August 2005

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

IMPLEMENTATION OF FIPS 201, PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS

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

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has several efforts underway to help federal agencies implement Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. The standard, which was approved by the Secretary of Commerce in February 2005, supports improved security for the forms of identification that are used to gain access to government facilities and information. Citing the need for better quality and security of the processes for identifying individuals, Homeland Security Presidential Directive (HSPD) 12, issued in August 2004, called for the development of a mandatory, government-wide standard for secure and reliable forms of identification for government employees and contractors.

FIPS 201 specifies technical and operational requirements for interoperable PIV systems that issue PIV cards as identification credentials and that use the cards to authenticate an individual's identity. Authentication of an individual's identity is an essential component of secure access control to facilities and to information systems. NIST recently developed supplementary guidelines and recommendations that support agencies in implementing the technical and administrative requirements of FIPS 201. Some of these publications are available in final form, and some are currently available as draft documents that will be finalized in the near future. To help agencies acquire PIV systems that correctly implement FIPS 201, NIST has started a conformance testing program for the standard.

Requirements for PIV Accreditation

In implementing FIPS 201, agencies must assure that the PIV cards which are issued are secure and reliable means of identification, and that the cards have been issued only by providers whose reliability has been established by an official accreditation process. This requirement for an accreditation process was included in HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. HSPD 12 affirmed the government's requirements for a common government-wide identification system to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The directive stated that secure and reliable forms of identification should be:

Continued on Page 2

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 June 2004:

- *Information Technology Security Services: How to Select, Implement, and Manage,* June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance for Selecting Secure Techniques*, August 2004
- *Information Security Within the System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA, November 2004*
- *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
- *Protecting Sensitive Information That is Transmitted Across Networks: NIST Guidance for Selecting and Using Transport Layer Security Implementations, July 2005*

- Based on sound criteria for verifying an individual's identity;
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Rapidly authenticated electronically; and
- Issued only by providers whose reliability has been established by an official accreditation process.

NIST developed Special Publication (SP) 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, by Dennis Branstad, Alicia Clay, and Joan Hash, to help agencies that are preparing to issue PIV cards. The guidelines describe how to conduct processes for assuring the reliability of the PIV card issuer (PCI). The PCI may be a federal organization or a contractor that works under the direction and authorization of a federal organization. The PCI must be authorized by the head of an agency or department to perform the services specified in FIPS 201 for identity proofing, for enrolling approved applicants in the PIV system, and for issuing PIV cards. Applicants for these cards may be employees, future employees, contractors, and guests. Each agency is expected to authorize at least one PCI, but agencies may wish to cooperatively establish a joint PCI. Large, dispersed organizations may establish several PCIs to provide needed services in the various geographic areas that are served.

To assure the reliability of the PCI, NIST recommends that agencies use certification and accreditation processes that have been employed to assess the security of information systems. These recommended processes have been detailed in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, by Ron Ross, Marianne Swanson, Gary Stoneburner, Stu Katzke, and Arnold Johnson, and in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, by Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, and Annabelle Lee. The certification and accreditation processes defined in NIST SP 800-37 and in NIST SP 800-53 should be used to accredit the information systems that are used by the PCI. In addition, NIST SP 800-79 outlines the processes that establish the reliability of the PCI to provide the needed PIV services.

NIST SP 800-79 and the other special publications mentioned in this bulletin are available on NIST's web pages:

http://csrc.nist.gov/publications/nistpubs/index.html

Links to information about the PIV program, including the standard, supporting documents, answers to frequently asked questions, and contact information are also available on NIST web pages:

http://csrc.nist.gov/piv-program/index.html

Certification and Accreditation Processes

NIST SP 800-79 describes the fundamentals of PCI certification and accreditation, including the roles and responsibilities of the key participants of the PCI and the agency that it supports, the types of accreditation decisions that can be made, and requirements for supporting documentation. The required and desired attributes of the PCI are explained, and methods are suggested for assessing the presence of the attributes. The major functions, services, and operations of PCIs are discussed. The appendices include a comprehensive list of references, a list of definitions, acronyms, summaries of tasks and subtasks to be carried out in the certification and accreditation processes, and sample accreditation transmittal and decision documents.

Agencies need complete, accurate, and trustworthy information about their PCI in order to make informed decisions about whether to accredit the PCI. Certification is the formal process for assessing the attributes of the PCI to verify that the PCI is reliable and capable of enrolling approved applicants and issuing PIV cards. Attributes include organization structure, policies, capabilities, facilities, and availability, and methods of assessment including interviews, document reviews, laboratory test results, procedure evaluations, and component validation reports. Accreditation of a PCI is the official management decision of a Designated Accreditation Authority (DAA) to authorize operation of a PCI after that official determines that the reliability of the PCI has been satisfactorily established through appropriate assessment and certification processes.

The recommended certification and accreditation processes are conducted in four phases:

In the **Initiation Phase,** responsible agency officials prepare for certification and accreditation by reviewing the PCI's operations plan and confirming that the plan is consistent with FIPS 201, and that the provided services and operations comply with the standard. The resources needed for certification and

accreditation are identified, and a schedule and milestones are established. The operations plan is analyzed and accepted.

In the **Certification Phase**, the agency officials determine whether services and specifications required by FIPS 201 are provided and whether they are implemented correctly and as intended. The officials also determine if the requirements of the agency are being met by the PCI. Needed actions are identified to correct any deficiencies that are noted in the operations of the PCI in order to minimize risks and mitigate vulnerabilities. When this phase is successfully completed, the DAA should have the information that is needed to recommend an appropriate accreditation decision.

In the **Accreditation Phase,** the DAA makes the decision whether to accredit the PCI and completes the accreditation documentation. After accreditation, the PCI is authorized to conduct the PCI services defined in its operations plan, or to conduct the PCI services on an interim basis under specific terms and conditions. Accreditation of the PCI could also be denied.

In the **Monitoring Phase**, agency officials oversee and monitor the operations of the PCI, and notify the DAA if there are changes that affect the reliability of the PIV systems or its components. The certification and accreditation processes should be conducted at least every three years.

Implementation of Technical Requirements

FIPS 201 incorporates three technical publications that specify interface and other technical requirements.

NIST SP 800-73, *Interfaces for Personal Identity Verification*, by James F. Dray, Scott B. Guthery, and Teresa Schwarzhoff, specifies interface requirements for retrieving and using identity credentials from the PIV card. It specifies the PIV data model, card interface requirements, and the Application Programming Interface. It designates requirements when the standards that are applied include options and branches. The goal is to assure that client application programs, compliant card applications, and compliant integrated circuit cards can be used interchangeably throughout federal agencies.

Two specifications are included in NIST SP 800-73. One is a transitional card specification that is derived from the Government Smart Card Interoperability Specification, which agencies with existing identity card systems may continue to use as an optional and intermediate step toward the government-wide uniformity and interoperability specifications. These interoperability specifications, designated as Part 2 card specifications in FIPS 201, are to be used by agencies that do not have an existing PIV system. The Part 2 specifications also may be used by those agencies that wish to make the transition to uniformity and interoperability specifications now. Part 2 provides details for the many components and processes that will support a smart-card-based platform, including the PIV card, and the card and biometric readers. The specifications for PIV components support interoperability between components in systems and enable the systems of different departments and agencies to work together.

Draft NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*, by Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli, helps federal agencies and implementers of PIV systems to apply the technical specifications for biometric data that are included in FIPS 201. This publication provides requirements for capturing and formatting fingerprint and facial images information. It is based on voluntary industry standards, and provides the proper selection when there are options in the standards that would interfere with interoperability if implemented in different ways. The goal is to ease implementation, facilitate interoperability, and assure the performance of PIV systems.

SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, by W. Timothy Polk, Donna F. Dodson, and William E. Burr, provides the technical specifications for the mandatory and optional cryptographic keys specified in FIPS 201. These specifications support the PIV card, the infrastructure components that manage the issuance and management of the PIV card, and applications that rely on credentials used by the PIV card to provide security services. The publication identifies symmetric and asymmetric encryption algorithms, digital signature algorithms, and message digest algorithms. Mechanisms are provided to identify the algorithms associated with PIV cards or digital signatures.

Other NIST Special Publications that support the implementation of the technical requirements of FIPS 201 include:

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.

Draft NIST SP 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines*, by Ramaswamy Chandramouli, Levent Eyuboglu, and Ketan Mehta, provides test plans, processes, and a test suite that can be used to verify the conformance of PIV components to the specifications contained in NIST SP 800-73. The conformance tests for the interoperability of PIV middleware and PIV card applications were developed to meet the overall interoperability goals of FIPS 201.

Draft NIST SP 800-87, *Codes for the Identification of Federal and Federally Assisted Organizations*, by William C. Barker and Hildegard Ferraiolo, provides the organizational codes that are necessary to establish the Federal Agency Smart Credential Number (FASC-N). This number is included in the Card Holder-Unique Identifier (CHUID), one of the specified requirements in FIPS 201. The CHUID identifies the individual within the PIV system.

Designation of NIST Personal Identity Verification Program (NPIVP) Test Facilities

Conformance tests are important to the correct implementation of FIPS 201. Since August 8, 2005, NIST has designated five organizations as interim NIST Personal Identity Verification Program (NPIVP) test facilities. The designated organizations include COACT, Inc. CAFÉ Laboratory, InfoGard Laboratories, Inc., DOMUS IT Security Laboratory, BKP Security Labs, and BT Cryptographic Module Testing Laboratory. These organizations may employ NIST-provided test suites to validate PIV components, subsystems, and integrated systems as required by FIPS 201 to meet the NPIVP requirements. Additional information regarding the laboratories is available at http://csrc.nist.gov/cryptval/. NIST expects to add other facilities to the list of NPIVP test facilities in the near future. During the next year, the designated laboratories will be assessed by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) for accreditation for PIV testing. Once NVLAP accreditation is achieved, the "Interim" designation will be removed. Testing under the NPIVP will begin with a limited scope of tests based on FIPS 201, but the scope of tests will be increased as the testing program moves forward.

Other Government Activities Supporting the Implementation of FIPS 201

In August, the Office of Management and Budget issued a Memorandum for the Heads of All Agencies and Departments (M-05-24), detailing the steps that should be taken to implement FIPS 201 and HSPD 12. The memorandum is available from the NIST web page http://csrc.nist.gov/piv-program/index.html. Some of the requirements include:

- Agencies and departments must adopt and accredit a registration process consistent with identify proofing, registration, and accreditation requirements of FIPS 201 for all new employees, contractors, and other applicable individuals. This process applying to the new identity credentials issued must be established by **October 27, 2005**. Background investigations, conducted as the National Agency Check with Written Inquiries (NACI), should be initiated before the issuance of credentials. All new contracts involving contractor access to federal facilities and information must include requirements for the application of FIPS 201 to contractor personnel.

- For all current employees, contractors, and other applicable individuals, agencies and departments must develop a plan and start the required background investigations. These activities also should be established by **October 27, 2005**.

- By **October 27, 2006**, agencies and department must begin deploying products and operational systems that are compliant with Parts 1 and 2 of FIPS 201 for all new employees and contractors. For current employees, agencies and departments must phase in the issuance and use of identity credentials that meet the standard by **October 27, 2007**. Agencies and departments also must implement the technical requirements of the standard in the areas of personal authentication, access controls, and card management. Card authentication mechanisms described in the standard should be used, and at least one digital certificate should be used on the identity credential for access control.

- The General Services Administration will develop acquisition services to enable agencies and departments to acquire products and services that are interoperable to help agencies that are preparing to issue PIV cards, and compliant with FIPS 201.

Future Needs

The efforts of agencies and department to implement FIPS 201 will help to improve the security of federal facilities and information systems, and will strengthen the trust in the credentials issued by all federal organizations to their employees and contractors. To enable continued effective implementation of the standard, NIST has identified other needed guidelines, reference implementations, and conformance tests:

- Additional guidance on implementing and using the PIV system;
- Methods for protecting the personal privacy of all subscribers of the PIV system;
- Methods for authenticating identity source documents to obtain the correct legal name of the person applying for a PIV card;
- Techniques for electronically obtaining and storing required biometric data such as fingerprints and facial images from the PIV system subscriber;
- Techniques for creating a PIV card that is personalized with data needed by the PIV system to later grant access to the subscriber to federal facilities and information systems;
- Ways to assure appropriate levels of security for all applicable federal applications; and
- Methods to provide for interoperability among federal organizations using the standard.

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.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900