator?
6. Are there additional authenication objects for the alternate authenticator to be recommended when used with the APL-approved 13.01 or 13.02 solutions?

# 8 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, Version 2.3, September 9, 2022, or as amended
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

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

**[FBCA]** X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), Version 3.0, October 19, 2022, or as amended
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf

**[FIPS 201]** Federal Information Processing Standard 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors
https://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

**[PROF]** Common Policy X.509 Certificate and Certificate Revocation list (CRL) Profiles, Version 2.2, September 2022, 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, NST Special Publication 800-73-4, May 2015 or as amended
https://csrc.nist.gov/publications/detail/sp/800-73/4/final

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

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

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

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

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

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

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

**[VPAT]** Voluntary Product Accessibility Template Version 2.4 Rev 508 – the U.S. Federal accessibility standard, March 2022
VPAT 2.4Rev 508 (March 2022)

# 9 Functional Requirements and Test Cases Matrix

*Table 10 – Functional Requirements and Test Cases Matrix*

| Classification | Test Case # | PKI-CAK from 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** | | **Note all requirements sourced from [E-PACS] unless otherwise noted.** |
| | **2.01** | | | **Signature Verification** | | |
| SR-1 | 2.01.01 | 46 | 00 | Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential. | Registration succeeds. | PIA-2 thru PIA-7 |
| SR-1 | 2.01.02 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first. | Registration succeeds. | PIA-2 thru PIA-7 |
| SR-1 | 2.01.03 | 16 | 01 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize invalid signature on an intermediate CA in the certification path. | Registration fails. | PIA-3.2, PIA-3.4, PIA-4, PIA-5 |
| | **2.02** | | | **Certificate Validity Periods** | | |
| SR-1 | 2.02.01 | 16 | 02 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when *notBefore* date of the intermediate CA certificate is sometime in the future. | Registration fails. | PIA-3.5, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.02.02 | 10 | 00 | Register alternative token 10 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when *notAfter* date of the End Entity Signing CA is sometime in the past. | Registration fails. | PAI-3.2, PIA-3.4, PIA-4 |
| SR-1 | 2.02.03 | 12 | 00 | Register alternative token 12 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future. | Registration fails. | PIA-3.5 |
| SR-1 | 2.02.04 | 16 | 03 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when *notAfter* date of the intermediate certificate is sometime in the past. | Registration fails. | PIA-3.5, PIA-5 |
| SR-1 | 2.02.05 | 13 | 00 | Register alternative token 13 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past. | Registration fails. | PIA-3.5 |
| | **2.03** | | | **Name Chaining** | | |
| SR-1 | 2.03.01 | 16 | 04 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate. | Registration fails. | PIA-3.2, PIA-5 |
| | **2.04** | | | **Basic Constraints** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.04.01 | 16 | 05 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the intermediate CA certificate is missing Basic Constraints extension. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.04.02 | 16 | 06 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the Basic Constraints extension is present and critical in the intermediate CA certificate but the cA component is false. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.04.03 | 16 | 07 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the Basic Constraints extension is present and not critical in the intermediate CA certificate but the cA component is false. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.04.04 | 16 | 08 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the first certificate in the path includes Basic Constraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate. | Registration fails. | PIA-3.2, PIA-5 |
| | **2.05** | | | **Key Usage Verification** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.05.01 | 16 | 09 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which *keyCertSign* is false. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.05.02 | 16 | 10 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the intermediate certificate includes a non-critical Key Usage extension and rejects the path because a CA's Key Usage extension must always be marked critical. | Registration fails. | PIA-3.2, PIA-5, [PROF] Worksheet 3 |
| SR-1 | 2.05.03 | 16 | 11 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which *crlSign* is false. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.05.04 | 16 | NEW | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to recognize when intermediate certificate includes Key Usage extension *keyCertSign* and *crlSign* false, and Key Usage not critical. | Registration fails. | PIA-3.2, PIA-5 |
| | **2.06** | | | **Certificate Policies** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.06.01 | 16 | 12 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With required policy set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11), verify product's ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings. | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.06.02 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With the trust anchor set to ICAM Test Card PIV Root CA, verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for the PIV Authentication Certificates will be set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11) by the relying party solution. | Registration succeeds. | PIA-3.2, PIA-5 |
| SR-1 | 2.06.03 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With the trust anchor set to ICAM Test Card PIV Root CA, verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-cardAuth* (2.16.840.1.101.3.2.1.48.13) by the relying party solution. | Registration succeeds. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.06.04 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With the trust anchor set to ICAM Test Card PIV Root CA, verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.48.86) by the relying party solution. | Registration succeeds. | PIA-3.2, PIA-5 |
| SR-1 | 2.06.05 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With the trust anchor set to ICAM Test Card PIV Root CA, verify the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 2.3.4.5). | Registration fails. | PIA-3.2, PIA-5 |
| SR-1 | 2.06.06 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>With the trust anchor set to ICAM Test Card PIV Root CA, verify the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 3.4.5.6). | Registration fails. | PIA-3.2, PIA-5 |
| | **2.07** | | | **Generalized Time** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.07.01 | 16 | 24 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to process valid use of generalized time post year 2049 in the path. | Registration succeeds. | PIA-3.2, PIA-5 |
| SR-1 | 2.07.02 | 16 | 25 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify product's ability to process invalid use of generalized time before year 2049 in the path. | Registration fails. | PIA-3.2, PIA-5 |
| | **2.08** | | | **Name Constraints** | | |
| SR-1 | 2.08.01 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree. | Registration succeeds. | PIA-3.2, PIA-5 |
| SR-1 | 2.08.02 | 16 | 13 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree. | Registration fails. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.08.03 | 16 | 14 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree. | Registration fails. | PIA-3.2, PIA-5 |
| | **2.09** | | | **Certificate Revocation Tests (CRL)** | | |
| SR-1 | 2.09.01 | 16 | 15 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify 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 | 16 | 16 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify 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 | 16 | 18 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.04 | 16 | 19 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when a certificate in the path points to a CRL with an expired *nextUpdate* value (an expired CRL). | Registration fails. | PIA-3.5, PIA-5, PIA-7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.09.05 | 16 | 20 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when a certificate in the path points to a CRL with a *notBefore* Date in the future. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.06 | 16 | 21 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when a certificate in the path has an incorrect CRL distribution point. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.07 | 16 | 17 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the CRL has an invalid signature. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.08 | 16 | 34 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when an incorrectly formatted CRL is present in the path. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.09 | 16 | 36 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when an invalid CRL signer is in the path. | Registration fails. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 2.09.10 | 58 | 00 | Register alternative token 58 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the Card Authentication Certificate is revoked. | Registration fails. | [SP 800-73], PIA-3, PIA-3.2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.09.11 | 58 | 00 | Register alternative token 58 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the end-entity Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available. | Registration fails. | [SP 800-73], PIA-3, PIA-3.2 |
| SR-1 | 2.09.12 | 58 | 00 | Disable revocation checking before registering alternative token 58 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Turn revocation checking back on and have the system verify validity status of existing credentials. Verify the system recognizes when the Card Authentication Certificate is revoked, but Card 46 is not revoked. AIA to OCSP is not available and crlDP to CRL is available. Credential associated with 58 is disabled, but 46 remains operational. | Registration succeeds, but 58 disabled when revocation status is checked. | [FIPS 201] §2.9.4, [SP 800-73], PIA-3, PIA-3.2 |
| | **2.10** | | | **CHUID Verification** | | |
| | **2.11** | | | **Facial Image Verification** | | |
| | **2.12** | | | **Copied Containers** | | |
| | **2.13** | | | **Fingerprint Verification** | | |
| | **2.14** | | | **Security Object Verification** | | |
| | **2.15** | | | **OCSP Response Checking** | | |
| SR-1 | 2.15.01 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system successfully validates a good credential using an OCSP response with a good signature. | Registration succeeds. | PIA-3.2, PIA-3.5 |
| SR-1 | 2.15.02 | 58 | 00 | Register alternative token 58 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the Card Authentication Certificate is not expired but is revoked; AIA to OCSP is available and crlDP to CRL is not available. | Registration fails. | PIA-3.2, PIA-4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.15.03 | 58 | 00 | Disable revocation checking before registering alternative token 58 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Turn revocation checking back on and have the system verify validity status of existing credentials. Verify the system recognizes when the Card Authentication Certificate is revoked, but Card 46 is not revoked. AIA to OCSP is available and crlDP to CRL is not available. Credential associated with 58 is disabled, but 46 remains operational. | Registration succeeds, but 58 disabled when revocation status is checked. | [FIPS 201] §2.9.4, [SP 800-73], PIA-3, PIA-3.2 |
| | **2.16** | | | **Interoperability Testing** | | |
| SO-1 | 2.16.01 | 46 | 00 | Register CAK from Card 46, then verify the system recognizes a 14-decimal-digit FASC-N and uses this as the primary Identifier.<br><br>Note: Although this test case is optional, this test case or test case 2.16.02 is required. | Registration succeeds. | PIA-6, [SP 800-116] Appendix E |
| SO-1 | 2.16.02 | 46 | 00 | Register CAK from Card 46, then verify the system recognizes a full 16-byte Card UUID and uses this as the primary Identifier.<br><br>Note: Although this test case is optional, this test case or test case 2.16.01 is required. | Registration succeeds. | PIA-6, [SP 800-116] Appendix E |
| SR-1 | 2.16.03 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when the Extended Key Usage extension keyPurposeId OID *id-PIV-cardAuth* (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate. | Registration succeeds. | [FIPS 201] |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 2.16.04 | 16 | 00 | Register alternative token 16 as secondary credential to the same PACS identity that was created when Card 46 was registered. Requires 2.01.01 test to be completed first.<br><br>Verify the system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID *id-PIV-cardAuth* (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate. | Registration fails. | [FIPS 201] |
| | **2.17** | | | **Cryptography Testing** | | |
| | **2.18** | | | **Discovery Object and PIN Usage Policy** | | |
| | **2.20** | | | **SM and OCC-AUTH** | | |
| | **4.0** | | | **Requirements for Automated Provisioning, Deprovisioning, and Modifications, In Accordance With [E-PACS] PIA-8** | | **Note all requirements sourced from [E-PACS] unless otherwise noted.** |
| UR-2 | 4.01.01 | | | Verify E-PACS accepts 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 | | | Verify E-PACS accepts 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 | | | Verify E-PACS accepts 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 | | | Verify E-PACS supports a secure channel (e.g., mutual-auth over TLS) for all transactions with the trusted source. | Design analysis passes. | PIA-8; [Roadmap], §9.2.3.1 including Figure 94 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **5.0** | | | **Authentication at Time of Access Test Cases** | | |
| | **5.01** | | | **Signature Verification** | | |
| SR-1 | 5.01.01 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-CAK credential. | Access granted. | PIA-2 thru PIA-7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.01.02 | 16 | 01 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize invalid signature on an intermediate CA in the certification path. | Access denied. | PAI-3.2, PIA-3.4, PIA-4, PIA-5 |
| SR-1 | 5.01.03 | 05 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize invalid signature on the End Entity certificate (Invalid: Certificate Signature is Invalid).<br><br>This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access. | Access denied. | PAI-3.2, PIA-3.4, PIA-4 |
| SR-1 | 5.01.04 | 23 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize certificate/private key mismatch. | Access denied. | PAI-3.2, PIA-3.4, PIA-4 |
| SR-1 | 5.01.05 | 41 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize public key from card does not match public key previously registered to the system.<br><br>This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access. | Access denied. | PIA-3.2 |
| SR-1 | 5.01.06 | 53 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system successfully handles cards with a slightly larger than recommended Card Authentication Certificate (2160 bytes). | Registration succeeds. | [SP800-73] |
| | **5.02** | | | **Certificate Validity Periods** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-3 | 5.02.01 | 16 | 02 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to reject a credential when the *notBefore* date of the intermediate CA certificate is sometime in the future. | Access denied. | PIA-3.5, PIA-5 |
| SR-2 | 5.02.02 | 12 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to reject a credential when *notBefore* date of the End Entity certificate is sometime in the future.<br><br>This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access. | Access denied. | PIA-3.5 |
| SR-1 | 5.02.03 | 16 | 03 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to reject a credential when notAfter date of *any* certificate in the path is sometime in the past. | Access denied. | PIA-3.5, PIA-5 |
| SR-1 | 5.02.04 | 13 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to reject a credential when *notAfter* date of the End Entity certificate is sometime in the past.<br><br>This shall not be tested when the solution leverages a cached copy of the public key extracted at time of registration for signature verification at time of access. | Access denied. | PIA-3.5 |
| | **5.03** | | | **Name Chaining** | | |
| SR-1 | 5.03.01 | 16 | 04 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's' ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate. | Access denied. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **5.04** | | | **Basic Constraints** | | |
| SR-1 | 5.04.01 | 16 | 05 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the intermediate CA certificate is missing the Basic Constraints extension. | Access denied. | PIA-3.2, PIA-5 |
| SR-3 | 5.04.02 | 16 | 06 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the Basic Constraints extension is present and critical in the intermediate CA certificate but the *cA* component is false. | Access denied. | PIA-3.2, PIA-5 |
| SR-3 | 5.04.03 | 16 | 07 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the Basic Constraints extension is present and not critical in the intermediate CA certificate but the *cA* component is false. | Access denied. | PIA-3.2, PIA-5 |
| SR-1 | 5.04.04 | 16 | 08 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the first certificate in the path includes Basic Constraints extension with a *pathLenConstraint* of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate. | Access denied. | PIA-3.2, PIA-5 |
| SR-3 | 5.04.06 | 16 | 33 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to detect a mismatched AKID with the authority (issuer) public key in the certificate. | Access denied. | PIA-3.2, PIA-5 |
| | **5.05** | | | **Key Usage Verification** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.05.01 | 16 | 09 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which keyCertSign is false. | Access denied. | PIA-3.2, PIA-5 |
| SR-3 | 5.05.02 | 16 | 10 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the intermediate certificate includes a non-critical Key Usage extension and rejects the path because a CA's Key Usage extension must always be marked critical. | Access denied. | PIA-3.2, PIA-5, [PROF] Worksheet 3 |
| SR-1 | 5.05.03 | 16 | 11 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when the intermediate certificate includes a Key Usage extension in which crlSign is false. | Access denied. | PIA-3.2, PIA-5 |
| SR-1 | 5.05.04 | 16 | NEW | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to recognize when intermediate certificate includes Key Usage extension *keyCertSign* and *crlSign* false, and Key Usage not critical. | Access denied. | PIA-3.2, PIA-5 |
| | **5.06** | | | **Certificate Policies** | | |
| SR-2 | 5.06.01 | Valid PIV | Common Policy Root | With the trust anchor set to Common Policy, verify the validation software is able to recognize when an explicit certificate policy is required and present in the PIV Authentication certificate path. The explicit policy will be set to *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.3.13) by the relying party solution. | Access granted. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.06.02 | Valid PIV | Common Policy Root | With the trust anchor set to Common Policy, verify the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the PIV Authentication certificate path (e.g., OID value 1.2.3.4). | Access denied. | PIA-3.2, PIA-5 |
| SR-1 | 5.06.03 | Valid PIV | Common Policy Root | With Common Policy anchor, verify the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path but does not map to the end entity certificate such as *id-fpki-common-High* (2.16.840.1.101.3.2.1.3.16). | Access denied. | PIA-3.2, PIA-5 |
| SR-2 | 5.06.04 | 16 | 12 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered, and with required policy set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11)…<br><br>Verify product's ability to process a path that includes a *policyConstraints* extension with *inhibitPolicyMapping* set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings. | Access denied. | PIA-3.2, PIA-5 |
| SR-1 | 5.06.05 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered,, and with the trust anchor set to ICAM Test Card PIV Root CA…<br><br>Verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Authentication Certificates will be set to the CITE test OID for *id-fpki-common-authentication* (2.16.840.1.101.3.2.1.48.11) by the relying party solution. | Access granted. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.06.07 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered, and with the trust anchor set to ICAM Test Card PIV Root CA…<br><br>Verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for Card Authentication Certificates will be set to the CITE test OID for *id-fpki-common-cardAuth* (2.16.840.1.101.3.2.1.48.13) by the relying party solution. | Access granted. | PIA-3.2, PIA-5 |
| SR-1 | 5.06.08 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered, and with the trust anchor set to ICAM Test Card PIV Root CA…<br><br>Verify the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy for CHUID signature certificates will be set to the CITE test OID for *id-fpki-common-piv-contentSigning* (2.16.840.1.101.3.2.1.48.86) by the relying party solution. | Access granted. | PIA-3.2, PIA-5 |
| SR-1 | 5.06.09 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered, and with the trust anchor set to ICAM Test Card PIV Root CA…<br><br>Verify the validation software is able to recognize when an explicit certificate policy is required and not present in the Card Authentication certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the Card Authentication certificate path (e.g., OID value 2.3.4.5). | Access denied. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.06.10 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered, and with the trust anchor set to ICAM Test Card PIV Root CA…<br><br>Verify the validation software is able to recognize when an explicit certificate policy is required and not present in the CHUID signature certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the CHUID signature certificate path (e.g., OID value 3.4.5.6). | Access denied. | PIA-3.2, PIA-5 |
| | **5.07** | | | **Generalized Time** | | |
| SR-3 | 5.07.01 | 16 | 24 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to process valid use of generalized time post year 2049 in the path. | Access granted. | PIA-3.2, PIA-5 |
| SR-3 | 5.07.02 | 16 | 25 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify product's ability to process invalid use of generalized time before year 2049 in the path. | Access denied. | PIA-3.2, PIA-5 |
| | **5.08** | | | **Name Constraints** | | |
| SR-1 | 5.08.01 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree. | Access granted. | PIA-3.2, PIA-5 |
| SR-1 | 5.08.02 | 16 | 13 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree. | Access denied. | PIA-3.2, PIA-5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.08.03 | 16 | 14 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the intermediate certificate includes a Name Constraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and *subjectAltName* with a DN that falls outside that subtree. | Access denied. | PIA-3.2, PIA-5 |
| | **5.09** | | | **Certificate Revocation Tests (CRL)** | | |
| SR-1 | 5.09.01 | 16 | 15 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when no revocation information is available for the End Entity certificate. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.02 | 16 | 16 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when a second intermediate CA certificate is revoked. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.03 | 16 | 17 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the CRL has an invalid signature. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.04 | 16 | 18 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.05 | 16 | 19 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when a certificate in the path has an expired *nextUpdate* value (an expired CRL). | Access denied. | PIA-3.5, PIA-5, PIA-7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-3 | 5.09.06 | 16 | 20 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when a certificate in the path points to a CRL with a *notBefore* date in the future. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.07 | 16 | 21 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when a certificate in the path has an incorrect CRL distribution point. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.08 | 16 | 34 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when an incorrectly formatted CRL is present in the path. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.09 | 16 | 36 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when an invalid CRL signer is in the path. | Access denied. | PIA-3.5, PIA-5, PIA-7 |
| SR-1 | 5.09.10 | 58 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the Card Authentication Certificate is revoked. | Access denied. | [SP 800-73], PIA-3, PIA-3.2 |
| SR-1 | 5.09.11 | 58 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the end-entity Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available. | Access denied. | [SP 800-73], PIA-3, PIA-3.2 |
| | **5.10** | | | **Content Signer Verification** | | |
| | **5.12** | | | **Fingerprint Verification** | | |
| | **5.14** | | | **OCSP Response Checking** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SR-1 | 5.14.01 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system successfully validates a valid CAK credential using an OCSP response with a valid signature. | Access granted. | PIA-3.2, PIA-3.5 |
| SR-2 | 5.14.02 | 42 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify that validation fails using an OCSP Responder with an expired signature certificate for a good card. | Access denied. | PIA-3.2, PIA-3.5, PIA-3.6 |
| SR-3 | 5.14.03 | 43 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify that validation succeeds using an OCSP Responder with a revoked signature certificate for a good credential with PKIX_OCSP_NOCHECK present. | Access granted. | PIA-3.2, PIA-3.5 |
| SR-2 | 5.14.04 | 44 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify that validation fails using an OCSP Responder with a revoked signature certificate for a good credential without PKIX_OCSP_NOCHECK present. | Access denied. | PIA-3.2, PIA-3.5, PIA-3.6 |
| SR-1 | 5.14.05 | 45 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify that validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good credential. | Access denied. | PIA-3.2, PIA-4 |
| SR-1 | 5.14.06 | 45 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the Card Authentication Certificate is not expired but is revoked; AIA to OCSP is not available and crlDP to CRL is available. | Access denied. | PIA-3.2, PIA-4 |
| | **5.15** | | | **Interoperability Testing** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SO-1 | 5.15.01 | 46 | 00 | With ICAM Test PKI-CAK 46 registered with the PACS, verify the system recognizes a 14-decimal-digit FASC-N and treats the credential as the primary identifier throughout the system.<br><br>Note: Although this test case is optional, this test case or test case 5.15.02 is required. | Access granted. | PIA-6, [SP 800-116] Appendix E |
| SO-1 | 5.15.02 | 46 | 00 | With ICAM Test PKI-CAK 46 registered with the PACS, verify the system recognizes a full 16-byte Card UUID and uses this as the primary identifier.<br><br>Note: Although this test case is optional, this test case or test case 5.15.01 is required. | Access granted. | PIA-6, [SP 800-116] Appendix E |
| SR-3 | 5.15.03 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when the Extended Key Usage extension *keyPurposeId* OID (2.16.840.1.101.3.6.8) is present in the Card Authentication certificate. | Access granted. | [FIPS 201] |
| SR-3 | 5.15.04 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system recognizes when an explicit Extended Key Usage extension *keyPurposeId* OID (e.g., 1.2.3.4.5.6.7) is not present in the Card Authentication certificate. | Access denied. | [FIPS 201] |
| SR-1 | 5.15.05 | 47 | 00 | With ICAM Test Card 47 registered with the PACS…<br><br>Verify the FIPS 201-2 card results in an access granted decision using PKI-CAK method with the *pivFASC-N* positioned after the *entryUUID* in the *GeneralNames* sequence within the Subject Alternative Names extension of the PIV CAK certificate. | Access granted. | [FIPS 201] |
| SR-1 | 5.15.06 | 53 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Verify the system successfully handles cards with a slightly larger than recommended Card Authentication Certificate (2160 bytes). | Access granted. | [SP800-73] |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **5.17** | | | **Discovery Object and PIN Usage Policy** | | |
| | **5.18** | | | **ISO 7816-3 2006 PPS Protocol Compliance** | | |
| UR-3 | 5.18.01 | 37 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Using PKI-CAK, verify the system's contactless readers recognize and negotiate a bit rate based on a response from a card with a PPS indicating a bit rate of 848 KBps. | Access granted. | [ISO 14443-4] |
| | **5.19** | | | **SM and OCC-AUTH** | | |
| | **7.0** | | | **PACS Design Use Cases** | | |
| | **7.01** | | | **Continuity of Operations Testing** | | |
| | **7.02** | | | **Security Boundaries** | | |
| | **7.03** | | | **Registering Physical Access Privileges** | | |
| | **7.04** | | | **PKI Configuration** | | |
| | **7.05** | | | **Credential Number Specifications** | | |
| UO-3 | 7.05.01 | 16 | | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Configure system for 128- bit FASC-N. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes | Solution supports FICAM conformant 128-bit FASC-N credential numbers as specified in *Table 4*. | PAU-2, PAU-3; *Table 6-1* row 3 |
| | **7.06** | | | **Validation at Time of Access** | | |
| UO-1 | 7.06.01 | 16 | 00 | With Card 46 registered to the PACS and Card 16 registered as secondary credential to the same PACS identity that was created when Card 46 was registered…<br><br>Use Authentication Test logs to verify that all good cards were allowed access at the door reader. | Solution supports contactless Card Authentication Key (PKI-CAK). | PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7, §10.1.1 |
| | **7.07** | | | **Portal Hardware** | | |
| | **7.08** | | | **Auditing and Logging** | | |
| | **7.09** | | | **Security Certification and Accreditation** | | |
| | **7.10** | | | **Biometric in PACS** | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 7.11 | | | Operational Controls | | |
| | 7.12 | | | Accessibility | | |
| | 8.0 | | | Handheld Requirements | | |
| | 8.01 | | | Communications | | |
| | 8.02 | | | Operational Requirements | | |
| | 8.03 | | | Docking Station | | |
| | 8.04 | | | FINGERPRINT Verification | | |
| | 8.05 | | | Import Function | | |
| | 8.06 | | | Operational | | |
| | 8.07 | | | Online Validation Requirements | | |
| | 8.08 | | | Online PACS Integration Requirements | | |
| | 8.09 | | | Offline Validation Requirements | | |
| | 8.10 | | | Offline PACS Integration Requirements | | |