January 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

TESTING AND VALIDATION OF PERSONAL IDENTITY VERIFICATION (PIV) COMPONENTS AND SUBSYSTEMS FOR CONFORMANCE TO FEDERAL INFORMATION PROCESSING STANDARD 201

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST), Information Technology Laboratory, has set up a new program to test and validate personal identity verification (PIV) components and subsystems for conformance to Federal Information Processing Standard (FIPS) 201, *Personal Identification Verification (PIV) of Federal Employees and Contractors*. Approved by the Secretary of Commerce in February 2005, FIPS 201 applies to the identification cards that are issued by federal government departments and agencies to their employees and contractors who require access to federal facilities and information systems. PIV cards incorporate an individual's identity credentials on smart cards. PIV components and subsystems use the electronically stored data on the cards to carry out automated identity verification of the individual.

The program for testing and validating PIV components and subsystems for conformance to FIPS 201 is managed by the NIST PIV Program (NPIVP), and testing organizations will be accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP), which provides third-party accreditation to testing and calibration laboratories. NVLAP accredits public and private sector laboratories, including commercial, manufacturers' in-house, university, and federal, state and local government laboratories, based on evaluation of their technical qualifications and their competence to carry out specific calibrations or tests.

FIPS 201 Requirements

Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, established the requirement for a common standard for identification credentials. Issued in August 2004, HSPD 12 directed NIST to develop a mandatory standard for secure and reliable forms of identification for use throughout the federal government. Secure forms of identification are needed to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. In developing the standard, NIST worked with private industry and with other federal agencies, including the Office of Management and Budget, the Office of Science and Technology Policy, and the Departments of Defense, State, Justice, and Homeland Security.

FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that issue smart cards as identification credentials and that use the cards to

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since January 2005:

- *Integrating IT Security into the Capital Planning and Investment Control Process, January 2005*
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* April 2005
- *Recommended Security Controls for Federal Information systems: Guidance of Selecting Cost-effective Controls Using a Risk-based Process, May 2005*
- *NIST's Security Configuration Checklists Program for IT Products,* June 2005
- *Implementation of FIPS 201, Personal Identify Verification (PIV) of Federal Employees and Contractors, August 2005*
- *Biometric Technologies: Helping to Protect Information and Automated Transactions I Information Technology Systems, September 2005*
- *National Vulnerability Database: Helping Information Technology System Users and Developers Find Current Information About Cyber Security Vulnerabilities,* October 2005
- *Securing Microsoft Windows XP Systems: NIST Recommendations for Using a Security Configuration Checklist,* November 2005
- *Preventing and Handling Malware Incidents: How to Protect Information Technology Systems from Malicious Code and Software, December 2005*

authenticate an individual's identity. FIPS 201 was issued in two parts to assist agencies in planning for a smooth migration to secure, reliable personal identification processes. The first part of FIPS 201 (PIV I) describes the minimum requirements needed to meet the control and security objectives of HSPD 12, including the process to prove an individual's identity. Agencies may issue credentials only to applicants whose identities have been established and who have had a background investigation. Federal departments and agencies were required to implement Part 1 in October 2005.

The second part of the standard (PIV II) provides the detailed technical specifications to support the control and security objectives of Part 1, as well as the requirements for the interoperability of PIV cards and systems. Part 2 specifies the policies and minimum requirements for PIV cards, which will allow for the interoperability of PIV cards when used for physical access to facilities and for logical access to information systems. Part 2 also describes the processes for collecting, storing, and maintaining the information and the documentation needed to authenticate and assure an individual's identity.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at
301-975-2832 or
elizabeth.lennon@nist.gov

Federal organizations that are currently using different electronic credential systems will have additional time to phase in their changeover to interoperable systems based on the Part 2 specifications. The Office of Management and Budget (OMB) in its August 5, 2005, Memorandum M-05-24 provides instructions to federal organizations for implementing HSPD 12 and FIPS 201. Federal organizations are required to begin implementation of Part 2 by October 27, 2006. Details on these requirements are available at the OMB website: www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.

When FIPS 201 is fully implemented, it will be possible for a card issued by one agency to be electronically recognized by any other agency, thus enabling a decision to be made about whether to grant the cardholder access to facilities and information systems.

The Validation Program

The use of products that have been tested by independent laboratories and validated for conformance to established standards promotes security and confidence in the products. Initially, the NIST Personal Identity Verification Program (NPIVP) will test and validate the FIPS 201 interface of PIV card applications and PIV middleware for correct implementation of the technical requirements detailed in NIST Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification,* one of the specifications referenced by FIPS 201. The PIV Middleware and PIV Card Application test suites have been modeled according to NIST SP 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines (SP800-73 compliance).*

All of the testing under the NPIVP will be handled by the third-party test facilities. The test facilities, which are listed below, have been designated as interim NPIVP Test Facilities for FIPS 201 components and subsystems. When these NPIVP laboratories have been assessed for NPIVP testing and accredited by NVLAP, the "Interim" designation will be removed.

Interim NPIVP Laboratories

Atlan Laboratories, McLean, Virginia
atsec information security company, Austin, Texas
BKP Security Laboratories, Santa Clara, California
BT Cryptographic Module Testing Laboratory, Fleet, Hampshire, UK
CEAL: a CygnaCom Solutions Laboratory, McLean, Virginia
COACT Inc. CAFÉ Laboratory, Columbia, Maryland
DOMUS IT Security Laboratory, Ottawa, Canada
EWA – Canada IT Evaluation and Test Facility, Ottawa, Canada
ICSA Labs, a division of Cybertrust, Inc., Mechanicsburg, Pennsylvania
InfoGuard Laboratories, Inc., San Luis Obispo, California
LogicaCMG FIPS Laboratory, Leatherhead, Surrey, UK

These interim laboratories for testing FIPS 201 components and subsystems are also accredited to perform conformance testing for FIPS 140-1 and 140-2, *Security Requirements for Cryptographic Modules*. NIST and the Communications Security Establishment (CSE) of the government of Canada jointly administer the Cryptographic Module Validation Program (CMVP), which has issued more than 620 validation certificates representing more than 1,000 modules. All cryptographic modules used in PIV systems, both on the card and in issuer software, must be validated to FIPS 140-2 under the CMVP.

NIST plans to develop additional testing and validation programs under the NPIVP in the future.

FIPS 201 Specifications

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications.

- NIST Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification,* by James F. Dray, Scott B. Guthery, and Teresa Schwarzhoff, specifies the interface requirements for retrieving and using the identity credentials from the PIV card. NIST SP 800-73 provides the PIV data elements, identifiers, structure, and format, and describes the Application Programming Interface (API) and the card interface requirements that will enable PIV identity credentials to be used interchangeably throughout federal agencies. NIST SP 800-73 includes two specifications to help agencies make the transition to conformance with FIPS 201: a transitional card specification that is derived from the Government Smart Card Interoperability Specification and that agencies already invested in smart card implementations might want to consider using; and a Part 2 card specification for agencies choosing to move directly to the Part 2 architecture. A reference implementation for NIST SP 800-73 is available at the NPIVP web page listed in the More Information section below.

- NIST Draft SP 800-76, *Biometric Data Specification for Personal Identity Verification,* by Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli, specifies the technical acquisition and formatting requirements for biometric data used by the PIV system. To assist agencies in implementing FIPS 201, the specification selects options from published biometric standards to facilitate interoperability and ensure performance of PIV systems. Included are specifications for the fingerprints used in the PIV systems, optional specifications for facial images, the format for all PIV biometric data representation, and the requirements for biometric devices. NIST expects to issue the final version of NIST SP 800-76 in early 2006.

- NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* by W. Timothy Polk, Donna F. Dodson, and William E. Burr, specifies the acceptable cryptographic algorithms and key sizes to be implemented in the PIV system. The publication covers the infrastructure components for issuance and management of the PIV card, and the applications for security services that rely on the credentials supported by the PIV card. NIST SP 800-78 identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, and message digest algorithms, and details the mechanisms to identify the algorithms associated with PIV keys or digital signatures. Algorithms and key sizes were selected to be consistent with federal standards and ensure adequate cryptographic strength for PIV applications.

Other NIST Special Publications also support the implementation of FIPS 201 and the testing and validation program.

- NIST SP 800-21-1 is the second edition of the *Guideline for Implementing Cryptography in the Federal Government,* which was issued in November 1999. Written by Elaine B. Barker, William C. Barker, and Annabelle Lee, the revision updates and replaces the 1999 version of the guideline, and provides new tools and techniques for using cryptography to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. NIST SP 800-21-1 provides guidance on Federal Information Processing Standards and NIST Special Publications that have been issued, or amended, since 1999, and on cryptographic modules and algorithms that are validated for conformance to standards. The guideline assists federal organizations in selecting cryptographic controls and in implementing the controls on new or existing systems.

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

- NIST SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations,* by Dennis Branstad, Alicia Clay, and Joan Hash, assists federal agencies in assessing the reliability of organizations that provide PIV card issuing (PCI) services. HSPD 12 requires that all identity cards be issued by providers whose reliability has been established by an official accreditation process. Agencies must have accurate, reliable, and trustworthy information about their PCI in order to make appropriate decisions about whether to authorize its operation. Certification is the formal process for assessing that the PCI is reliable and capable of enrolling approved applicants and of issuing PIV cards. Accreditation is the official management decision to authorize the operation of a PCI after a thorough certification process has been conducted.

▪ NIST SP 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines (SP800-73 compliance)*, by Ramaswamy Chandramouli, Levent Eyuboglu, and Ketan Mehta, specifies the test plan, processes, derived test requirements, and the detailed test assertions and conformance tests needed for testing PIV middleware and the PIV card application for conformance with the specifications detailed in NIST SP 800-73. NIST SP 800-85 supports developers of PIV middleware and PIV card applications in the development and testing of their software modules, and it assists testing laboratories in developing appropriate test suites for the interface requirements in NIST SP 800-73. The guidelines for conformance testing help to advance the availability of validated, interoperable PIV products and the acquisition of these products by federal organizations.

▪ NIST SP 800-87, *Codes for the Identification of Federal and Federally Assisted Organizations,* by William C. Barker and Hildegard Ferraiolo, provides four-character identifying codes for federal organizations. These codes are used in the implementation of FIPS 201 to establish the Federal Agency Smart Card Credential Number (FASC-N), which is part of the Card Holder Unique Identifier (CHUID).

- NIST Interagency Report (NISTIR) 7284, *Personal Identity Verification Card Management Report,* by Jim Dray and David Corcoran, presents an overview of card management systems, and identifies generic card management requirements. Card management refers to the preparation of a smart card before it is issued, and the administrative functions that are related to the use of the card. The report provides some technical approaches to filling the existing gaps in PIV card management in order to achieve a higher level of consistency and testability for PIV card issuance processes, enhance an organization's ability to outsource various card management components and functions, and thereby improve the overall security for the Federal PIV framework.

Future Technical Support

As FIPS 201 is implemented and used, the procedures and technical specifications will be reviewed regularly and may be updated when necessary. NIST has identified additional guidelines, reference implementations, and conformance tests that will be needed to implement and use the PIV system; to protect the personal privacy of individuals using the PIV system; to authenticate identity source documents and obtain the correct legal name of the person applying for a PIV card; to obtain electronically and store required biometric data, such as fingerprints and facial images, from the PIV system applicant; to create a PIV card that is personalized with the data needed by the PIV system to later grant the individual access to federal facilities and information systems; to assure appropriate levels of security for federal applications; and to provide for interoperability among federal organizations using the standards. NIST will pursue these projects to the extent that its resources permit.

PIV Demonstration

In November 2005, NIST announced the Personal Identity Verification (PIV) Demonstration project and invited vendors with commercially available products to participate in the project and to join in a Cooperative Research and Development Agreement (CRADA) with NIST. Products that vendors submit to be included in the demonstration must be tested and validated in accordance with the NPIVP. The purpose of the project is to provide proof-of-concept demonstrations of commercially available products that support FIPS 201, Part 2. Additionally, the demonstrations will show the interoperability of NPIVP-certified PIV cards and PIV middleware. The demonstrations will be available to all federal agencies interested in FIPS 201 implementations. Information about these activities is available at the demonstration website http://csrc.nist.gov/piv-program/CRADA/index.html.

More Information about NPIVP

Information about the NPIVP, interim laboratories, and validation testing is available at http://csrc.nist.gov/npivp/.

The NPIVP director is Ramaswamy Chandramouli (Mouli); telephone: (301) 975-5013; fax: (301) 948-0279. Requests for general information or questions about the program may be sent by e-mail to the NPIVP Project Team at npivp@nist.gov.

FIPS 201 is available on the NIST website http://csrc.nist.gov/publications/fips/index.html.

NIST Special Publications are available on the NIST website http://csrc.nist.gov/publications/nistpubs/index.html.

NVLAP provides an unbiased third-party evaluation and recognition of performance, as well as expert technical guidance to upgrade laboratory performance. NVLAP accreditation signifies that a laboratory has demonstrated that it operates in accordance with NVLAP management and technical requirements pertaining to quality systems; personnel; accommodation and environment; test and calibration methods; equipment;

measurement traceability; sampling; handling of test and calibration items; and test and calibration reports. Information about NVLAP is available at http://csrc.nist.gov/npivp/.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.