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

NISTIR 7337

Personal Identity Verification Demonstration Summary

Erika McCallister
Hildegard Ferraiolo

NISTIR 7337

Personal Identity Verification Demonstration Summary

Erika McCallister

Hildegard Ferraiolo

C O M P U T E R S E C U R I T Y

Information Technology Laboratory

National Institute of Standards and Technology

Gaithersburg, MD, 20899-8940

August 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William A. Jeffrey, Director

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This Interagency Report discusses ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report, 19 pages

(August 2006)

Acknowledgements

The authors, Erika McCallister and Hildegard Ferraiolo of the National Institute of Standards wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many contributions from the product developers and integrators for participation in the PIV demonstration project.

Table of Contents

List of Appendices

List of Figures

1. Introduction

On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 required the development and implementation of a government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by HSPD-12, the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standard 201 (FIPS 201). Subsequently, NIST issued a number of Special Publications in support of FIPS 201 to enable interoperable implementations. To ensure interoperability, NIST created a conformance test suite for Personal Identity Verification (PIV) card applications and middleware, which is being used by independent laboratories to conduct the conformance testing.

With the October 27, 2006, deadline for agencies to implement FIPS 201 fast approaching, NIST sought voluntary participation by companies offering products and services supporting FIPS 201 for the PIV Demonstration. The PIV Demonstration provided NIST the opportunity to conduct proof of concept and interoperability demonstrations of products supporting FIPS 201 and accompanying Special Publications. The demonstration resulted in a useful exchange of information among Federal agencies, vendors, and NIST.

2. Background

The PIV Demonstration took place from May 15 to June 14, 2006. Forty-four companies voluntarily participated through a Cooperative Research and Development Agreement (CRADA) with NIST. The purpose of the demonstration was to show proof of concept and interoperability demonstrations of commercially available products that support FIPS 201 and the accompanying special publications. Personnel from over 25 different Federal agencies and departments attended the PIV Demonstration.

The demonstration was divided into two phases. During the first phase, each company met with NIST representatives for 2-3 hours to demonstrate and to discuss their FIPS 201 product solution. This provided NIST with a unique opportunity to observe and discuss current product capabilities. The companies were provided the opportunity to ask questions of NIST and to provide general input to NIST about the PIV Program. During the second phase of the demonstration, Federal agencies and departments were invited to the NIST campus to attend the PIV Demonstration. Agency representatives were provided the opportunity to meet with technical representatives from each of the companies to observe demonstrations of FIPS 201 solutions and to ask questions relevant to each agency's implementation.

As part of the CRADA, companies were required to make their products available for use by NIST for the entire one month period of the PIV Demonstration. NIST used this opportunity to further study the product capabilities. As part of the interoperability aspect of the demonstration, NIST tried each of the issued cards in the various readers provided to observe interoperability among PIV components.

3. Summary

The PIV Demonstration focused on FIPS 201 components in the following categories:

+ PIV Cards
+ Enrollment and Identity Management System (IDMS)
+ Issuance, Management, and Printing
+ Contact Readers
+ Contactless Readers and Physical Access Control System (PACS)
+ Public Key Infrastructure (PKI)
+ Biometrics

The following subsections provide summaries of the products from each category. The summaries are based on vendor presentations, demonstration, and product specifications[1].

3.1 PIV Cards

Nine companies presented ten PIV cards for the demonstration. The companies included smart card manufacturers, PIV card application developers capable of working with a variety of smart cards, and integrators capable of issuing a variety of PIV cards. All ten of the cards were either in process for conformance testing or had completed testing. Half of the cards had completed the PIV card application conformance testing through NIST PIV Program (NPIVP), while the cards' cryptographic module validation for FIPS 140-2 compliance through the Cryptographic Validation Program (CMVP) is progressing as shown in figure 1:

[1] NIST makes no guarantees, expressed or implied, about the reliability of the statements from the companies. *The summary is for informational purposes only and does not represent an endorsement of any specific product, group or individual by NIST nor does it reflect the opinions or beliefs of NIST.* [1]

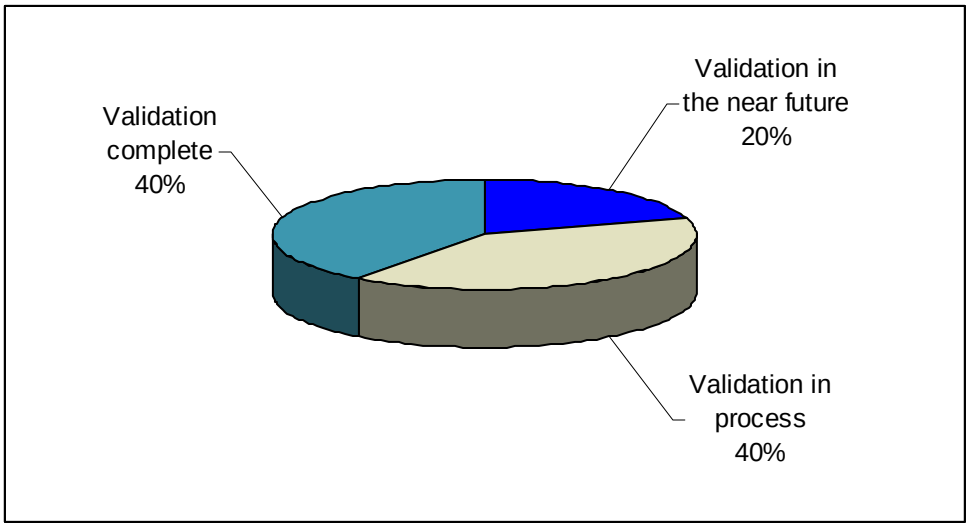

Figure 1: Status of Cryptographic module validation

Of the ten cards, twenty percent supported a transition interface, in addition to the endpoint interface specified in Special Publication 800-73 (SP 800-73), *Interfaces for Personal Identity Verification*. For the contact interface, sixty percent of the cards supported both transmission protocols T=0 and T=1, ten percent supported only T=1, and thirty percent of the cards supported only T=0. With respect to additional card interfaces, four cards claimed to have capabilities to support the 125 kHz interface. Four companies indicated that other types of interfaces could be added to the cards.

All of the cards supported the Rivest Shamir Adleman (RSA) algorithm, but the supported key lengths varied by company. Triple Data Encryption Standard (Triple-DES) was the most supported symmetric algorithm, and Advanced Encryption Standard (AES) was also common. Two companies supported elliptic curve cryptography (ECC) at the time of the demonstration.

Additionally, NIST learned of a possible issue with respect to the mapping of answer-to-reset (ATR) to the Cryptographic Service Provider (CSP) for Windows logon. The ATR of the PIV card is unspecified in the standard so it can vary among vendors. Therefore, if there are multiple CSPs on the Windows system, then the CSP could have problems connecting to the PIV card. A possible solution to avoid the problem is to set the PIV CSP as the default and registering other CSPs with specific ATRs.

3.2 Enrollment and IDMS

Fifteen companies provided products in this category. Some of the companies provided enrollment stations capable of sending data packages to other systems for management and issuance, while other companies provided a limited set of enrollment capabilities, such as the biometric capture. Several of the companies provided only IDMS functionality.

Eighty-seven percent of the systems were capable of recording the outcome of the National Agency Check with Inquiries (NACI). Of those capable systems, fifty-four percent recorded a binary indicator field, twenty-three percent stored the background investigation data, and fifteen percent were configurable.

Ninety-three percent of the systems were designed to enforce separation of duty, and the remaining seven percent indicated separation of duty enforcement would be a future capability.

For biometric capture products, ninety-three percent of the companies indicated their systems perform 10-fingerprint captures. Of those products, seventy-one percent provided automated feedback to the enrollment station operator about the image quality. Sixty-two percent of the systems checked the minutiae against the image, and fifteen percent stated that this check was a configurable feature.

In the IDMS product category, eighty-six percent of the products were capable of using their stored data to populate physical and logical access control systems as shown in figure 2:

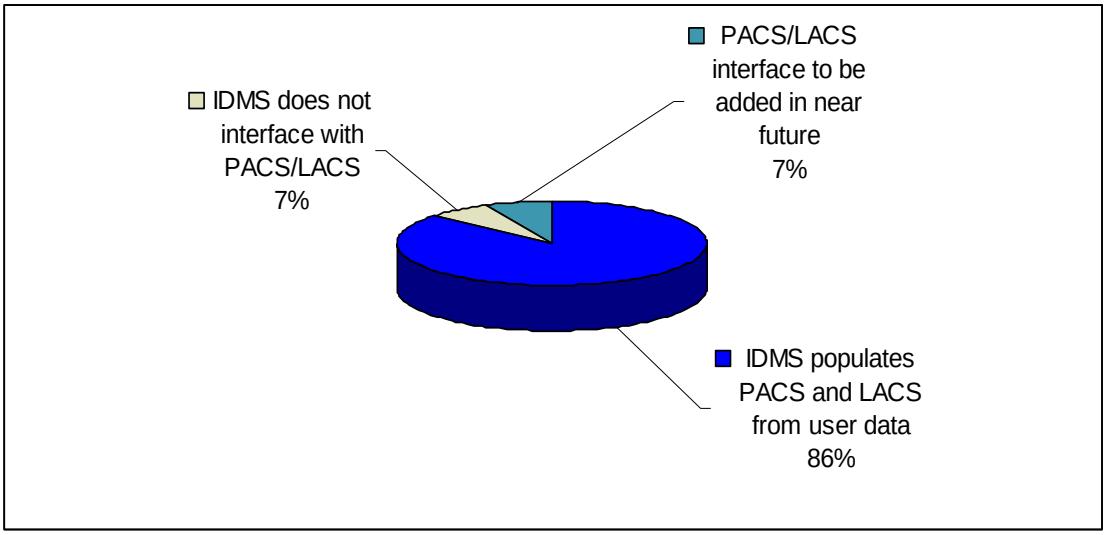

Figure 2: IDMS interface to PACS and LACS

3.3 Issuance, Management, and Printing

Seventeen of the companies provided products in this category. The products included card issuance and management systems and card printers. Some of the issuance and management systems worked with specific enrollment systems, while others accepted packaged data from a variety of enrollment systems.

All of the card printers met the basic requirements, such as not printing in reserved areas, not interfering with the Integrated Circuit Chip (ICC), and providing anti-tampering features. As illustrated in figure 3, the printer solutions capability to produce anti tampering and counterfeiting security features ranges from one to up to five different features.

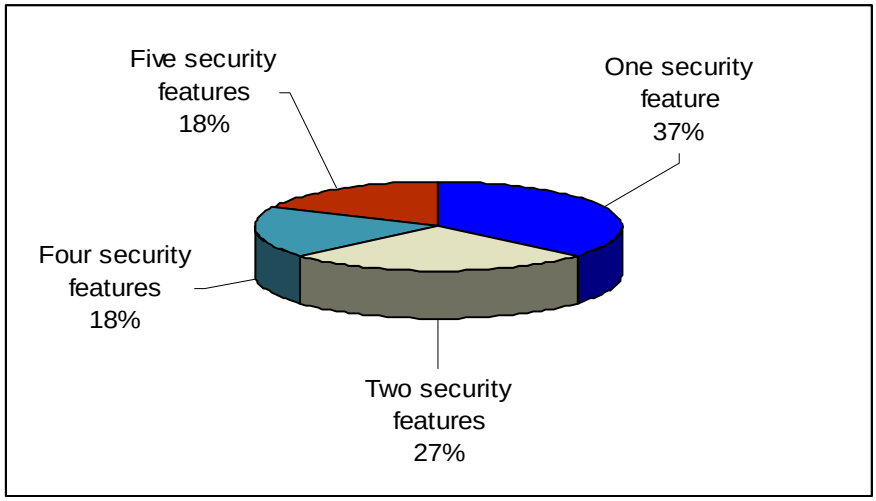

Figure 3: Number of implemented security features per printer

The implemented security features are a subset of the following anti tampering and counterfeiting measures:

+ Hologram
+ Microprinting
+ Lense Manufacturing
+ Laminate
+ Foil
+ UV Printing
+ Covert Marking
+ Mediametrix
+ OBD

All of the companies asserted that their printers placed an industry-accepted amount of stress on the cards during printing, which would not affect the functionality of the chips.

In the issuance and management category, all of the companies stated that their issued cards contained the mandatory data elements. Seventy-five percent indicated that their issued cards contained optional data elements, and seventeen percent pointed out that the optional data elements were configurable. For post-issuance updates, seventy-five percent of the companies indicated that their card management system performed a cryptographic challenge-response.

3.4 Contact Readers

Nine contact readers were provided by eight different companies. All companies asserted that their readers conform to the International Organization for Standardization (ISO) 7816 (ISO/IEC 7816).

Seventy-eight percent of the readers supported the Personal Computer / Smart Card (PC/SC). Of the readers connected to a PC, sixty percent claimed to be plug-n-play on the Windows platform.

3.5 Contactless Readers and PACS

Eighteen companies provided products in this category. The products included standalone contactless readers and integrated PACS. Ninety-four percent of the contactless readers conformed to ISO 14443 (ISO 14443). Of those 14443 readers, ninety-three percent supported both type A and type B communication signal interfaces. Seven percent supported only type A.

All of the companies asserted that their product could read the Cardholder Unique Identifier (CHUID). The contact readers and/or systems varied on which parts of the CHUID could be used after the initial read. Specifically, all indicated that the Federal Agency Smart Card Number (FASC-N) could be used, and some could additionally use the expiration date (figure 4) and Global Unique Identification Number (GUID).

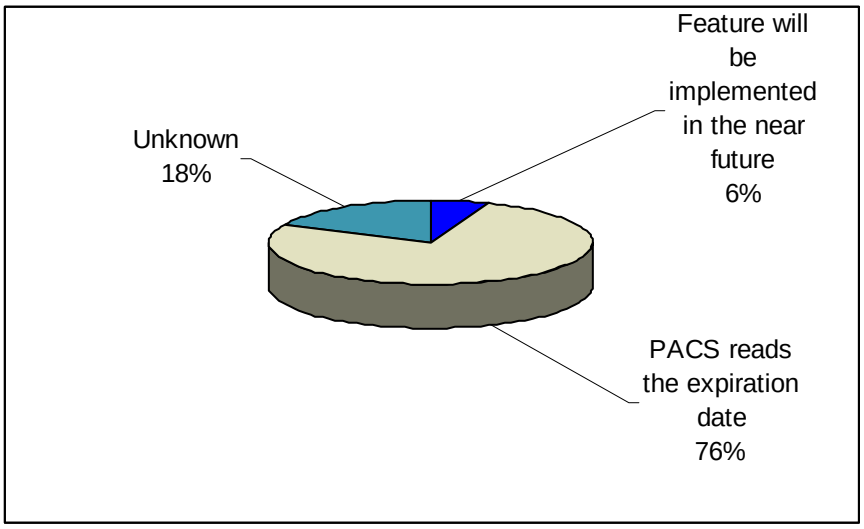

Figure 4: PACS capable of reading the expiration date from the CHUID

With respect to contact readers interfacing with the PACS, eighty-six percent included a Personal Identification Number (PIN) input component, and eighty-three percent were capable of biometric authentication. Moreover, fifty percent included PKI capabilities. These PACS were capable of verifying the signature on CHUID as well as perform the certificate status check.

Most companies indicated that their readers were flash-programmable.

3.6 PKI

Six of the companies provided PKI functionality. Most of these companies provided card issuance capabilities and partnered with a Certificate Authority (CA). Eighty percent indicated that their CA was part of the Federal Bridge, and the remaining twenty percent stated that joining their CA to the Federal Bridge was in their future plans. At the time of the demonstration, sixty-seven percent of the companies issued certificates following the Common Policy. Eighty-three percent indicated that the FASC-N was contained in the subject alternative name extension of the PIV Authentication X.509 certificate.

3.7 Biometrics

Twelve of the companies provided biometric capabilities. Some of the companies were providers of biometric technologies, whereas others licensed the technologies for use within their integrated solutions. All of the companies were using multi-finger scanners certified by the Federal Bureau of Investigation (FBI). These yield fingerprints for background checks required for PIV applicants. Seventy-three percent were using a minutiae template generator that was subjected to the Minutiae Interoperability Exchange Test (MINEX[2]) testing as illustrated in figure 5.

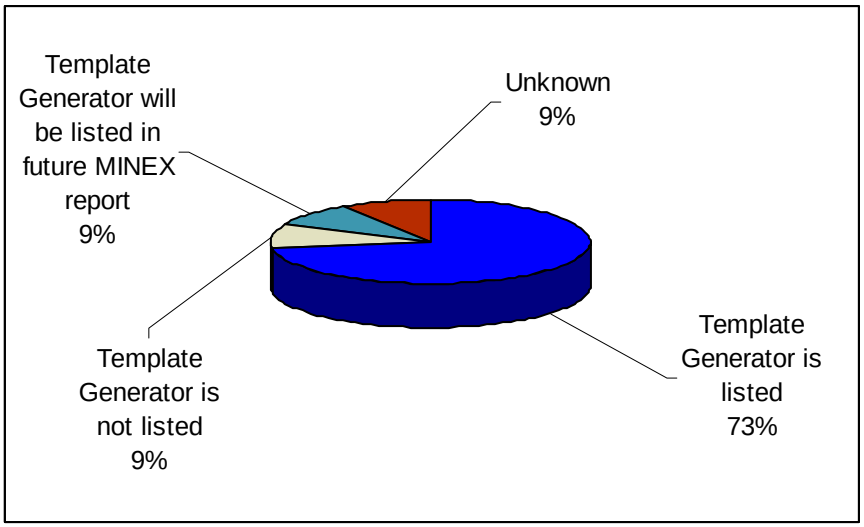

Figure 5: Minutiae Template Generators listed in the MINEX report

[2] The MINEX homepage http://fingerprint.nist.gov/minex04/ documents performance tests of interoperable fingerprint templates.

4. Conclusion

The PIV Demonstration successfully showed that based on vendor presentations, demonstration, and product specifications, current commercial products are available as FIPS 201 solutions to facilitate meeting HSPD-12 mandate for Federal Agencies. The demonstration enabled exchange of useful information between the participating companies and Federal agencies, which will aid agencies in their implementation of HSPD-12.

Appendix A—Vendor Participants

The following list identifies the companies that participated in the PIV Demonstration through the CRADA. This list does not represent an endorsement by NIST of the products or services offered by any of the companies. Additionally, NIST does not represent that the products or services offered by these companies are on the GSA Approved Products List (APL).

+ 3M
+ ACI Worldwide, Inc.
+ ActivIdentity
+ ADT
+ AMAG Technology
+ Aware, Inc.
+ BQT Solutions
+ BridgePoint Systems
+ Centech Group
+ Cogent Systems
+ ColorID
+ Condortech Services
+ Cross Match Technologies
+ EC4 Technologies
+ Entrust
+ Fargo Electronics
+ Giesecke & Devrient (G&D)
+ Gemplus Corporation
+ Hirsch Electronics
+ Honeywell
+ Identix
+ ImageWare Systems
+ Integrated Engineering

+ Intellisoft
+ Intercede
+ Lenel Systems
+ Lockheed Martin
+ MDI
+ Novell
+ Oberthur Card Systems
+ Probaris Technologies
+ Quintron Systems
+ RSA Security Inc.
+ Sagem Morpho
+ SCM Microsystems
+ Secure Network Systems
+ Software House
+ SETECS, Inc
+ StepNexus
+ TecSec
+ Ultra Electronics
+ Unisys
+ Viscount Systems
+ XTec

Appendix B—Acronyms

The following acronyms and abbreviations are used throughout this document:

AES	Advanced Encryption Standard
APL	Approved Products List
ATR	Answer to Reset
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CMVP	Cryptographic Module Validation Program
CRADA	Cooperative Research and Development Agreement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FBI	Federal Bureau of Investigation
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standards
GUID	Global Unique Identification Number
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Chip
ID	Identification
IDMS	Identity Management System
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
MINEX	Minutiae Interoperability Exchange Test
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NPIVP	NIST's Personal Identity Verification Program
OCSP	Online Certificate Status Protocol
PACS	Physical Access Control System
PC/SC	Personal Computer/Smart Card

PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFU	Reserved for Future Use
RSA	Rivest Shamir Adleman
SP	Special Publication

Appendix C—Bibliography

Citation Code	Document
FIPS 201	Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. (See http://csrc.nist.gov)
SP 800-73	NIST Special Publication 800-73, Interfaces for Personal Identity Verification, March 2006. (See http://csrc.nist.gov)
MINEX	Minutiae Interoperability Exchange Test. See http://fingerprint.nist.gov/minex04 and http://fingerprint.nist.gov/minex
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors. See http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html
ISO/IEC 7816	ISO/IEC 7816, Identification cards - Integrated circuit(s) cards with contacts
ISO/IEC 14443	ISO/IEC 14443, Identification cards - Contactless integrated circuit(s) cards - Proximity cards