March 2005

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS: FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 201 APPROVED BY THE SECRETARY OF COMMERCE

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

A new Federal Information Processing Standard (FIPS) for a government-wide personal identity verification (PIV) system was approved by Carlos M. Gutierrez, the U.S. Secretary of Commerce, on February 25, 2005. The system is based on the use of smart cards, which will be issued by all federal government departments and agencies to their employees and contractors who require access to federal facilities and information systems.

Homeland Security Presidential Directive (HSPD) 12, issued by President Bush on August 27, 2004, cited the wide variations in the quality and security of the forms of identification used to gain access to federal and other facilities, and called for the development of a mandatory standard for secure and reliable forms of identification to be used throughout the federal government. The directive stated the government's requirements for a common governmentwide identification system that would enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) developed the standard, working in conjunction with private industry and with other federal agencies, including the Office of Management and Budget (OMB), the Office of Science and Technology Policy, and the Departments of Defense, State, Justice, and Homeland Security.

How the Standard Was Developed

HSPD 12 stated that the secure and reliable forms of identification should be:

- 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, the Department of Commerce (DoC), and the Office of Management and Budget (OMB) held public meetings in October and November 2004 to discuss the technical and policy issues related to developing the needed standard. NIST drafted the FIPS and announced it in the *Federal Register* for public review and comment in November. NIST also issued drafts of two supporting technical documents in December. Another public meeting was held in January 2005 to address privacy and security issues that might affect individuals to whom PIV cards are issued. The comments received in the open forums and from more than 80 organizations and individuals during the formal review process were carefully considered and helped to shape the final standard. In addition, the Federal Identity Credentialing Committee and the Smart Card Interagency Advisory Board made many valuable contributions to the technical framework of the standard.

The standard does not apply to identification systems for national security systems and facilities.

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 December 2003

- *Security Considerations in the Information System Development Life Cycle*, December 2003
- *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 2004
- *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, March 2004
- *Selecting Information Technology Security Products*, April 2004
- *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 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

NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

Technical and Operational Requirements

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 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. In the past, hand-held credentials such as driver's licenses and badges have been used to control access to facilities, and passwords have been widely employed for access to information systems. More recently, cryptographic and biometric technologies have been employed to replace the older methods.

FIPS 201 has been issued in two parts to allow for a smooth migration to a secure, reliable personal identification process. 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 identity has been established and who have had a background investigation. Agencies must inspect at least two identity source documents submitted by an applicant for the PIV credential. At least one of the documents presented by the applicant must be a valid state- or federal government-issued picture identification (ID). Applicants for credentials must be examined through an Office of Personnel Management (OPM) background investigation process, the National Agency Check with Written Inquiries (NACI), to establish assurance of identity. While the National Agency Check has been a requirement for federal government employees since the 1950s, it may be a new requirement for some contractors. The initial phase of the NACI must be completed before the new ID card is issued. When the written inquiries part of the NACI is completed, the agency reviews the results and takes appropriate action if negative results are received. These are current practices for most agencies.

The PIV Card

HSPD 12 stated that the standard should include graduated criteria, from least secure to most secure, to give agencies flexibility in selecting the appropriate level of security for each application. Agencies will continue to have full flexibility in determining who is allowed to have access to their systems and facilities.

The PIV card is the primary component of the system. The size of a credit card, the PIV card will use cryptographic and biometric technologies to support the required graduated levels of security for agency applications. Cards will contain a Personal Identification Number (PIN); this is the data used to authenticate the cardholder to the card, as a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card. The card will also have a Cardholder Unique Identifier (CHUID), which identifies the individual within the PIV system. There will also be two electronic fingerprints, which will be securely stored and protected on integrated circuit chips. Public Key Infrastructure (PKI)-based cryptography will be used to protect the integrity of information that will be stored on the card.

No other personal information, such as Social Security number, address, or telephone number, is required by FIPS 201 to be stored on the card. The release of biometric information required to be stored on the card by FIPS 201 and use of the private key takes place only after the cardholder provides the correct PIN. Only the CHUID will be available through a wireless interface.

Fingerprints were chosen as the biometric information to be stored on the cards because fingerprints are the least invasive and most cost-effective, reliable, repeatable, and accurate means of verification available using public available technology. Two fingerprints will be stored on the cards. An electronic facial image is not required, but may be used. A printed photograph of the cardholder is required to be printed on the card for visual inspection and verification. Also the cardholder's name and the expiration date of the card will be printed on the card. Agencies may include other optional information such as their agency seals and the issue date of the card if they wish to do so.

PIV II Requirements

The second part (PIV II) of FIPS 201 explains the many components and processes that will support a smart-card-based platform, including the PIV card and card and biometric readers. The specifications for PIV components support interoperability between components in systems and among the different department and agency systems. An operational system contains three subsystems:

❑ PIV Front-End Subsystem – PIV card, card and biometric readers, and personal identification (PIN) input device.

❑ PIV Card Issuance and Management Subsystem – components responsible for identity proofing and registration, card and key issuance and management, and repositories and services such as the public key infrastructure (PKI directory).

❑ Access Control Subsystem – physical and logical access control systems, the protected resources, and the authorization data.

PIV II also describes a means to collect, store, and maintain information and documentation needed to authenticate and assure an individual's identity.

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/.

Schedule for Implementation of FIPS 201

By June 27, 2005, agencies must establish a program to ensure that the identification forms issued by their organizations meets the PIV standard. By August 27, 2005, they are required to identify any additional applications, beyond the scope of the standard, for which the standard should be used, and report them to the Assistant to the President for Homeland Security and to OMB.

By October 27, 2005, agencies must have procedures in place for verifying employees' identities and for issuing smart cards that meet the requirements of PIV I. To operate and maintain PIV systems, agencies will have to obtain the services of an accredited PIV card issuer, and adopt procedures for PIV card applicants to provide acceptable identity source documents. Agencies also will need to acquire services for capturing biometric information, as well as PIV card readers and PKI services.

With the October 27th implementation of PIV I by all federal agencies, there will be a basis for trust among agencies and for the mutual recognition of their employee and contractor credentials. PIV II, which will take longer to implement because of the many electronic credential systems now in place, focuses on the common technical interoperability requirements of HSPD 12. When this part is implemented, a card from one agency will be electronically recognized by any other agency so that a decision about granting access to the cardholder can be made.

NIST Supporting Activities

NIST is developing three key companion documents that will support the implementation of FIPS 201 by vendors and users. The first publication, *Interfaces for Personal Identity Verification,* to be issued as NIST Special Publication 800-73, will specify interface requirements for retrieving and using data from the PIV card. 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. 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 FIPS 201 PIV II card specification for agencies choosing to move directly to the PIV II target architecture.

The second publication, *Biometric Data Specification for Personal Identity Verification,* by Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli, will be issued as NIST Special Publication 800-76 and will specify technical acquisition and formatting requirements for the biometric credentials of the PIV system. Designed to ease agency implementation of FIPS 201 by facilitating interoperability and ensuring performance of PIV systems, the specification selects options from published biometric standards. It includes specifications for the fingerprints used in the PIV systems, facial image optional specifications, the format for all PIV biometric data representation, and the requirements for biometric devices.

The third publication, *Cryptographic Algorithms and Key Sizes*, will be issued as NIST Special Publication 800-78 and will specify cryptographic algorithms and key sizes that will be authorized for use in PIV systems in current and future time frames.

Draft versions of NIST Special Publications 800-73 and 800-76 have been made available for public review and comment. See the "For More Information" section below for details about accessing these two draft documents.

Insofar as its resources permit, NIST also plans to investigate other technical issues that will help support the use of the standard. Some of these requirements include: reference implementations and conformance tests to enable testing of implementations for conformance with the standard; measures to protect privacy of users of PIV systems; ways to authenticate identity source documents; and methods to incorporate data needed by different agencies while assuring appropriate levels of security and providing for interoperability among federal PIV systems.

Other Federal Agency Support Activities

OMB is responsible for overseeing agency implementation of HSPD 12 and will develop implementation guidance for federal agencies, including privacy and implementation guidelines to federal agencies. OMB will determine the timeline for agencies to comply with the second part of the standard.

The General Services Administration (GSA) is responsible for assisting agencies in procuring and operating PIV subsystems such as card and biometric readers. OPM is responsible for assisting agencies in authenticating and vetting applicants for the PIV card.

Protecting Privacy

Privacy is an issue of special concern and a basic obligation established by the presidential directive. The standard requires federal department and agencies to ensure the privacy of applicants for identity credentials. Some of the requirements include:

❑ Assigning an individual to the role of senior agency official for privacy;

- ❑ Conducting a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV;
- ❑ Writing, publishing, and maintaining a clear and comprehensive document listing the types of information that will be collected about individuals, the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency;
- ❑ Assuring that systems containing personal information adhere to fair information practices;
- ❑ Maintaining appeals procedures for those who are denied a credential or whose credentials are revoked;
- ❑ Auditing compliance of PIV systems with stated privacy policies and practices governing the collection, use, and distribution of information; and
- ❑ Limiting access for information in PIV systems to those persons with a legitimate need for the information.

FIPS 201 does not require that the federal government establish a central database to track movement of employees and contractors or the systems that they access. Personally identifiable information stored on the card is minimal, and the information stored on the PIV card, such as electronic fingerprints, will be protected since the cardholder must enter a PIN to release the information.

The technology on the card does not allow for tracking movement of contractors and employees while moving throughout a building. Because the information on the PIV card may be read by a wireless device, there has been some concern that data can be inadvertently or maliciously captured. To alleviate this concern, employees will be required to keep the card in an electronically opaque sleeve when not in use to minimize the risk of unauthorized reading of data from the card without the consent of the cardholder.

For More Information

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

Draft NIST Special Publications 800-73 and 800-76 are available on the NIST website http://csrc.nist.gov/publications/nistpubs/index.html.

The NIST website http://csrc.nist.gov/piv-project/index.html provides links to other information about the PIV project, including workshops held in 2004 and 2005, and HSPD 12. Also available on the web pages are answers to frequently asked questions about the PIV standard and contact information. The comments received by NIST concerning the draft FIPS 201 are also available.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply llrecommendation 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

Official Business
Penalty for Private Use $300
Address Service Requested