



Federal Identity, Credentialing, and Access Management

Personal Identity Verification Interoperable (PIV-I)

Test Plan

Version 1.2.0
Final

October 18, 2016

Table of Contents

| | | |
|------------|--|----|
| 1 | Introduction..... | 1 |
| 1.1 | Background..... | 1 |
| 1.2 | Purpose..... | 1 |
| 2 | Test Strategy..... | 2 |
| 2.1 | Test Environment..... | 2 |
| 2.2 | Test Process..... | 3 |
| 3 | PIV-I Card Validation Test Procedures..... | 4 |
| 4 | PIV-I Data Model Test Procedures..... | 6 |
| 5 | PIV-I Application Interoperability Test Procedures..... | 8 |
| 5.1 | Physical Application Testing with a PKI enabled PACS..... | 8 |
| 5.2 | PACS 1 Testing..... | 8 |
| 5.3 | PACS 2 Testing..... | 13 |
| Appendix A | PIV-I Requirements for Card Validation..... | 17 |
| Appendix B | PIV-I Requirements for Data Model Testing..... | 19 |
| Appendix C | PIV-I Requirements for Application Interoperability Testing..... | 36 |
| Appendix D | References..... | 37 |
| Appendix E | Acronyms..... | 41 |

Figures

| | |
|--|----|
| Figure 1: Location of Zone 11 on Example Portrait PIV-I Card | 5 |
| Figure 2: Example Landscape PIV-I Card | 5 |
| Figure 3: PACS 1 Logical Architecture | 9 |
| Figure 4: PACS 2 Logical Architecture | 13 |

Tables

| | |
|--|----|
| Table 1: PIV-I Card Validation Test Procedures | 4 |
| Table 2: Automated Data Model Test Procedures | 6 |
| Table 3: Manual Data Model Test Procedures | 6 |
| Table 4: PACS 1 Equipment Overview | 10 |
| Table 5: PACS 1 Testing | 11 |
| Table 6: PACS 2 Equipment Overview | 14 |
| Table 7: PACS 2 Testing | 15 |
| Table 8: PIV-I Requirements for Card Validation | 17 |
| Table 9: PIV-I Requirements for Data Model Tests | 19 |
| Table 10: Optional Facial Image PIV Tests Mandatory for PIV-I | 31 |
| Table 11: Optional Card Authentication PIV Tests Mandatory for PIV-I | 32 |
| Table 12: PIV-I Requirements for Data Model Tests, PIV Tests Skipped for PIV-I | 33 |
| Table 13: PIV-I Requirements for Application Interoperability Testing | 36 |

Document History

| Status | Release | Date | Comment | Audience |
|--------|---------|-----------|---|------------------------------|
| Draft | 0.1.0 | 10/7/10 | Initial Delivery | External Review |
| Draft | 0.2.0 | 11/30/10 | Final Polish | Judy Spencer |
| Final | 1.0.0 | 12/9/10 | Final edits and formatting | Judy Spencer, Deb Gallagher |
| Final | 1.1.0 | 2/17/2011 | Updates based on feedback from Carl Wallace (DoD), Dan Jeffers (DoD) and Anil John (DHS), Updates to tests PIV-I-B.07, PIV-I-B.08, PIV-I-B.12, PIV-I-B.13, PIV-I-B.17, PIV-I-B.18, PIV-I-B.22, PIV-I-B.23, PIV-I-B.27, PIV-I-B.28, PIV-I-B.45, PIV-I-B.46; which may not apply based on results from PIV-I-B.36, PIV-I-B.38; to make allowances for non-PIV-I digital signature and key management certificates. | ICAM SC Chair; PIV-I vendors |
| Final | 1.2.0 | 10/18/16 | Revised Section 2.2 to align with streamlined application process. Corrected typos and formatting throughout. Updated references links where possible. | ICAM SC Chair; PIV-I vendors |

Editors

| | | |
|----------------|-------------|-----------|
| Sandra Metzger | Dave Silver | CertiPath |
| Wendy Brown | Nhan Huynh | |

1 Introduction

1.1 Background

Personal Identity Verification (PIV) Interoperability for Non-Federal Issuers [PIV-I NFI], updated in July 2010, provides information for non-federal organizations interested in issuing identity credentials that are technically interoperable with the Federal PIV Card and issued in a manner that facilitates trust. Subsequently, the Federal Identity, Credential, and Access Management (ICAM) community determined that the establishment of specific Public Key Infrastructure (PKI) certificate policy requirements for Personal Identity Verification Interoperable (PIV-I) would further facilitate this trust. These PIV-I policy requirements were added to the *X.509 Certificate Policy for the Federal Bridge Certification Authority* [FBCA CP] in May 2010. As a result, commercial PKI providers may cross certify with the Federal Bridge Certification Authority (FBCA) in order to provide PIV-I credentials to their users. Cross certification requires PIV-I Card interoperability testing in order to demonstrate that the PIV-I Card conforms to the policy requirements and can technically interoperate with elements of the Federal smart card infrastructure.

1.2 Purpose

The purpose of this test plan is to certify prospective PIV-I Cards of entities wishing to cross certify with the Federal PKI (FPKI). The requirements in this document are derived from all applicable authoritative government publications (see Appendix D). This set of requirements is subject to change as the authoritative documents change. At a minimum, a prospective PIV-I Card must conform to all the requirements stated in this test plan. The Physical Access Control System (PACS) systems used in PIV-I card testing must be approved by the Federal Public Key Infrastructure Policy Authority (FPKIPA). There are two acceptable approaches to prospective PIV-I Card testing:

1. An entity can use the ICAM Lab to perform testing based on this test plan; or
2. An entity performs its own testing using its own test plan in its own test environment, which has to be evaluated for comparability to this document, and both the plan and test environment must be approved by the FPKIPA.

2 Test Strategy

An entity needs to provide the ICAM Lab with one prospective PIV-I Card. ICAM Lab personnel then test the card to determine whether it conforms to all PIV-I requirements. There are three categories of PIV-I Card testing:

1. **PIV-I Card Validation** –The PIV-I Card must be manually scanned to ensure that it has the appropriate markings such as the cardholder’s facial image and name printed on the card itself, uses approved card stock and smartcard applets. The card validation test procedures are described in section 3, PIV-I Card Validation Test Procedures.
2. **PIV-I Data Model Validation** – The PIV-I Card data model (i.e., the structure and contents of the smart card) is defined in [FBCA CP] Appendix A. The data model test procedures are described in section 4, PIV-I Data Model Test Procedures.
3. **PIV-I Application Interoperability Validation** – One of the major benefits of the PIV-I program is the ability to use third-party, trusted, smart card credentials with Federal Government infrastructure (e.g., PACS, LACS, smart card readers, PK-enabled applications). Therefore, it is important that the PIV-I Card interfaces correctly with applications known to be capable of processing PIV-I. For this purpose, the Federal ICAM community has teamed with CertiPath (one of the other PKI Bridges operating at PIV-I) to test PIV-I Cards against PACS implementations. The PIV-I application interoperability test procedures are described in Section 5, PIV-I Application Interoperability Test Procedures.

2.1 Test Environment

PIV-I testing will be conducted in the ICAM Lab test environment¹ and at a CertiPath lab facility in Herndon, Virginia. CertiPath is supplying PKI-capable PACS for use in the testing.¹ The CertiPath PACS environment was originally part of a GSA commissioned effort to demonstrate a multi-factor PKI capable PACS, and has been approved by the FPKIPA for use in PIV-I testing.

All tests will be conducted by ICAM Lab personnel. For automated and manual testing, to inspect the PIV-I Card, testers will use a standard Smart Card Reader with a PC/SC interface and Smart Card middleware as specified in [NIST SP 800-73-3]. Some tests require the use of ActivIdentity ActivClient v6.1 or v6.2. Preliminary PACS testing at the CertiPath lab can be scheduled on an as-needed basis. The PIV-I Data Model testing will include the execution of the [PIV-I Data Model Tester]. This tool is based on GSA’s NIST SP 800-85B Data Conformance Test Tool [PIV Data Model Test Tool], with specific modifications to determine conformance with the PIV-I standard. The tool will perform tests which require access to any URLs included in the PIV-I Card.

¹ For purposes of this test plan, use of a test PKI environment is preferable to a production PKI environment.

2.2 Test Process

The PIV-I Card test process is as follows:

1. Entity notifies the FPKIPA that they wish to issue PIV-I cards.
2. The FPKIPA co-chairs inform the ICAM Lab of a PIV-I cross certification, and that PIV-I Card testing is needed.
3. The ICAM Lab schedules and performs a kickoff meeting with entity. The meeting addresses issues such as logistics, communication, timelines, and resources.
4. The entity develops a test PKI environment to support PIV-I testing. All Online Certificate Status Protocol (OCSP), Authority Information Access (AIA) and Certificate Revocation List Distribution Point (CRLDP) URLs to be verified in PIV-I testing must be accessible from the ICAM Lab.
5. The ICAM Lab performs cross certification with the entity's test PKI environment as necessary.
6. The entity generates a test PIV-I Card. If the entity intends to include any optional elements such as digital signature and key management certificates, these must be included in the test PIV-I Card.
7. If the entity intends to include any optional elements such as symmetric keys, key history or retired key management objects, the entity negotiates with the ICAM Lab to develop appropriate tests.
8. The ICAM Lab receives the PIV-I Card and performs the test procedures listed in section 3, PIV-I Card Validation Test Procedures, and section 4, PIV-I Data Model Test Procedures.
9. The ICAM Lab arranges to have further PIV-I testing performed at the CertiPath lab.
 - ICAM Lab personnel observe the test procedures in section 5, PIV-I Application Interoperability Test Procedures being performed.
 - Fingerprint matching tests are performed.
 - The user whose fingerprints are stored on the PIV-I Card must be present for this stage of testing.
10. The ICAM Lab collaborates with the entity to resolve issues identified during testing.
11. The ICAM Lab documents and reports test findings to the FPKIPA.
12. The ICAM Lab continues to address remaining issues as necessary.

3 PIV-I Card Validation Test Procedures

This section describes the tests that support the requirements listed in *Appendix A, PIV-I Requirements for Card Validation*.

Requirements pertaining to the visual appearance of a PIV-I Card were written to prevent a PIV-I Card from being mistaken for a Government-issued PIV Card. While the constraints on the appearance of a PIV-I Card are less stringent than those of a PIV Card, the data model elements must be examined more carefully to ensure compliance with standards. Testers will validate each test presented in Table 1.

Table 1: PIV-I Card Validation Test Procedures

| Test ID | Test Procedure |
|-----------|---|
| PIV-I-A.1 | <p>Verify that the PIV-I Card is visually distinct from a PIV Card, that at a minimum it does not have images or logos placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201] and as shown in</p> <p>. A landscape orientation, as illustrated in Figure 2, also qualifies.</p> |
| PIV-I-A.2 | <p>Verify that the PIV-I Card contains: a. Cardholder facial image; b. Cardholder full name; c. Organizational Affiliation, if exists; otherwise the issuer of the card; and d. Card expiration date.</p> |
| PIV-I-A.3 | <p>Verify that the PIV-I Card printed expiration date does not exceed 5 years beyond the testing date.</p> |
| PIV-I-A.4 | <p>Retrieve the card model listed on the back of the test card. If the model is not listed, the tester will insert the card into a card reader and open the ActivClient tool or other SmartCard viewers and retrieve the model from the —Smart Card pane of ActivClient. The tester will then verify that the data model is listed in the Approved Products List (APL) in [FIPS 201 APL].</p> |
| PIV-I-A.5 | <p>Insert the card into a card reader and open the ActivClient Advanced Diagnostics tool or other appropriate SmartCard viewers' tool. Execute the SmartCard diagnostics. In the results, the tester will find the —ATR listing below —Card inserted = YES!. Within parenthesis is the smartcard applet type. Verify that this applet type is listed in [NIST Approved Applets]</p> |
| PIV-I-A.6 | <p>If the card issuer intends to use any optional card material, for example asymmetric key, key history objects and retired key management keys as described in FIPS 201 Section 4.1.5.1 and [NIST SP800-73-3] Part 1, the issuer must present samples of each optional element for testing, work with the ICAM lab to design a test strategy and assist in performing associated tests.</p> |
| PIV-I-A.7 | <p>Verify that the Cardholder Facial Image is printed on the front of the card, and at a minimum that:</p> <ul style="list-style-type: none"> • Only the subject cardholder appears in the image; • A frontal pose; • Taken on a neutral background; <p>Verify all other requirements as applicable to [NIST SP 800-76-1] Section 5.</p> |

| Test ID | Test Procedure |
|-----------|---|
| PIV-I-A.8 | Manual inspection and review of all card materials using a Microsoft Certificate Store Viewer, ActivClient, or other automated tool to ensure conformance with all PIV-I requirements and that all visually printed information are accurate. |

Figure 1: Location of Zone 11 on Example Portrait PIV-I Card

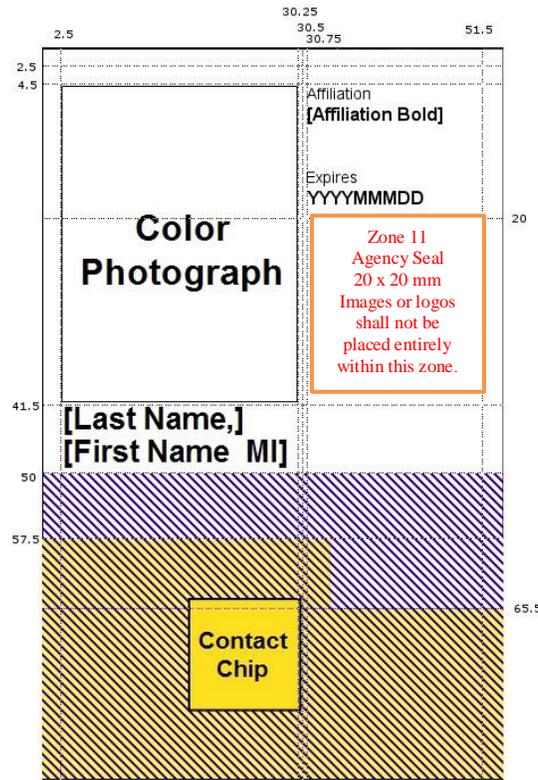
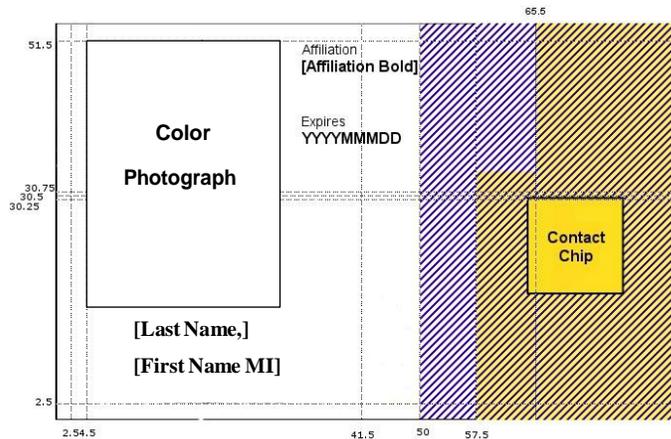


Figure 2: Example Landscape PIV-I Card



4 PIV-I Data Model Test Procedures

This section describes the tests that support the requirements listed in *Appendix B, PIV-I Requirements for Data Model Testing*.

Data model testing requires an updated version of the PIV Data Model Test Tool v.6.1.0. Some tests will indicate that further manual review is required. ICAM Lab personnel will perform test procedures listed in Table 2. When tests are complete, ICAM Lab personnel will manually review the items listed in Table 3 and scan the final report in the Modified PIV Data Model Test Tool for errors.

Table 2: Automated Data Model Test Procedures

| Test ID | Automated Test Procedure |
|--------------------------|---|
| PIV-I-B.01 to PIV-I-B.55 | Insert the PIV-I Card into a PC/SC smartcard reader with a PC/SC interface and execute all tests available as shown in the [PIV-I Data Model Tester]. If issuer intends to include any optional elements such as Digital Signature, Key Management, Key History Objects and/or Retired Key Management objects, then the tester shall select these optional elements in the tool by selecting Edit->Enable/Disable Optional Tests and highlight all included optional elements. Perform all manual reviews as indicated in the final report provided by the tool, found in apdu_tests_data_model/reports/Report.html. Adjust the final report by following the manual test procedures listed in Table 3. |

Table 3: Manual Data Model Test Procedures

| Test ID | Manual Test Procedure |
|------------|---|
| PIV-I-B.36 | If PIV-I.B.38 Fails, the Digital Signature Certificate does not have a policy OID cross certified with the PIV-I Hardware policy OID, as described in [FBCA CP] Appendix A Item 4, and is therefore not required to conform to [PIV-I Profile]. In this case, the following test cases no longer apply: PIV-I-B.07 PIV-I-B.12 PIV-I-B.17 PIV-I-B.22 PIV-I-B.27 PIV-I-B.45 |
| PIV-I.B.38 | If PIV-I.B.38 Fails, the Key Management Certificate does not have a policy OID cross certified with the PIV-I Hardware policy OID, as described in [FBCA CP] Appendix A Item 4, and is therefore not required to conform to [PIV-I Profile]. In this case, the following test cases no longer apply: PIV-I-B.08 PIV-I-B.13 PIV-I-B.18 PIV-I-B.23 PIV-I-B.28 PIV-I-B.46 |
| PIV-I-B.44 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #79, to retrieve the PIV-I X.509 Certificate PIV Authentication OU extracted from the certificate DN. Validate that at least one OU matches either the affiliated organization name or the Entity CA’s Name. |
| PIV-I-B.45 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #80, to retrieve the PIV-I X.509 Certificate Digital Signature OU extracted from the certificate DN. Validate that at least one OU matches either the affiliated organization name or the Entity CA’s Name. Test requirement does not apply if PIV-I-B.36 fails. |
| PIV-I-B.46 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #81, to retrieve the PIV-I X.509 Certificate Key Management OU extracted from the certificate DN. Validate that at least one OU matches either the affiliated organization name or the Entity CA’s Name. Test requirement does not apply if PIV-I.B.38 fails. |

| Test ID | Manual Test Procedure |
|----------------|---|
| PIV-I-B.47 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #82, to retrieve the PIV-I X.509 Certificate Content Management OU extracted from the certificate DN. Validate that at least one OU matches either the affiliated organization name or the Entity CA's Name. |
| PIV-I-B.48 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #83, to retrieve the PIV-I Card Authentication OU extracted from the certificate DN. Validate that this OU matches either the affiliated organization name or the Entity CA's Name |
| PIV-I-B.49 | Review the test results from the Modified PIV Data Model Test Tool, certificate profile conformance test #84, to retrieve the CHUID expiration date. Verify that this certificate does not expire before the PIV-I expiration date on the card. |

5 PIV-I Application Interoperability Test Procedures

This section describes the tests that support the requirements listed in *Appendix C, PIV-I Requirements for Application Interoperability Testing*.

The ICAM Lab will schedule a testing date at the CertiPath testing facility and then notify the entity of the date. On the scheduled date, testing is performed. ICAM Lab personnel will observe and monitor all stages of testing to ensure compliance with the processes specified in this document. PACS testing will include fingerprint identification, so the subject cardholder whose fingerprints are on the card must be present for this testing.

The equipment and test environments used by CertiPath for PIV-I Testing may be subject to change over time as new capabilities and requirements for physical access with PIV-I credentials are created.

5.1 Physical Application Testing with a PKI enabled PACS

Physical Access application testing performed at the CertiPath facility uses PKI-enabled PACS that were tested by CertiPath's Trusted PACS certification program. This ensures each PACS can operate in several modes of authentication and can differentiate between valid and invalid access attempts. For more information about CertiPath's APL visit <http://CertiPath.com/apl>. CertiPath conducts Physical Access application testing with two PACS implementations, and thus are divided into two sections:

1. PACS 1; and
2. PACS 2 Testing.

5.2 PACS 1 Testing

The CertiPath Lab Technician must complete each test listed in Table 5. The Lab Technician will ensure that the test card can authenticate to the PACS.

Figure 3 shows the logical architecture of the PKI-enabled PACS used for this portion of application testing. Supporting information about the components used in the system is specified in Table 4

Figure 3: PACS 1 Logical Architecture

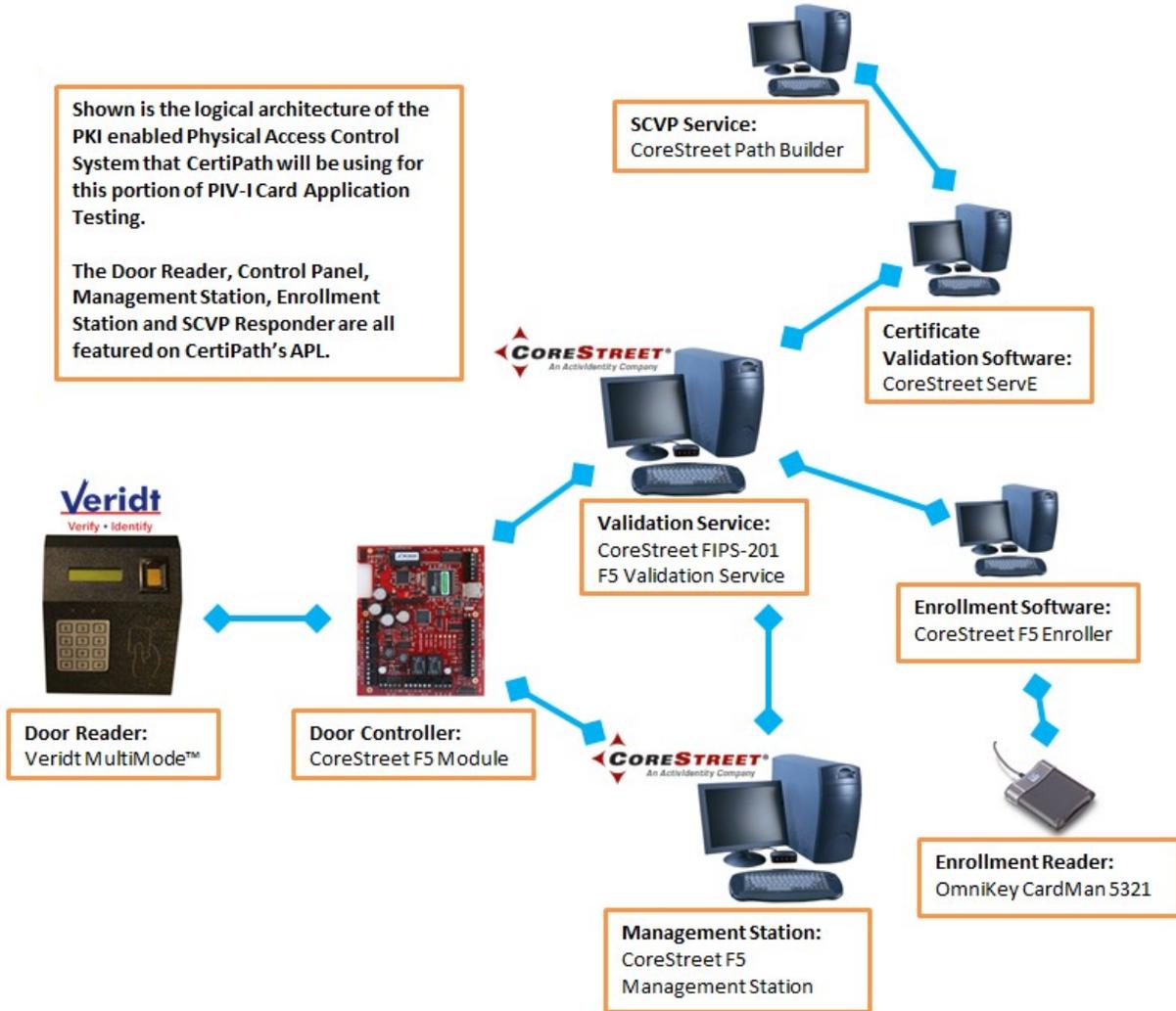


Table 4: PACS 1 Equipment Overview

| Manufacturer | Product Name | Product Role |
|-------------------------------|-----------------------|--|
| Veridt, Inc. | MultiMode™ | <p>The Veridt MultiMode™ is a Three Factor Door Reader (PKI+PIN+BIO) used for CertiPath's Test PACS.</p> <p>The Door Reader's purpose is to support several modes of authentication to demonstrate a PIV-I test card's ability to operate correctly with a PK-enabled PACS.</p> |
| CoreStreet | F5 Module | <p>The CoreStreet F5 Module acts as the Door Controller for CertiPath's Test PACS.</p> <p>The Door Controller's purpose is to talk directly with the Door Reader. When a Cardholder requests access at the Reader the Door Controller connects to the Validation Service to check if the Cardholder is enrolled in the system as well as the validity of the credential used to request access.</p> <p>If the Validation Service responds with either an access granted or access denied response back to the F5 Module relays located on the board trigger accordingly.</p> |
| CoreStreet | F5 Management Station | <p>The F5 Management Station acts as the System Controller for CertiPath's Test PACS.</p> <p>The System Controller is responsible for pushing Access Control List settings generated by the Enrollment Station and validation data from the Validation Service to the Door Controller to ensure that the Door Controller's cached data is kept up to date in case of any temporary service outages.</p> <p>The System Controller also determines the configuration of the Door Reader's authentication modes, relay settings and output settings.</p> |
| CoreStreet | F5 Enroller | <p>The F5 Enroller acts as the Enrollment Software and Head End System for CertiPath's Test PACS.</p> <p>In order to register a Cardholder with the system, the Enrollment Software checks the certificate validity of the Cardholder with the Certificate Validation Software. If responses from the Validation Software are positive the Cardholder is enrolled.</p> |
| CoreStreet | Path Builder | <p>CoreStreet Path Builder acts as the SCVP Server for CertiPath's Test PACS.</p> <p>Path Builder is responsible for performing path discovery and path validation. Therefore, CertiPath's Test PACS does not need to rely on local trust stores for information about certificate paths.</p> |
| HID Global Corporation | CardMan 5321 | <p>The CardMan 5321 card reader is a dual interface contact/contactless smartcard reader.</p> <p>The CardMan 5321's primary purpose is to act as the reader for the CoreStreet F5 Enroller.</p> |

| Manufacturer | Product Name | Product Role |
|--------------|-----------------------------|--|
| CoreStreet | FIPS-201 Validation Service | <p>The CoreStreet FIPS-201 Validation Service performs Validation Service for the F5 Module.</p> <p>The primary purpose of the Validation Service is to keep the cached validation data up to date to provide quick responses to the F5 Module when queried. In the event that a response is not available in the cached validation data the Validation Service relies on the CoreStreet SerVE for real-time SCVP, OCSP or CRL-based validation responses.</p> |
| CoreStreet | Path Builder SerVE | <p>CoreStreet’s SerVE Software performs Certificate Validation for CertiPath’s Test PACS.</p> <p>SerVE’s primary purpose is to pass responses about the validity of certificates back to the FIPS-201 Validation Service.</p> <p>SerVE relies on the SCVP Service for Path Discovery and Path Validation but can also leverage OCSP or CRLs.</p> |

Table 5: PACS 1 Testing

| ID | Item | Requirement | Testing Requirements |
|-------|------------|---|---|
| PS1T1 | Enrollment | The Cardholder can be successfully enrolled to the PACS using the AIA URLs, ie without using local trust stores | <p>First, the Lab Technician will configure the Certificate Trust Anchors and settings for Path Builder SerVE and Path Builder.</p> <p>Once the setup is complete, the Lab Technician will attempt to enroll the Cardholder into the PACS.</p> <p>If enrollment fails, no subsequent tests will be run.</p> |
| PS1T2 | CHUID Mode | The Cardholder can authenticate to a PACS using the cards CHUID | <p>First, the Lab Technician will configure PACS 1 for CHUID authentication mode at the Door Reader.</p> <p>Second, using the contactless interface the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>Last, using the contact interface the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>The test fails if access is denied in either contact or contactless mode.</p> |

| ID | Item | Requirement | Testing Requirements |
|--------------|-------------------------------|--|---|
| PS1T3 | CAK Mode (Asymmetric only) | The Cardholder can authenticate to a PACS using the Card Authentication Certificate/Key | <p>First, the Lab Technician will configure PACS 1 for Card Authentication Key (CAK) authentication mode at the Door Reader.</p> <p>Second, using the contactless interface the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>Last, using the contact interface the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>The test fails if access is denied in either contact or contactless mode.</p> |
| PS1T4 | PKI + PIN Mode | The Cardholder can authenticate to a PACS using the Authentication Certificate/Key | <p>First, the Lab Technician will configure PACS 1 for PKI + PIN authentication mode at the Door Reader.</p> <p>Second, using the contact interface the cardholder presents the card to the Door Reader.</p> <p>Last, when prompted, the cardholder enters their PIN and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |
| PS1T5 | PKI + PIN + Fingerprint Mode | <p>The Authentication Certificate/Key is still able to authenticate when multi-factor authentication is required</p> <p>The PACS can interact with the test card to validate that the fingerprint on the card matches the person presenting the card</p> | <p>First, the Lab Technician will configure PACS System 1 for PKI + PIN + Fingerprint authentication mode at the Door Reader.</p> <p>Second, using the contact interface the cardholder presents the card to the Door Reader.</p> <p>Third, when prompted, the cardholder enters their PIN.</p> <p>Last, when prompted, the cardholder places their finger on the biometric sensor and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |
| PS1T6 | PKI + PIN Mode, Access Denied | The Cardholder cannot authenticate to a PACS using the Authentication Certificate/Key with an incorrect PIN | <p>First, the Lab Technician will configure PACS 1 for PKI + PIN authentication mode at the Door Reader.</p> <p>Second, using the contact interface, the cardholder presents the card to the Door Reader.</p> <p>Last, when prompted, the cardholder enters an incorrect PIN and waits for an access granted response.</p> <p>The test fails if access is granted.</p> |

| ID | Item | Requirement | Testing Requirements |
|-------|---|---|---|
| PS1T7 | PKI + PIN + Fingerprint Mode, Access Denied | <p>The Authentication Certificate/Key cannot be used to authenticate with the incorrect fingerprint</p> <p>The PACS can interact with the test card to validate that the fingerprint on the card matches the person presenting the card</p> | <p>First, the Lab Technician will configure PACS System 1 for PKI + PIN + Fingerprint authentication mode at the Door Reader.</p> <p>Second, using the contact interface, the cardholder presents the card to the Door Reader.</p> <p>Third, when prompted, the cardholder enters their PIN.</p> <p>Last, when prompted, a user other than the cardholder places their finger on the biometric sensor and waits for an access granted or denied response.</p> <p>The test fails if access is granted.</p> |

5.3 PACS 2 Testing

A Lab Technician must complete each test listed in Table 7. The Lab Technician will ensure that the test card can authenticate to the PACS. Figure 4 shows the logical architecture of the PKI-enabled PACS used for this portion of application testing. Supporting information about the components used in this system is located in Table 7.

Figure 4: PACS 2 Logical Architecture

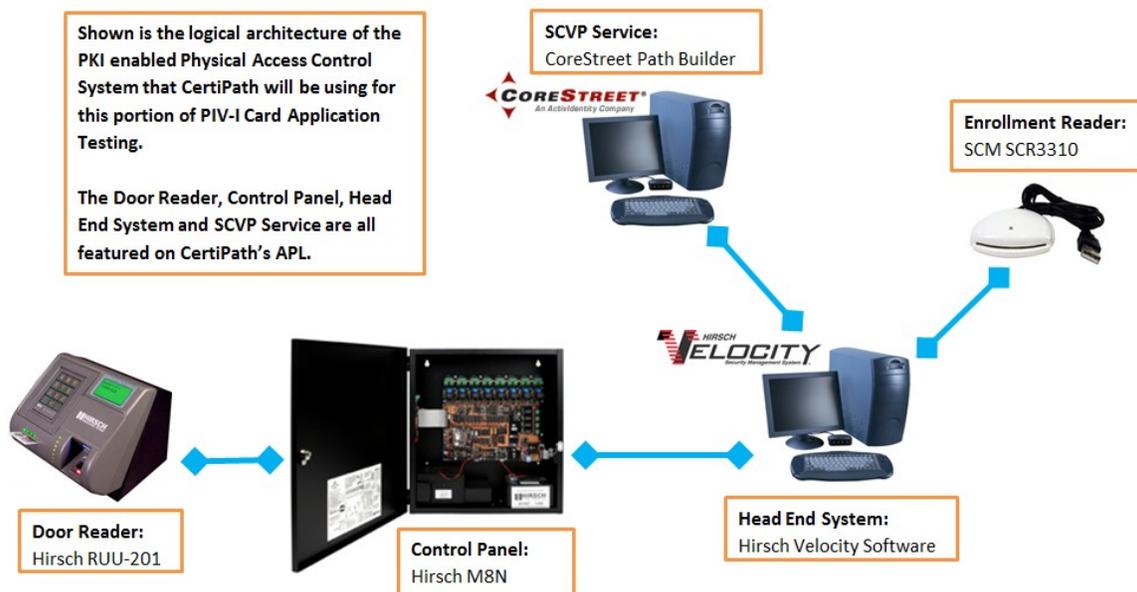


Table 6: PACS 2 Equipment Overview

| Manufacturer | Product Name | Product Role |
|------------------------|--------------------------|---|
| Hirsch Electronics | Digi*Trac M8 Controller | The Hirsch M8N Control Panel is an all in one access controller. It accepts input from the door reader and various sensors, alerts the head end to any changes in status, and provides a relayed response to the door controls. It can accept |
| Hirsch Electronics | RUU Verification Station | The Hirsch RUU-201 Verification Station Card Reader provides the end entity an interface with the Hirsch system. The key feature of this reader is the scramblepad, which randomizes the location of digits used for entering the PIN. The Door Reader's purpose is to support the challenge/response and |
| Hirsch Electronics | Velocity Software | The Velocity Server acts as both a Head End System for the M8N Control Panel as well as an Enrollment Station. The Head End System interfaces with both the Control Panel and the SCVP Responder. The Velocity Server maintains the Access Control List and device configuration for the Hirsch system. |
| SCM Microsystems, Inc. | SCR3310 | Enrollment Station Reader. |
| CoreStreet | Path Builder | CoreStreet Path Builder acts as the SCVP Server for CertiPath's Test PACS. Path Builder is responsible for performing path discovery and path validation. Therefore, CertiPath's Test PACS does not need to rely on local trust stores for information about certificate paths. |

Table 7: PACS 2 Testing

| ID | Item | Requirement | Testing Requirements |
|-------|----------------|---|---|
| PS2T1 | Enrollment | The Cardholder can be successfully enrolled to the PACS using the AIA URLs, i.e, without using local trust stores | <p>First, the Lab Technician will configure the Certificate Trust Anchors and settings for Path Builder.</p> <p>Once the setup is complete, the Lab Technician will attempt to enroll the Cardholder into the PACS.</p> <p>If enrollment fails, no subsequent tests will be run.</p> |
| PS2T2 | CHUID Mode | The Cardholder can authenticate to a PACS using the cards CHUID | <p>First, the Lab Technician will configure PACS 2 for CHUID authentication mode at the Door Reader.</p> <p>Second, using the contactless interface, the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>Last, using the contact interface, the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |
| PS2T3 | CAK Mode | The Cardholder can authenticate to a PACS using the Card Authentication Certificate/Key | <p>First, the Lab Technician will configure PACS 2 for Card Authentication Key (CAK) authentication mode at the Door Reader.</p> <p>Second, using the contactless interface, the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>Last, using the contact interface, the cardholder presents the card to the Door Reader and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |
| PS2T4 | PKI + PIN Mode | The Cardholder can authenticate to a PACS using the Authentication Certificate/Key | <p>First, the Lab Technician will configure PACS 2 for PKI + PIN authentication mode at the Door Reader.</p> <p>Second, using the contact interface, the cardholder presents the card to the Door Reader.</p> <p>Last, when prompted, the cardholder enters their PIN and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |

| ID | Item | Requirement | Testing Requirements |
|-------|---------------------------------------|--|---|
| PS2T5 | PKI + PIN + Fingerprint Mode | <p>The Authentication Certificate/Key is still able to authenticate when multi-factor authentication is required</p> <p>The PACS can interact with the test card to validate that the fingerprint on the card matches the person presenting the card</p> | <p>First, the Lab Technician will configure PACS 2 for PKI + PIN + Fingerprint authentication mode at the Door Reader.</p> <p>Second, using the contact interface, the cardholder presents the card to the Door Reader.</p> <p>Third, when prompted, the cardholder enters their PIN.</p> <p>Last, when prompted, the cardholder places their finger on the biometric sensor and waits for an access granted response.</p> <p>The test fails if access is denied.</p> |

Appendix A PIV-I Requirements for Card Validation

Table 8 lists the card validation requirements.

Table 8: PIV-I Requirements for Card Validation

| Source | Test ID | Test Requirement |
|--|-----------|--|
| [FBCA CP] Appendix A Item 8 | PIV-I-A.1 | Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201]. |
| [FBCA CP] Appendix A Item 9 | PIV-I-A.2 | The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card: a. Cardholder facial image; b. Cardholder full name; c. Organizational Affiliation, if exists; otherwise the issuer of the card; and d. Card expiration date. |
| [FBCA CP] Appendix A Item 10 | PIV-I-A.3 | PIV-I Cards shall have an expiration date not to exceed 5 years of issuance. |
| [FBCA CP] Appendix A Item 1 | PIV-I-A.4 | To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA’s FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID) |
| [FBCA CP] Appendix A Item 1 | PIV-I-A.5 | To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA’s FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID) |
| [FIPS 201] Section 4.1.5.1, [NIST SP 800-76-1] and [NIST SP 800-73-3] Part 1-3 | PIV-I-A.6 | The PIV data model may be optionally extended to meet department or agency-specific requirements. If the data model is extended, this standard establishes requirements for the following four classes of logical credentials: ... symmetric card authentication keys for supporting additional physical access application ... Symmetric key(s) associated with the card management system. |
| [FIPS 201] Section 4.1.4.1 and [NIST SP800-76] Section 5 | PIV-I-A.7 | Mandatory Items on the Front of the PIV Card Zone 1—Photograph. The photograph shall be placed in the upper left corner and be a full frontal pose from top of the head to shoulder, as depicted in Figure 4-1. A minimum of 300 dots per inch (dpi) resolution shall be used. The background should follow recommendations set forth in SP 800-76. |

| Source | Test ID | Test Requirement |
|--|-----------|---|
| [FIPS 201], [FBCA CP], [PIV-I Profile] | PIV-I-A.8 | Verify that the card conforms to all PIV-I requirements |

Appendix B PIV-I Requirements for Data Model Testing

The majority of the PIV-I data model tests are the same as the PIV data model tests presented in [EP]. Refer to *Appendix D, References for baseline document versions*. Therefore, only the differences will be presented in this appendix. For readability, four tables are presented.

- Table 9 – lists the new requirements for PIV-I that are not present in [EP]. The first value listed in the Test ID column is the PIV-I Test Plan Test ID. The second value, following in parenthesis, is the [PIV-I Data Model Tester] CHECK_certificate_profile conformance (PT CP) test id, or by the CHECK_digital_signature (PT DS) test id.
- Table 10 – lists the optional [EP] PIV Facial Image Data Model tests that are mandatory for PIV-I. Please refer to [EP] for the test requirement text. The requirement is derived from [FBCA CP] Appendix A Item 6: —PIV-I Cards shall contain an electronic representation (as specified in [NIST SP 800-73] and [NIST SP 800-76]) of the Cardholder Facial Image printed on the card.
- Table 11 – lists the optional [EP] PIV Card Authentication Data Model tests that are mandatory for PIV-I. Please refer to [EP] for the test requirement text. The requirement is derived from [FBCA CP] Appendix A Item 3: —The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
- Table 12 – lists the [EP] PIV tests that will be skipped since they do not apply to PIV-I.

Table 9: PIV-I Requirements for Data Model Tests

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|--|------------------------------------|-----------------------|--|
| [FBCA CP] Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | NIST SP 800-73-3 PART1 Section 3.3 | PIV-I-B.01 (PT CP 36) | PIV-I CHUID: If the card is a PIV-I Card, the FASC-N in the CHUID shall have Agency Code equal to 9999, System Code equal to 9999, the Credential Number equal to 999999, indicating that a UUID is the primary credential identifier. |
| [FBCA CP] Appendix A Item 5 | PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that: a. conforms to [PIV-I - Profile]; b. conforms to [NIST SP 800-73]; and c. is issued under the PIV-I Card Authentication policy. | [PIV-I Profile] Worksheet 4 | PIV-I-B.02 (PT CP 37) | PIV-I X.509 Certificate Card Authentication: SubjectAltName must only include UUID name form. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|---|---|-----------------------|---|
| [FBCA CP] Appendix A Item 5 | PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that: a. conforms to [PIV-I - Profile]; b. conforms to [NIST SP 800-73]; and c. is issued under the PIV-I Card Authentication policy. | [PIV-I Profile] Worksheet 4 -AND- SP 800-73-3 PART1 Section 3.3 | PIV-I-B.03 (PT CP 38) | PIV-I X.509 Certificate Card Authentication: SubjectAltName: This field contains the UUID from the CHUID of the PIV-I Card encoded as a URI as specified in Section 3 of RFC 4122. -AND- The value of the GUID data element of the CHUID data object shall be a 16-byte binary representation of a valid UUID. |
| [FBCA CP] Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | [PIV-I Profile] Worksheet 5 -AND- SP 800-73-3 PART1 Section 3.3 | PIV-I-B.04 (PT CP 39) | PIV-I X.509 Certificate PIV Authentication: SubjectAltName, This field contains the UUID from the CHUID of the PIV-I Card encoded as a URI as specified in Section 3 of RFC 4122. -AND- The value of the GUID data element of the CHUID data object shall be a 16-byte binary representation of a valid UUID. |
| [FBCA CP] Appendix A Item 5 | PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that: a. conforms to [PIV-I - Profile]; b. conforms to [NIST SP 800-73]; and c. is issued under the PIV-I Card Authentication policy. | [PIV-I Profile] Section 4 | PIV-I-B.05 (PT CP 40) | PIV-I X.509 Certificate Card Authentication: including Self-Issued CA and Cross-certificate: To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Section 4 | PIV-I-B.06 (PT CP 41) | PIV-I X.509 Certificate PIV Authentication: including Self-Issued CA and Cross-Certificate: To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Section 4 | PIV-I-B.07 (CP 42) | PIV-I X.509 Certificate Digital Signature, if present: including Self-Issued CA and Cross-Certificate: To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates. Test requirement does not apply if PIV-I-B.36 fails. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|--|---|-----------------------|--|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Section 4 | PIV-I-B.08 (PT CP 43) | PIV-I X.509 Certificate Key Management, if present: including Self-Issued CA and Cross-certificate: To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates. Test requirement does not apply if PIV-I-B.38 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Section 4 | PIV-I-B.09 (PT CP 44) | PIV-I X.509 Content Signing Certificate: including Self-Issued CA and Cross-certificate: To help ensure that name constraints are applied correctly, CAs should encode each attribute value in a name constraint using the same encoding as is used to encode the corresponding attribute value in subject names in subsequent certificates |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].; Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 4 -AND- [PIV-I Profile] Worksheet 3 | PIV-I-B.10 (PT CP 45) | PIV-I X.509 Self-Issued CA -AND- Card Authentication Certificate: CRLDistributionPoints: This extension is required in all CA and EE certificates and must contain at least one HTTP URI. CRL Profile: The reasons and cRLIssuer fields must be omitted. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].; Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 5 -AND- Wk 3 | PIV-I-B.11 (PT CP 46) | PIV-I X.509 Self-Issued CA -AND- PIV Authentication Certificate: CRLDistributionPoints: This extension is required in all CA and EE certificates and must contain at least one HTTP URI. CRL Profile: The reasons and cRLIssuer fields must be omitted. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|--|---|-----------------------|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].; Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 6 -AND- [PIV-I Profile] Worksheet 3 | PIV-I-B.12 (PT CP 47) | PIV-I X.509 Self-Issued CA -AND- Digital Signature Certificate: CRLDistributionPoints: This extension is required in all CA and EE certificates and must contain at least one HTTP URI. CRL Profile: The reasons and cRLIssuer fields must be omitted. Test requirement does not apply if PIV-I-B.36 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].; Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 7 -AND- [PIV-I Profile] Worksheet 3 | PIV-I-B.13 (PT CP 48) | PIV-I X.509 Self-Issued CA -AND- Key Management Certificate: CRLDistributionPoints: This extension is required in all CA and EE certificates and must contain at least one HTTP URI. CRL Profile: The reasons and cRLIssuer fields must be omitted. Test requirement does not apply if PIV-I-B.38 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile].; Entity CAs that issue PIV-I Certificates shall comply with [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 8 -AND- [PIV-I Profile] Worksheet 3 | PIV-I-B.14 (PT CP 49) | PIV-I X.509 Self-Issued CA -AND- Content Signing Certificate: CRLDistributionPoints: This extension is required in all CA and EE certificates and must contain at least one HTTP URI. CRL Profile: The reasons and cRLIssuer fields must be omitted. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|---|-----------------------------|-----------------------|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 4 | PIV-I-B.15 (PT CP 50) | PIV-I X.509 Certificate Card Authentication: AuthorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 5 | PIV-I-B.16 (PT CP 51) | PIV-I X.509 Certificate PIV Authentication: AuthorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 6 | PIV-I-B.17 (PT CP 52) | PIV-I X.509 Certificate Digital Signature: AuthorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. Test requirement does not apply if PIV-I-B.36 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 7 | PIV-I-B.18 (PT CP 53) | PIV-I X.509 Certificate Key Management: AuthorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. Test requirement does not apply if PIV-I-B.38 fails. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|---|---|-----------------------|--|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.19 (PT CP 54) | PIV-I X.509 Content Signing Certificate: AuthorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued for PIV-I must include an authorityInfoAccess extension with at least one instance of the caIssuers access method that specifies an HTTP URI. The OCSP access method must also be included since the FBCA mandates OCSP distribution of status information for this certificate. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 4 -AND- [PIV-I Profile] Section 5 | PIV-I-B.20 (PT CP 55) | PIV-I X.509 Self-Issued CA -AND- Card Authentication Certificate: AuthorityInfoAccess id-ad-caIssuers When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found. -AND- Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 5 -AND- [PIV-I Profile] Section 5 | PIV-I-B.21 (PT CP 56) | PIV-I X.509 Self-Issued CA -AND- PIV Authentication Certificate: AuthorityInfoAccess id-ad-caIssuers When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found. -AND- Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|---|---|-----------------------|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 6 -AND- [PIV-I Profile] Section 5 | PIV-I-B.22 (PT CP 57) | PIV-I X.509 Self-Issued CA -AND- Digital Signature Certificate: AuthorityInfoAccess id-ad-caIssuers When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found. -AND- Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI. Test requirement does not apply if PIV-I-B.36 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 7 -AND- [PIV-I Profile] Section 5 | PIV-I-B.23 (PT CP 58) | PIV-I X.509 Self-Issued CA -AND- Key Management Certificate: AuthorityInfoAccess id-ad-caIssuers When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found. -AND- Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI. Test requirement does not apply if PIV-I-B.38 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 1 -AND- [PIV-I Profile] Worksheet 8 -AND- [PIV-I Profile] Section 5 | PIV-I-B.24 (PT CP 59) | PIV-I X.509 Self-Issued CA -AND- Content Signing Certificate: AuthorityInfoAccess id-ad-caIssuers When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible Web server or an LDAP accessible directory server where certificates issued to the issuer of this certificate may be found. -AND- Certificates issued for PIV-I must include an authorityInfoAccess extension that contains at least one instance of the id-ad-caIssuers access method. The access location for this instance must be an HTTP URI. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|--------------------------------|---|-----------------------------|-----------------------|--|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 4 | PIV-I-B.25 (PT CP 60) | PIV-I X.509 Certificate Card Authentication: AuthorityInfoAccess id-ad-ocsp When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 6 | PIV-I-B.26 (PT CP 61) | PIV-I X.509 Certificate PIV Authentication: AuthorityInfoAccess id-ad-ocsp When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 6 | PIV-I-B.27 (PT CP 62) | PIV-I X.509 Certificate Digital Signature: AuthorityInfoAccess id-ad-ocsp When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. Test requirement does not apply if PIV-I-B.36 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 7 | PIV-I-B.28 (PT CP 63) | PIV-I X.509 Certificate Key Management: AuthorityInfoAccess id-ad-ocsp When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. Test requirement does not apply if PIV-I-B.38 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.29 (PT CP 64) | PIV-I X.509 Content Signing Certificate: AuthorityInfoAccess id-ad-ocsp When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate. |
| [FBCA CP] 3.1.1 Types of Names | PIV-I Card Authentication: Non-Null Subject Name, and Subject Alternative Name | [PIV-I Profile] Worksheet 4 | PIV-I-B.30 (PT CP 65) | PIV-I X.509 Certificate Card Authentication: Subject name: MUST include a Non-NULL Subject DN |
| [FBCA CP] Appendix A Item 5 | PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that: a. conforms to [PIV-I - Profile]; b. conforms to [NIST SP 800-73]; and c. is issued under the PIV-I Card Authentication policy. | [PIV-I Profile] Worksheet 4 | PIV-I-B.31 (PT CP 66) | PIV-I X.509 Certificate Card Authentication: CertificatePolicies: One policy that maps to id-fpki-certpcy-pivi-cardAuth must be present. Other policies may be asserted as well. The Certificate path will be validated to show a policy mapping to 2.16.840.1.101.3.2.1.3.19, or Test OID 2.16.840.1.101.3.2.1.48.79 |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|--|-----------------------------|-----------------------|--|
| [FBCA CP] Appendix A Item 5 | PIV-I Cards shall contain an asymmetric X.509 Certificate for Card Authentication that: a. conforms to [PIV-I - Profile]; b. conforms to [NIST SP 800-73]; and c. is issued under the PIV-I Card Authentication policy. | [PIV-I Profile] Worksheet 4 | PIV-I-B.32 (PT CP 67) | PIV-I X.509 Certificate Card Authentication: SubjectAltName criticality flag must be false |
| [FBCA CP] Appendix A Item 3 | The mandatory X.509 Certificate for Authentication shall be issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID. | [PIV-I Profile] Worksheet 5 | PIV-I-B.33 (PT CP 68) | PIV-I X.509 Certificate PIV Authentication: CertificatePolicies: One policy that maps to id-fpki-certpcy-pivi-hardware must be present. Other policies may be asserted as well. The Certificate path will be validated to show a policy mapping to 2.16.840.1.101.3.2.1.3.18, or Test OID 2.16.840.1.101.3.2.1.48.78 |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 5 | PIV-I-B.34 (PT CP 69) | PIV-I X.509 Certificate PIV Authentication: SubjectAltName criticality flag must be false |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 6 | PIV-I-B.35 (PT CP 70) | PIV-I X.509 Certificate Digital Signature: certificates cannot have a subjectPublicKey modulus of 1024 bits |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 6 | PIV-I-B.36 (PT CP 71) | PIV-I X.509 Certificate Digital Signature: CertificatePolicies, One policy that maps to id-fpki-certpcy-pivi-hardware must be present. Other policies may be asserted as well. Must map to 2.16.840.1.101.3.2.1.3.18, or Test OID 2.16.840.1.101.3.2.1.48.78 |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 7 | PIV-I-B.37 (PT CP 72) | PIV-I X.509 Certificate Key Management: cannot have a subjectPublicKey modulus of 1024 bits |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|------------------------------|---|-----------------------------|-----------------------|--|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 7 | PIV-I-B.38 (PT CP 73) | PIV-I X.509 Certificate Key Management: CertificatePolicies: One policy that maps to id-fpki-certpcy-pivi-hardware must be present. Other policies may be asserted as well. Must map to 2.16.840.1.101.3.2.1.3.18, or Test OID 2.16.840.1.101.3.2.1.48.78 |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.39 (PT CP 74) | The Content Signing certificate keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.40 (PT CP 75) | PIV-I X.509 Content Signing Certificate: Content Signing Certificate is required |
| [FBCA CP] Appendix A Item 12 | The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.41 (PT CP 76) | PIV-I X.509 Content Signing Certificate: CertificatePolicies: One policy that maps to id-fpki-certpcy-pivi-contentSigning must be present. Other policies may be asserted as well. Must map to 2.16.840.1.101.3.2.1.3.20, or Test OID 2.16.840.1.101.3.2.1.48.80 |
| [FBCA CP] Appendix A Item 12 | The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. The PIV-I Content Signing certificate shall conform to [PIV-I Profile]. | [PIV-I Profile] Worksheet 8 | PIV-I-B.42 (PT CP 77) | PIV-I X.509 Content Signing Certificate: ExtendedKeyUsage must have criticality set to true and contain id-fpki-pivi-contentSigning (2.16.840.1.101.3.8.7) |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|-----------------------------|---|-------------------|-----------------------|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.43 (PT CP 78) | For PIV-I X.509 Certificate: Card Authentication subscriber certificates - use of the subscriber common name is prohibited. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.44 (PT CP 79) | PIV-I X.509 Certificate PIV Authentication: PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: For certificates with an Affiliated Organization: cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}. For certificates with no Affiliated Organization: cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.45 (PT CP 80) | PIV-I X.509 Certificate Digital Signature, if present: PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: For certificates with an Affiliated Organization: cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}. For certificates with no Affiliated Organization: cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}. Test requirement does not apply if PIV-I-B.36 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.46 (PT CP 81) | PIV-I X.509 Certificate Key Management, if present: PIV-I Hardware certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: For certificates with an Affiliated Organization: cn=Subscriber's full name, ou=Affiliated Organization Name, {Base DN}. For certificates with no Affiliated Organization: cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}. Test requirement does not apply if PIV-I-B.38 fails. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.47 (PT CP 82) | PIV-I X.509 Certificate Content Signing certificates shall clearly indicate the organization administering the CMS. |

| FBCA Source | FBCA Test Requirement | Additional Source | Test ID | Test Requirement |
|------------------------------|---|---------------------------------------|--|--|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [FBCA CP] 3.1.1 | PIV-I-B.48 (PT CP 83) | PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: For certificates with an Affiliated Organization: serialNumber=UUID, ou=Affiliated Organization Name, {Base DN}. For certificates with no Affiliated Organization: serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name, {Base DN}. |
| [FBCA CP] Appendix A Item 11 | Expiration of the PIV-I Card should not be later than expiration of PIV-I Content Signing certificate on the card. | | PIV-I-B.49 (PT CP 84) | PIV-I Content Signing Certificate must not expire before the expiration date on the card or the signature of the CHUID. |
| FBCA CP Appendix A Item 10 | PIV-I Cards shall have an expiration date not to exceed 5 years of issuance. | | PIV-I-B.50 (PT CP 85) | PIV-I CHUID expiration date cannot extend beyond 5 years into the future. |
| FBCA CP Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | SP 800-73-3 Part 4 Section 2.5 Item 1 | PIV-I-B.51 (PT DS 67,69) (PT CP 86-90) | If the card is a PIV-I Card, the FASC-N shall be omitted from certificates and CMS-Signed data objects. |
| FBCA CP Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | SP 800-73-3 Part 4 Section 2.5 Item3 | PIV-I-B.52 (PT DS 68,70) | The same 16-byte binary representation of the UUID value shall be present as the value of an entryUUID attribute, as defined in [IETF RFC 4530], in any CMS-signed data object that is required to contain a pivFASC-N attribute on a PIV Card, i.e., in the fingerprint template and facial image data objects. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | [PIV-I Profile] Section 1 | PIV-I-B.53 (PT CP 91-95) | X509 Certificates must be Version 3. |
| FBCA CP Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | | PIV-I-B.54 (PT CP 96-100) | Dates through year 2049 must be formatted YYMMDDHHMMSSZ, after YYYYMMDDHHMMSSZ. |
| FBCA CP Appendix A Item 2 | PIV-I Cards shall conform to [NIST SP 800-73]. | | PIV-I-B.55 (PT CP 101-105) | Certificate Serial number cannot be negative. |

Table 10: Optional Facial Image PIV Tests Mandatory for PIV-I

| Test ID | Source |
|---------|---|
| EP.17 | NIST SP 800-73-3, Appendix A |
| EP.23 | NIST SP 800-76-1, Section 6 Para 2 pg.17 |
| EP.24 | NIST SP 800-76-1, Section 6 Para 14 pg.17 |
| EP.25 | NIST SP 800-76-1, Section 6 Para 3 pg.18 |
| EP.26 | NIST SP 800-76-1, Section 6 Para 3 pg.18 |
| EP.27 | NIST SP 800-76-1, Section 6 Para 14 pg.17 |
| EP.28 | NIST SP 800-76-1, Section 6 Para 3 pg.18 |
| EP.29 | NIST SP 800-76-1, Section 6 Para 3 pg.18 |
| EP.30 | NIST SP 800-76-1, Section 6 Para 3 pg.18 |
| EP.31 | NIST SP 800-76-1 Para 3 pg.18 |
| EP.32 | NIST SP 800-76-1 Para 3 pg.18 |
| EP.33 | NIST SP 800-76-1 Para 3 pg.19 |
| EP.34 | NIST SP 800-76-1 Para 3 pg.19 |
| EP.35 | NIST SP 800-76-1 Para 3 pg.17 |
| EP.60 | NIST SP 800-76-1, Section 5.2 Para 1 pg.14 |
| EP.61 | NIST SP 800-76-1, Section 5.2 Para 1 pg.14 |
| EP.100 | FIPS 201-1, Section 4.4.2 Para 2 pg.35 |
| EP.101 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.102 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.103 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.104 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.105 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.106 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.107 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.108 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.109 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.110 | NIST SP 800-78-2, Section 3.2.1 Para 2 pg.5 |
| EP.111 | FIPS 201-1, Section 4.4.2 Para 3 pg.36 |
| EP.112 | FIPS 201-1, Section 4.4.2 Para 3 pg.36 |
| EP.113 | FIPS 201-1, Section 4.4.2 Para 3 pg.36 |
| EP.114 | NIST SP 800-78-2, Section 3.2.1 Para 2 pg.5 |
| EP.115 | FIPS 201-1, Section 4.4.2 Para 3 pg.35 |
| EP.117 | NIST SP 800-78-2, Section 3.2.1 Para 2 pg.5 |
| EP.162 | NIST SP 800-78-2, Section 3.2.1 Para 2 pg.5 |

Table 11: Optional Card Authentication PIV Tests Mandatory for PIV-I

| Test ID | Source |
|----------------|-----------------------------|
| EP.163 | [FBCA CP] Appendix A Item 5 |
| EP.164 | [FBCA CP] Appendix A Item 5 |
| EP.166 | [FBCA CP] Appendix A Item 5 |
| EP.168 | [FBCA CP] Appendix A Item 5 |
| EP.169 | [FBCA CP] Appendix A Item 5 |
| EP.172 | [FBCA CP] Appendix A Item 5 |
| EP.173 | [FBCA CP] Appendix A Item 5 |
| EP.175 | [FBCA CP] Appendix A Item 5 |
| EP.21 | [FBCA CP] Appendix A Item 5 |

Table 12: PIV-I Requirements for Data Model Tests, PIV Tests Skipped for PIV-I

| PIV-I Source | PIV-I Test Requirement | Change from PIV to PIV-I | Test ID | PIV Source | PIV Test Requirement |
|-----------------------------|---|--|---------|--|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.116 | FIPS 201-1, Section 4.4.2 Para 4 pg.36 | The digital signature certificate used to sign PIV facial image biometric shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7). |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.135 | X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9 | The policyIdentifier field in the certificatePolicies must assert id-fpki-common-authentication (OID = 2.16.840.1.101.3.2.1.3.13). |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.137 | FIPS 201-1, Section 4.3 | The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute (OID = 2.16.840.1.101.3.6.6). |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.138 | X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9 | The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present and contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. |

| PIV-I Source | PIV-I Test Requirement | Change from PIV to PIV-I | Test ID | PIV Source | PIV Test Requirement |
|---------------------------------------|---|--|---------|--|---|
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.167 | X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6 | The policyIdentifier field in the certificatePolicies must assert id-fpki-common-cardAuth (OID = 2.16.840.1.101.3.2.1.3.17). |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.171 | X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6 | The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present contain an interim_indicator field which is populated with a Boolean value. This extension is not critical. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.174 | Derived | The FASC-N in the subjectAltName field in the card authentication certificate is the same as the FASC-N present in the CHUID. |
| [FBCA CP] Appendix A Item 4 | All certificates issued a policy OID cross certified with the PIV-I Hardware policy OID shall conform to [PIV-I Profile]. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.80 | FIPS 201-1, Section 4.2.2 Para 3 pg.31 | The digital signature certificate used to sign the CHUID shall in the extKeyUsage assert id-PIV-content-signing OID = 2.16.840.1.101.3.6.7). |
| SP 800-73-3 Part 4 Section 2.5 Item 1 | If the card is a PIV-I Card... In this case, the FASC-N shall be omitted from certificates and CMS-Signed data objects. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.34 | SP 800-76-1, Section 6 Para 3 pg.19 | The Data Type Encoding field in the PIV Patron Format shall contain the 25 bytes of the FASC-N component of the CHUID identifier. |
| SP 800-73-3 Part 4 Section 2.5 Item 1 | If the card is a PIV-I Card... In this case, the FASC-N shall be omitted from certificates and CMS-Signed data objects. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.94 | FIPS 201-1, Section 4.4.2 Para 3 pg.36 | The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card. |

| PIV-I Source | PIV-I Test Requirement | Change from PIV to PIV-I | Test ID | PIV Source | PIV Test Requirement |
|---------------------------------------|---|--|---------|--|---|
| SP 800-73-3 Part 4 Section 2.5 Item 1 | If the card is a PIV-I Card... In this case, the FASC-N shall be omitted from certificates and CMS-Signed data objects. | Test Skipped: conforms to PIV-I Profile, not PIV | EP.113 | FIPS 201-1, Section 4.4.2 Para 3 pg.36 | The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card. |

Appendix C PIV-I Requirements for Application Interoperability Testing

Table 13 lists the PACS testing requirements for PIV-I.

Table 13: PIV-I Requirements for Application Interoperability Testing

| Source | Test ID | Test Requirement |
|----------------------------|-----------|---|
| FBCA CP Appendix A Item 14 | PIV-I-C.1 | At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1. 3.2.3.1 Authentication of Human Subscribers. For PIV-I Certificates: The following biometric data shall be collected during the identity proofing and registration process, and shall be formatted in accordance with [NIST SP 800-76] (see Appendix A): An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. A new facial image shall be collected each time a card is issued; and Two electronic fingerprints to be stored on the card for automated authentication during card usage. |

- [PIV Data Model Test Tool] GSA's SP 800-85B Data Conformance Test Tool,
install_data_model_tester_6.0.0.jar
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwn
- [PIV Facial Image Test Tool] GSA's PIV Facial Image Test Runner,
install_facial_img_template_tester.jar
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwn
- [PIV-I NFI] Personal Identity Verification Interoperability for Non-Federal
Issuers; July 2010
https://www.idmanagement.gov/IDM/s/document_detail?Id=kA0t0000008OfMCAU
- [RFC 4122] A Universally Unique Identifier (UUID) URN Namespace, July 2005
<http://tools.ietf.org/html/rfc4122>

Appendix E Acronyms

| Acronym | Definition |
|---------|--|
| AIA | Authority Information Access |
| AID | Application Identifier |
| APL | Approved Products List |
| CA | Certification Authority |
| CAK | Card Authentication Key |
| CHUID | Cardholder Unique Identifier |
| CP | Certificate Policy |
| CPWG | Certificate Profile Working Group |
| CRL | Certificate Revocation List |
| CRLDP | Certificate Revocation List Distribution Point |
| CSS | Certificate Status Services |
| DN | Distinguished Name |
| FASC-N | Federal Agency. Smart Credential Number |
| FBCA | Federal Bridge Certification Authority |
| FIPS | Federal Information Processing Standard |
| FPKI | Federal Public Key Infrastructure |
| FPKIPA | Federal Public Key Infrastructure Policy Authority |
| GSA | General Services Administration |
| GUID | Global Unique Identifier |
| HTTP | HyperText Transfer Protocol |
| ICAM | Identity, Credential and Access Management |
| LACS | Logical Access Control System |
| LDAP | Lightweight Directory Access Protocol |
| NFI | Non-Federal Issuer |
| NIST | National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |

| Acronym | Definition |
|----------------|--|
| OID | Object Identifier |
| OU | Organizational Unit |
| PACS | Physical Access Control System |
| PDVal | Path Discovery and Validation |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PIV-I | PIV Interoperable |
| PK | Public Key |
| PKI | Public Key Infrastructure |
| RFC | Request for Comment |
| SCVP | Server-based Certificate Validation Protocol |
| SP | Special Publication |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| UUID | Universally Unique Identifier |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |