The NIST PIV Program (NPIVP)

Programmatic Guidance to PIV Card Application and Middleware Conformance Testing

1.0 Introduction

1.1 Authority

This guidance document is issued by the National Institute of Standards and Technology (NIST), which serve as the validation authority of the NIST PIV Program (NPIVP). The NPIVP is a program under which National Voluntary Laboratory Accreditation Program (NVLAP) accredited NPIVP testing laboratories test PIV card application and PIV middleware implementations for conformance to the Special Publications 800-73, *Interfaces for Personal Identity Verification* [SP800-73-1]. SP 800-73 is a associated publication of Federal Information Processing Standard 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, was developed to establish standards for identity credentials [FIPS201-1].

1.2 Purpose and Scope

This document is intended to provide general NPIVP programmatic guidance for laboratories. Additionally, this guidance includes clarifications and guidance for PIV card application and middleware conformance testing as specified in SP 800-85A *PIV Card Application and Middleware Interface Test Guidelines (SP800-73 Compliance)* [SP800-85A].

1.3 Maintenance

The guidance presented in this document is based on responses issued by NIST to questions posed by the NPIVP labs, vendors, and other interested parties. Information in this document is subject to change by NIST.

1.4 Document Overview

The document is organized as follows:

+ Section 1, *Introduction* provides the purpose, scope, authority and maintenance of the document and outlines its structure.

+ Section 2, *General Programmatic Guidance*, identifies and details the programmatic guidance for NPIVP laboratories to follow.

+ Section 3, *PIV Card Application Requirements* covers PIV card application implementation specific guidance.

+ Section 4, *PIV Middleware Requirements,* details PIV middleware implementation specific guidance.

+ Appendix A, *References*, contains the list of documents used as references by this document.

+ Appendix B, *Abbreviations and Acronyms* describes the vocabulary and textual representations used in the document.

+ Appendix C contains a PIV middleware validation certificate template

+ Appendix D contains a PIV card application validation certificate template

+ Appendix E contains the Vendor Product Configuration and Nomenclature Template for the PIV card application.

2.0 General Programmatic Guidance

2.1 Request for Guidelines

There are two types of requests: Official requests and informal requests for guidelines.

2.1.1 Official Request

2.1.1:
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

An official request for guidelines must be submitted to the NPIVP in writing in the Request for Guidance (RFG) format described below. The response to the request will be reviewed by NIST, and may require follow-up questions from the NPIVP. As a result, the official response may not be immediate.

Request for Guidance Format: Questions submitted in this format will result in an official response from the NPIVP that will state current policy or interpretations. This format provides the NPIVP a clear understanding of the question. A RFG includes:

1. Clear indication of whether the RFG is PROPRIETARY or NON-PROPRIETARY,
2. A descriptive title,
3. Applicable statement(s) from FIPS 201-1, SP 800-85A and/or, SP800-73
4. Applicable assertion(s) from the DTR in SP 800-85A,
5. Applicable required test procedure(s) from the SP800-85A DTR,
8. Background information if applicable, including any previous NPIVP official rulings or guidance,
9. A description of the problem, followed by a clear question regarding the problem, and
10. a suggested resolution that is being sought.

The information should also include a brief non-proprietary description of the implementation. All of this will enable a more efficient and timely resolution of the questions by the NPIVP. The statement of resolution shall be stated in a manner which

the NPIVP can either answer "YES" or "NO". The NPIVP may optionally provide rationale if the answer is not in line with the suggested statement of resolution.

When appropriate, the NPIVP may derive general guidance from the problem and response, and add it to this document. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

2.1.2 Informal Request

2.1.2
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

Informal requests are ad-hoc question, intended to clarifying issues about SP 800-85, SP800-73 and programmatic questions. Replies to informal requests by the NPIVP team are non-binding and subject to change. It is recommended that informal requests be submitted to all points of contact (see section 2.1.3). Every attempt is made to reply to informal request with accurate, consistent, clear replies on a timely basis.

2.1.3 NPIVP Contact Information

2.1.3
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

Chandramouli Ramaswamy:
Email: Chandramouli.Ramaswamy@nist.gov
Telephone: (301) 975-5013

Hildy Ferraiolo
Email: Hildegard.Ferraiolo@nist.gov
Telephone: (301) 975-6972

2.2 Completion of a Test Report

2.2
Applicable Levels: All
Original Publishing Date: 1/11/2008
Effective Date: 11/08/2006
Last Modified Date:

In order for NIST to perform validation reviews, the NPIVP laboratory shall provide to NPIVP a complete evaluation package that includes all of the following documents:

1. VTEC test runner generated output files:
   a) The test result summary files <pdf> and <html>.
   b) The result folder containing all test runner-generated results files and subfolder <xml>
   c) The logs folder containing all test runner-generated logs files <txt>
   d) All configuration files used to setup the test-scenario <xml>
   e) The report folder containing all test runner Reports files <xml> and <html>
2. A short report consisting of: <electronic copy in DOC or PDF>
   a) A brief description of the product in a paragraph or two, with:
      For PIV card Application:
         1. Completed forms in section E-1 or E-2 of Appendix E
      For PIV Middleware:
         1. PIV Middleware name and version
         2. Vendor legal name(s)
   b) A list of the optional implemented data objects (for PIV card application only)
   c) The name and location of the configuration file
   c) Justifications of any failed tests, if applicable
   d) Recommendation for validation.
3. The validation certificate containing the vendor and laboratory specific data in MS word format (see Appendix A and B for the templates)

The evaluation package shall be encrypted and sent via electronically mail to the following NIST points of contact:

Ramaswamy Chandramouli (Ramaswamy.Chandramouli@nist.gov)
and Hildegard Ferraiolo (Hildegard.Ferraiolo@nist.gov)

An initial check on the completeness of the evaluation package will not be performed upon initial receipt. The electronic submission of the evaluation package will determine the position in the NPIVP validation review queue. If the PIV card application or middleware is listed in the pre-validation list, the entry in the list will be updated to "Evaluation under Review", once the report reaches the top of the queue and a formal review is started.

2.3 Designing, Consulting and Testing of PIV Middleware and PIV Card Application Implementations

2.3
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

For PIV card application, please consult the Implementation Guidance (IG) in the Cryptographic Module Validation Program (CMVP) section G.4 for the designing, consulting and testing roles of the laboratories.

For PIV middleware, NPIVP defines the following roles of separation of the design, consulting and testing roles of the laboratories as follows:

1) A NPIVP Laboratory may not perform validation testing on a PIV middleware if the laboratory has designed implemented or developed original documentation of any part of the PIV middleware.

2) A NPIVP Laboratory may also not perform validation testing if it has any ownership or vested interest in the PIV middleware implementation under testing.

A NPIVP Laboratory may perform consulting services to clarify SP800-85A, SP800-73, FIPS 201 and other associated documents developed by the NIST at any time during the life cycle of the PIV middleware.

2.4 Relationship among Vendors, Laboratories and NIST

Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:
Applicable Levels: All

The NPIVP laboratories are accredited by NVLAP to perform PIV card application and middleware validation testing to determine compliance with SP 800-73. NIST relies on the NPIVP laboratories to use their extensive validation testing experience and expertise to make sound, correct, and independent decisions based on SP 800-85A, the derived test requirements, and implementation guidance. Once a vendor is under contract with a laboratory, NIST will only provide official guidance and clarification for the vendor's PIV card application and middleware through the point of contact at the laboratory.

In rare situation where the vendor and laboratory are at an irresolvable impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST. The vendor should use the format as described in section 1.1 and the point of contact at the laboratory must be carbon copied. All correspondence from NIST to the vendor on the issue will be issued through the laboratory point of contact.

2.5 Official Validation Certificates Source

2.5
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The NPIVP web-based validation list is the official source of validation information of PIV card application and PIV middleware implementations. The initial printed validation certificate and its softcopy is for informational purposes only.

If changes are made to a validation, that would change the referenced certificate information, only the web-based validation list will be updated, while the hardcopy validation certificate and its softcopy validation certificate (online) remain unchanged.

2.6 Use of NPIVP Trade Marks and Logo

2.6.1 Use NPIVP Trade Marks by Vendors

2.6.1
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo are intended for use in association with products complying with FIPS 201, Personal Identity Verification of Federal Employees and Contractors, and accompanying special publications. Vendors with FIPS 201 products that have been validated by NIST may use the phrases and NPIVP logo provided they agree to the following:

+ The phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo are Trade Marks of NIST, which retains exclusive rights to their use.

+ NIST reserves the right to control the quality of the use of the phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo.

+ Permission for advertising the phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo is conditional on and limited to those products that passed the appropriate conformance testing.

+ Use of the NPIVP logo on product reports, letterhead, brochures, marketing materials, product packaging, and any other printed usage must be accompanied by the following: "TM: A Trade Mark of NIST, which does not imply product endorsement by NIST." If the NPIVP certified item is a component of a product, then the phrase "NPIVP validated Product Inside" must accompany the logo.

+ Permission to use the phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo may be revoked at the discretion of NIST.

+ Permission to use the phrases "FIPS 201 Interface Conformant PIV Card Application™", "FIPS 201 Interface Conformant PIV Middleware™", "NIST Special Publication 800-7-3-1 End-Point Specification Compliant™", "NIST Special Publication 800-76 Compliant™", "FIPS 201 Compliant™", and the NPIVP logo in no way constitutes or implies product endorsement by NIST.

Electronic copies of the logo are available upon request from NIST.

2.6.2 Use of NPIVP logo by Laboratories:

2.6.2
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

NIST Personal Identity Verification Program (NPIVP) Testing Laboratories, subject to their NVLAP accreditation, may use the NPIVP logo. Use of the NPIVP logo shall be specified in the NPIVP Laboratories Quality Manual documentation. Laboratories accredited by NIST may use the NPIVP logo provided they agree to the following:

+ The NPIVP logo is a trade mark of NIST, which retains exclusive rights to its use.

+ Permission to use the NPIVP logo may be revoked at the discretion of NIST.

+ Permission to use the NPIVP logo is granted to NVLAP-accredited laboratories for the limited purpose of announcing their accredited status and for use on reports that describe only testing within the scope of the accreditation. NIST reserves the right to control the quality of the NPIVP logo.

+ NIST will control the use of the NPIVP logo to ensure that accredited laboratories express their accredited status in a manner that is clear and accurate, and not misleading.

+ Each test report bearing the term or logo shall include a statement that the report must not be used by the client to claim endorsement by NIST.

+ Electronic copies of the logo are available upon request from NIST.

3.0 PIV Card Application Requirements

3.1 PIV Card Application Test Guidelines

3.1
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

SP 800-85A specifies the test plan, processes, derived test requirements, and test assertions/conformance tests for testing PIV middleware and PIV card application.

Please consult SP 800-85A first for questions you might have in regards to the test plan, processes, DTR, and TA / conformance tests for testing PIV middleware and PIV card application. Further clarifications will be added to this section as needed.

3.2 PIV Card Application Pre-Validation Process

3.2
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The following phases describe the pre-validation process for evaluating and validating PIV Card Application.

PIV Card Application Testing in Progress:

+ There exists a viable contract between a vendor and a NPIVP testing facility for the testing of the vendor's PIV card application
+ The PIV card application and all of the required documentation have been submitted to the NPIVP testing facility.

PIV Card Application Interface Validation under Review

+ Complete set of test reports and associated documentation have been submitted to the NPIVP for review (see section 1.2)
+ Signed letter from the test facility stating recommendation for validation received by the NPIVP.
+ NPIVP is reviewing the test report and associated documentation.

PIV Card Application Interface Validated

+ All issues in validation review comments have been resolved.
+ Certificate number assigned.
+ Certificate printing and signature process initiated.

NPIVP maintains a pre-validation list at http://www.nist.gov/npivp. The participation on the list is voluntary and is a joint decision by the vendor and the NPIVP test facility. Products are listed alphabetically by vendor name. Posting on the list does not imply guarantee of final validation. The implementation listing will be removed from the pre-validation list and transferred to the PIV card application validation list once a vendor's PIV card application validation certificate has been approved and signed.

Laboratories should email npivp@nist.gov with the following information in order for NPIVP to add a new pre-validation entry.

1) PIV card application product name[1] and optionally version number
2) Vendor legal name(s)
3) Name, version and memory size of the hosting cryptographic module

3.3 PIV Card Application Validation Certificate

3.3
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

A validation certificate indicates that based on the test evidence, the tested and evaluated PIV card application is conformant to the end-point PIV card command interface specifications in Chapter 7 of NIST SP 800-73-1 as specified in the Derived Test Requirements (DTR) and Test Assertions (AS) in NIST Special Publication (SP) 800-85A *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-1 Compliance)*. The validation pertains to the card application coupled with its operational environment.

Upon validation, a paper certificate will be issued to the laboratory to be sent to the vendor. The NIST maintains a validation list of all validated PIV card application (past and present) for information purposes. The list is maintained in ascending order of certificate numbers and is updated as new PIV Card Applications receive validation certificates from the NPIVP.

3.4 FIPS 201 Compliance, SP 800-73 Compliance and FIPS 140-2 Compliance

3.4
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The PIV card application is considered “NIST Special Publication 800-73-1 End-Point

[1] See section 2.8 for guidance on PIV card application naming convention.

Specification Compliant™" if it has been validated to be conformant to the PIV end-point card command interface specifications in Chapter 7 of NIST SP 800-73-1 as evidenced by the validation certificate.

FIPS 201 appendix B.3 specifies that a PIV system/component is "FIPS 201-compliant" after each of its constituent parts have met individual validation requirements. For a PIV card (or ICC), the constituent parts requiring validation include 1) PIV card application validation for conformance to SP 800-73 through NPIVP and 2) cryptographic module validation for FIPS 140-2 *Security Requirements for Cryptographic Modules* [FIPS 140-2] compliance of the cryptographic module that hosts the PIV card application.

The PIV card application, thus, is considered "FIPS 201 Interface Conformant PIV card application" and/or "FIPS 201 Compliant™" if the associated cryptographic module is validated for FIPS 140-2 standard conformance and the accompanying FIPS 140-2 validation certificate references the PIV card application certificate[2].

3.5 Binding to Cryptographic Module Validation Certificate

3.5
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

PIV card application implementations are tested and validated under the NIST PIV Program (NPIVP). The PIV card application interface validation certificate states the name and version number of the validated implementation along with the operational environment and hosting cryptographic module. Additionally, the PIV Card application web-base validation list references the cryptographic module certificate(s) for each implementation.

The cryptographic module containing the PIV card application undergoes testing for compliance to FIPS 140-2. The validated module references the PIV card application certificate in the cryptographic module validation certificate.

For the cryptographic module validation of the module containing a validated PIV card application, the following requirements must be met:

+ a) The implementation of the validated PIV card application has not been modified upon integration into the cryptographic module undergoing testing

[2] Please note that the PIV Card application web-base validation also cross-references the cryptographic module certificate.

+ The operational environment under which the validated PIV card application implementation was tested by NPIVP must be identical to the one that the PIV card application is being tested under FIPS 140-2 validation by the CMVP laboratory.

The cover letter to the CMVP containing a FIPS 140-2 evaluation submission package, shall state that the cryptographic module contains a PIV card application and reference the PIV card application certificate number.

3.6 Updates to the PIV Card Application Validation List

3.6
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

A cryptographic module containing a validated PIV card application might be subjected to re-validation because of changes to the cryptographic module. If the changes to the cryptographic module are security related, then a new FIPS 140-2 validation certificate is issued. NPIVP laboratories shall inform NPIVP (npivp@nist.gov) if a cryptographic module containing a validated PIV card application has been re-validated and issued a new FIPS 140-2 certificate. Upon notification, the web-based PIV card Application validation list will be updated by adding the additional FIPS 140-2 validation certificate number to the corresponding PIV card application listing. The aforementioned scenario assumes that the validated PIV card application remains unchanged[3].

Laboratories should email npivp@nist.gov for all other updates such as vendor name changes and/or product name changes.

3.7 PIV Card Application Porting and Re-validation

3.7
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

PIV card applications can be ported to cryptographic modules that include the same operational environment[4] as the validated PIV card application's operational

[3]Refer to section 3.7 for PIV card application re-validation requirements

[4] For software implementations, operating environment includes processor and operating system; for firmware implementations, operating environment includes processor only; for hardware implementations, operating environment is not applicable)

environment. PIV card applications can also be ported with its associated cryptographic module. For cryptographic module porting guidance, please review CMVP's IG G.5.

In general, a PIV card application implementation is validated by NPIVP for a specific cryptographic module. Any modification to the PIV card application itself constitutes a different implementation and does not represent the validated implementation. Hence the new version requires validation in order to be listed in NPIVP's web-based validation list.

Changes to the PIV data model might cause changes to the PIV card application in implementations that have no logical separation between the PIV data model and the PIV card application. PIV card application that are a tight coupled to the PIV data-model might require source code changes to accommodate the updated PIV data model; thus, requiring re-validated. On the other hand, logically separated implementation between PIV card application and PIV data model are not affected to changes to the PIV data model and do not need re-validation.

3.8 Pre- ROM Mask Validation

3.8
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The PIV card application can reside in ROM (hard mask), as opposed to the EEPROM. Because the process of ROM-based software coding and debugging, can be long and involved, NPIVP will accept chip-simulators/emulators-based PIV card application test report for review. However, a review of a PIV card application report based on a simulated/emulated chip will not result in a validation certificate. Laboratories should be aware that the evaluation provided by NPIVP is a good-faith validation and does not guarantee that the masked PIV card application will validate.

3.9 PIV Card Application Naming Convention

3.9
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The PIV card application product name should reflect the name of the PIV card application implementation itself. It should not reflect the name of the cryptographic module that contains this implementation. Naming both the PIV card application

implementation and the cryptographic module the same might cause major problems later on when the PIV card application implementation is ported to another module. It might also cause confusion when a module version number changes but the PIV card application implementation version number does not, or visa versa. Additionally, vendors should assure that the name supplied should reflect the PIV card application's functionalities as per SP 800-73 and SP 800-85A and should not imply additional, out of scope capabilities.

4.0 PIV Middleware Requirements

4.1 PIV Middleware Test Guidelines

4.1
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

SP 800-85-A specifies the test plan, processes, derived test requirements, and test assertions/conformance tests for testing PIV middleware and PIV card application.

Please consult SP 800-85A first for questions you might have in regards to the test plan, processes, DTR, and TA / conformance tests for testing PIV middleware. Further clarifications will be added to this section as needed.

4.2 PIV Middleware Pre-Validation Process

4.2
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The following phases describe the PIV Middleware pre-validation process.

PIV Middleware Testing in Progress:

+ There exists a viable contract between a vendor and a NPIVP testing facility for the testing of the vendor's PIV Middleware.
+ The PIV Middleware and all of the required documentation have been submitted to the NPIVP testing facility.

PIV Middleware Validation under Review:

+ Complete set of test reports and associated documentation have been submitted to the NPIVP for review.
+ Signed letter from the test facility stating recommendation for validation received by the NPIVP.
+ NPIVP is reviewing the test report and associated documentation.

Middleware Validated:

+ All issues in validation review comments have been resolved.
+ Certificate number assigned - certificate printing and signature process initiated.

The NPIVP maintains a PIV middleware pre-validation list at http://www.nist.gov/npivp. Participation on the list is voluntary and is a joint decision by the vendor and NPIVP test facility. Products are listed alphabetically by name. Posting on the list does not imply guarantee of final validation. The status of each product in the process is identified in the list. The listing will be removed from the pre-validation list and transferred to the PIV middleware validation list once the PIV middleware product received a validation certificate.

Laboratories should email npivp@nist.gov with the following information in order for NPIVP to add a new pre-validation implementation.

1) Product name[5] and version and 2) Vendor legal name(s)

4.3 PIV Middleware Validation Certificate

4.3
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

A PIV middleware validation certificate indicates that based upon the test evidence submitted to the NPIVP, the validated PIV middleware implementation is conformant to the End-Point PIV client-application programming interface specifications in Chapter 6 of SP 800-73-1 as specified in the Derived Test Requirements (DTR) and Test Assertions (TA) in NIST Special Publication (SP) 800-85A *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-1 Compliance).*

[5] The product name should reflect the PIV middleware functionality and should not imply any out-of-scope capability not pertaining to FIPS 201, SP 800-85A or SP 800-73

The NIST maintains a validation list of all validated PIV middleware (past and present). The list is maintained in ascending order of certificate numbers and is updated as new PIV middleware receives validation certificates from the NPIVP.

4.4 FIPS 201 Compliance and SP 800-73 Compliance

4.4
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

A PIV middleware implementation is considered "FIPS 201 Interface Conformant PIV Middleware ™", "NIST Special Publication 800-73-1 End-Point Specification Compliant™" and/or "FIPS 201 Compliant™ "if (based upon the test evidence submitted to the NPIVP) it has been validated to be conformant to the End-Point PIV client-application programming interface specifications in Chapter 6 of SP 800-73-1. The validation pertains to the PIV middleware implementation coupled with the operational environment.

4.5 PIV Middleware Porting and Re- Validation

4.5
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The porting of PIV middleware implementations is applicable only if no source code changes are made to the validated PIV middleware. New versions of the implementations require re-validation.

4.6 PIV Middleware Naming Convention

4.6
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

The PIV middleware product name should reflect the PIV Middleware functionalities as per SP 800-73 and SP 800-85A and should not imply additional, out of scope capabilities.

4.7 Updates to the PIV Middleware Validation List

4.7
Applicable Levels: All
Original Publishing Date: 11/08/2006
Effective Date: 11/08/2006
Last Modified Date:

Update request such as vendor name changes and/or product name changes for the web-based PIV middleware validation list should be email (by the laboratory) to npivp@nist.gov.

Appendix A – Abbreviations and Acronyms

CMVP	Cryptographic Module Validation Program
DTR	Derived Test Requirements
EEPROM	Electrically Erasable Programmable Ready only Memory
FIPS	Federal Information Processing Standard
HTML	Hypertext Markup Language
ICC	Integrated Circuit Chip
IG	Implementation Guidance
NIST	The National Institute of Standards and Technology
NPIVP	NIST Personal Identity Verification Program
PDF	Portable Data Format
PIV	Personal Identity Verification
RFG	Request for Guidance
ROM	Read Only Memory
SP	Special Publication
TA	Test Assertion
XML	Extendable Markup Language

Appendix B - References

[FIPS201-1] Federal Information Processing Standard 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. (See http://csrc.nist.gov)

[FIPS 140-2] Security Requirements for Cryptographic Modules

[SP800-73-1] NIST Special Publication 800-73-1, Interfaces for Personal Identity Verification, March 2006. (See http://csrc.nist.gov)

[SP800-85A] PIV Card Application and Middleware Interface Test Guidelines (SP800-73 Compliance)

Appendix C – Certificate Template for PIV Middleware

PIV Middleware Interface Validation Certificate

Certificate No.

The National Institute of Standards and Technology, as the NIST Personal Identify Verification Program (NPIVP) Validation Authority; hereby validates the PIV Middleware software application identified as:

[Name of PIV middleware] Version [x]

in accordance with the Derived Test Requirements (DTR) and Test Assertions (TA) as specified in NIST Special Publication (SP) 800-85A *PIV Card Application and Middleware Interface Test Guidelines* (SP800-73 Compliance). SP 800-85A specifies the conformance requirements that have to be satisfied by PIV Middleware with the FIPS 201 Interface specifications in NIST SP 800-73.

This PIV middleware has been validated to be conformant to the End-Point PIV client-application programming interface specifications in Chapter 6 of SP 800-73-1 based upon the test evidence submitted to the NPIVP.

This PIV Middleware Software Application hereby may be labeled as "*FIPS 201 Interface Conformant PIV Middleware™*", "*NIST Special Publication 800-73-1 End-Point Specification Compliant™*" and/or "*FIPS 201 Compliant™*" so long as the product, throughout its life cycle, continues to be used as the validated version as specified in this certificate. No reliability test has been performed and no warranty of the products by NIST is either expressed or implied.

Signature: _____
Dated: _____
William C. Barker,
Chief, Computer Security Division
National Institute of Standards and Technology

Vendor information, product information and laboratory information are listed on the reverse side of the certificate

PIV Middleware Interface Validation Certificate

Certificate No.

Vendor Information:

Name:

Web Site:

Product Information:
Product name:
Version:

Test Laboratory Information:

Name:

NVLAP Laboratory Code:

Test Report Number and Date:

Test toolkit version:

Appendix D – Certificate Template f[illegible]ications

PIV Card Application Interface Validation Certificate

Certificate No.

The National Institute of Standards and Technology, Personal Identity Verification Program (NPIVP) Validation Authority; hereby validates the PIV Card Application identified as:

PIV card application name and version on [type of smart card]

in accordance with the Derived Test Requirements (DTR) and Test Assertions (TA) as specified in NIST Special Publication (SP) 800-85A *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-1 Compliance)*.

This card application has been validated to be conformant to the PIV card command interface specifications in Chapter 7 of NIST SP 800-73-1 based upon the test evidence submitted to the NPIVP. The card application, hereby shall be labeled as "*NIST Special Publication 800-73-1 End-Point Specification Compliant™*" so long as the product, throughout its life cycle continuous to be used as a validated version as specified in this certificate.

The PIV Card Application can be re-labeled as "*FIPS 201 Interface Conformant PIV Card Application™*" and/or "*FIPS 201 Compliant™*" if its associated cryptographic module is validated for FIPS 140-2 standard conformance and the accompanying FIPS 140-2 validation certificate references this certificate. No reliability test has been performed and no warranty of the product by NIST is either expressed or implied. This certificate does not imply that the PIV smart card platform meets all requirements in FIPS 201.

Signature: _____
Dated: _____
William C. Barker,
Chief, Computer Security Division
National Institute of Standards and Technology

Vendor information, product information and laboratory information are listed on the reverse side of the certificate

™

PIV Card Application Interface Validation Certificate

Certificate No.

Vendor Information

Name:[PIV card application Vendor Name]

Web Site: [Vendor Product Website]

Product Information

Product name: [PIV card application name] version [PIV card application version] on [crypto-module]
Version:[PIV card application version]

Test Laboratory Information

Name: [Name of Lab]
NVLAP Laboratory Code: [Lab-code]
Test Report: []

Test Toolkit version: [toolkit version]

Appendix E - Dual Chip and Single Chip Configuration Template

E-1: Single Chip Configuration:

TABLE E-1 – SINGLE CHIP PRODUCT CONFIGURATION AND TEST TOOLS CONFIGURATION –

Configuration Item / Label	Name	Vendor	Version
Top Level PIV Card Assembly			
PIV Card	Product Name		
Contact and Contactless Functionality Module – TID XX-XXXX-XXXX			
Crypto Module			
Chip			
Operating Environment			
PIV Applet			
Smart Card Protocol			
Contact - T= 0 (yes/no)	Contact - T=1 (yes/no)	Contactless – T=CL (yes/no)	
Test Tools			
Test Runner	Test Runner	T-VEC	2.9.8_b45

Enter Nomenclature Here:
In this report, *Product Under Test* refers to the [Product Name], an assembly of a crypto module (TID XX-XXXX-XXXX for contact and contactless) in a plastic card body per FIPS 201-1.

The NPIVP pre-validation listing corresponding to this report is:

Product Name	Vendor Name
[Product Name] on [Crypto Module Name]	[Vendor Name]

The CMVP in process listings corresponding to the crypto modules are:

Module Name	Vendor Name	TID
[Crypto Module Name]	[Vendor Name]	XX-XXXX-XXXX

Note that the TID number is not visible in the online CMVP listing.

E-2: Dual Chip Configuration

TABLE E-2 – DUAL CHIP PRODUCT CONFIGURATION AND TEST TOOLS CONFIGURATION

Configuration Item / Label	Name	Vendor	Version
Top Level PIV Card Assembly			
PIV Card	Product Name		
Contact Functionality Module – TID XX-XXXX-XXXX			
Contact Crypto Module			
Contact Chip			
Contact Operating Environment			
Contact PIV Applet			
Smart Card Protocol			
T= 0 (yes/no)	T=1 (yes/no)		
Contactless Functionality Module – TID XX-XXXX-XXXX			
Contactless Crypto Module			
Contactless Chip			
Contactless Operating Environment			
Contactless PIV Applet			
Smart Card Protocol			
T=CL (yes/no)			
Test Tools			
Test Runner	Test Runner	T-VEC	2.9.8_b45

Enter Nomenclature Here:
In this report, *Product Under Test* refers to the [Product Name], an assembly of [one / two] crypto module[s] (TID XX-XXXX-XXXX for contact and / or TID XX-XXXX-XXXX for contactless) in a plastic card body per FIPS 201-1.

The NPIVP pre-validation listing corresponding to this report is:

Product Name	Vendor Name
[Product Name] on [Crypto Module Name] – (Contact) and [Product Name] on [Crypto Module Name] – (Contactless)	[Vendor Name]

The CMVP in process listings corresponding to the crypto modules are:

Module Name	Vendor Name	TID
[Crypto Module Name] -	[Vendor Name]	XX-XXXX-

Contact		XXXX
[Crypto Module Name] - Contactless	[Vendor Name]	XX-XXXX-XXXX

Note that the TID number is not visible in the online CMVP listing.