FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems

A Smart Card Alliance Physical Access Council White Paper

Publication Date: September 2005

Publication Number: PAC-05001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, visit http://www.smartcardalliance.org.

TABLE OF CONTENTS

1 Introduction

This white paper provides an overview of the impact of the Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors,* and related specifications on Federal physical access control systems (PACS) and describes how the PIV card should be used in PACS throughout the Federal Government.

Historically, due to their purpose in the organization, logical and physical access control functions have been separate domains managed by different personnel implementing related but uncoordinated policies. As a result, the architecture, equipment, and identity verification requirements were independent and oriented toward their specific functional goals. The staff was trained and experienced in different security skills, with the PACS typically managed by security personnel and the logical access control system managed by the IT department.

Today, however, logical and physical access control systems are beginning to converge. Verifying the identity of individuals both within an organization and among different organizations has become critically important. Although the skill sets and technologies for logical and physical access are still specialized, requirements for uniform security policy enforcement and the adoption of new access control technologies are driving dramatic and necessary changes to integrate both functions and systems. A prime example is Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, which mandates the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 requires the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems. This policy is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

The convergence of logical and physical access control functions required by HSPD-12 benefits agencies in many ways. However, it also raises a unique set of challenges. In particular, combining physical and logical access on a single credential requires agencies to address issues that were handled by separate functional groups in the past.

HSPD-12 requires that the Federal credential (the PIV card) be secure and reliable, which is defined as a credential that:

- Is issued based on sound criteria for verifying an individual's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

The Department of Commerce and National Institute of Standards and Technology (NIST) were tasked with producing a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, on February 25, 2005. The FIPS 201 PIV card is to be used for both physical and logical access control, and other applications as determined by the individual agencies.

FIPS 201 consists of two parts: PIV I and PIV II. The standards in PIV I support the control objectives and security requirements described in HSPD-12. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II also specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal PIV system.

NIST has produced several additional publications that expand on the standards in PIV II[1]:

[1] All NIST publications can be found on the NIST PIV Program web site, http://csrc.nist.gov/piv-program/.

- NIST Special Publication 800-73 [SP 800-73], April 2005: *Interfaces for Personal Identity Verification*
- NIST Draft Special Publication 800-76 [SP 800-76], January 2005: *Biometric Data Specification for Personal Identity Verification*
- NIST Special Publication 800-78 [SP 800-78], April 2005: C*ryptographic Algorithms and Key Sizes for Personal identity Verification*
- NIST Special Publication 800-79 [SP 800-79], July 2005: *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*
- NIST Draft Special Publication 800-85 [SP 800-85], August 2005: *PIV Middleware and PIV Card Application Conformance Test Guidelines (SP 800-73 compliance)*
- NIST Draft Special Publication 800-87 [SP 800-87], August 2005: *Codes for the Identification of Federal and Federally-Assisted Organizations*

The documents referenced above are critical to implementing a FIPS 201-compliant PACS. In addition, the Physical Access Interagency Interoperability Working Group (PAIIWG) of the Government Smart Card Interagency Advisory Board (IAB) has published a document that is equally essential: *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2*, July 30, 2004 [PACS 2.2][2], which is currently being updated to version 2.3 to align it with the language in FIPS 201 and SP 800-73.

FIPS 201 alters the intrinsic approach taken by agencies to establish identity, perform credentialing, and protect access and will require new policies to be set both within an agency and across the entire Federal government. Other guidance that is critical for agencies implementing FIPS 201 includes:

- Office of Management and Budget Memorandum M-05-24 [OMB M-05-24], *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, issued on August 5, 2005.
- The General Services Administration (GSA) Memorandum: *Acquisitions of Products and Services for Implementation of HSPD-12*, issued on August 10, 2005.
- The GSA publication, *Federal Identity Management Handbook* (released as a public draft in March and July 2005)[3]. This document provides specific implementation direction on course of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

[2] Available at http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf.

[3] Available at http://www.cio.gov/ficc/.

2 Physical Access Control System (PACS) Requirements

A PACS has many benefits, foremost among which is the use of mature and proven technologies that can strengthen the trust relationship between an agency and an employee and enhance the security for personnel entering, leaving, or working within a building.

The following section summarizes the components and operation of a typical FIPS 201-compliant PACS. It should be noted that FIPS 201 does not mandate specific PACS mechanisms, but rather refers agencies to PACS 2.2.

2.1 Physical Access Control System Components and Operation

A typical FIPS 201-compliant PACS is composed of the following components:

- PIV card
- PIV card reader/keypad
- Biometric reader[4]
- Control panel
- Access control server
- Cardholder data repository
- Control points[5]

The PIV card stores a cardholder photograph, cryptographic keys, biometric data and the cardholder unique identifier (CHUID). (See section 3 for more details of the CHUID.) The card allows the identity of the cardholder to be verified. The card is presented to a card reader to initiate an authentication transaction and to request access authorization.

The card reader provides power to the card's interface and reads the electronically stored cardholder information from the card. This information may be the entire CHUID or portions thereof. Certain cardholder information may be read-protected and require a personal identification number (PIN) for read access. Once the data is read, the reader sends the information to the control panel.

The control panel is clock-synchronized and connected to the access control server, card reader/keypad, and control point hardware. The control panel receives the information from the card reader and compares it to data stored in its database. After the control panel determines that the data is valid, it compares the information to the access privileges in the local database registered to the cardholder and makes an access decision. This decision is based on criteria such as credential status, expiration date, day of the week, time of day, and control point location. The control panel sends the decision to the access control server to be displayed and logged. The door lock (or other control point) receives a signal from the control panel to unlock the door or inform the PIV cardholder and system that access has been denied. All successful and unsuccessful access attempts are typically logged by the PACS.

FIPS 201 assurance levels specify verification of the authenticity of both the card and the encoded data stored on the card. This is different and separate from verifying the authenticity of the person holding the credential. The assurance levels, titled *some confidence*, *high confidenc*e and *very high confidence*, represent different authentication processes. The process above describes the *some confidence* level.

[4] A biometric reader is optional, but is required for high or very high confidence levels.

[5] A control point is defined as any device that is controlled by a physical access system (for example, doors, turnstiles, gates, lights, cameras, elevators). There may be multiple control points for a single access requirement.

The FIPS 201 *high confidence* level requires biometric comparison of a fingerprint captured and encoded on the credential during the card-issuing process and a fingerprint scanned at the physical access point.[6] If the biometric data stored on the card is the fingerprint image, then this data is only accessible through the PIV card's contact interface. Image data is also PIN-protected and requires the individual to enter a PIN before the reader can access the data on the card. For PACS implementations that use biometric templates (instead of images) stored on the PIV card or in an agency-specific data repository, agencies can set their own policies for biometric access. (See section 3.2 for additional information on the use of biometrics with the PIV card.)

The *very high confidence* level requires that the process described above is completed at a control point attended by an official observer. In addition, site-specific asymmetric keys in both the card and reader are required to authenticate the encoded data. Agency-specific PKI keys are verified after the PIN is entered and before any further data exchange occurs between the credential and reader. (For a more detailed description of assurance levels, see section 5.)

FIPS 201 also specifies a provision for an expiration date. However, agencies may achieve compliance with this aspect of FIPS 201 according to their own security policies.

The access control server is an administrative tool used to register and enroll a cardholder's name, access privileges, and expiration date in the cardholder data repository. The cardholder data repository manages PIV cardholder physical access privileges. The server downloads the CHUID (or portion thereof), access level, and authorized functions to the access control panel. It also allows a system operator to temporarily assign a credential and access privileges to visitors or employees who forgot or misplaced their cards. Other data, such as a control point description (e.g., "Door 412, Communication equipment room") is entered and displayed to the system operator. The server maintains an active history (log) file of all events that occur in the PACS.

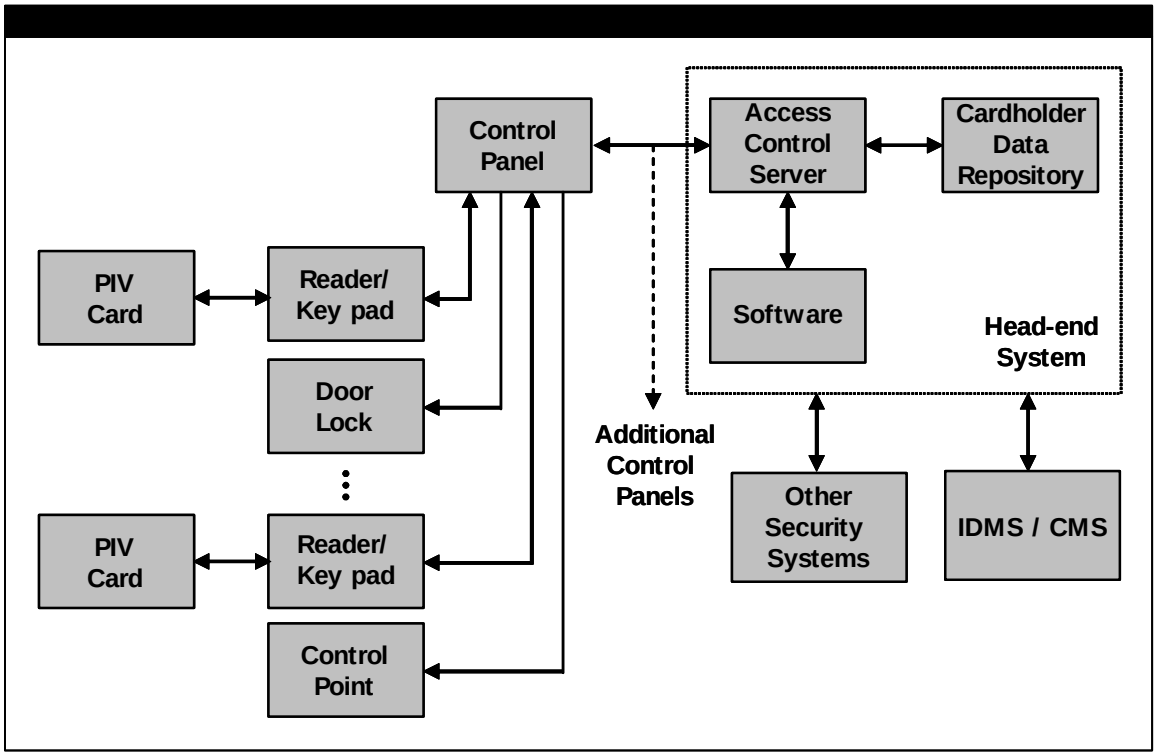
The access control server can also be used as a situation awareness tool. Different manufacturers offer different PACS features. Some systems integrate functions such as event-triggered closed-circuit TV (CCTV) cameras and video recordings. In these systems attempts at unauthorized entry would activate CCTV cameras for real-time assessment. Some systems can display the cardholder's digitally stored photograph on an operator console when the card is presented to selected readers. This allows an operator to compare the live person using the credential with a photograph of the cardholder recorded at the time of issuance. The operator, often a guard, can then manually provide access through a control point for the individual.

Revocation or temporary suspension of physical access privileges can be triggered by the local PACS, by a central identity management system (IDMS) database, by the card management system (CMS), by a system operator, or by an automatic event such as an expired card. Whatever the trigger, processes that update and synchronize credential status in affected databases and systems must be in place to ensure that PIV card status is accurate and valid. A more detailed discussion about revocation processes and the potential approaches an agency can use for implementation can be found in section 6.3.

Figure 2-1 illustrates a typical PACS.

[6] It is important to note that there is currently no final decision as to how the biometric data is to be formatted when stored on the PIV card. OMB has issued guidance that agencies may defer storing biometric data on the PIV card until NIST SP 800-76, Biometric Data Specification, is finalized.

Figure 2-1: Physical Access Control System Schematic



2.2 FIPS 201 PIV Card Requirements

Essential to the understanding of a FIPS 201-compliant PACS is an understanding of the basic card used to request physical access. The PIV card is the physical artifact issued to an individual that allows the claimed identity of the cardholder to be verified.

FIPS 201 requires that the PIV card be a smart card. The card body is similar to a bank credit card and conforms to the ISO/IEC 7810 specification. The card must contain both contact and contactless interfaces, which may be provided by two separate integrated circuit chips (ICC) or by one dual-interface ICC. The contact interface must conform to the ISO/IEC 7816 specification, and the contactless interface must conform to the ISO/IEC 14443 specification. In most cases, physical access applications will use the contactless interface, although there are special cases in which the contact interface will be used for such applications.

3 PIV Card Data: Cardholder Unique Identifier (CHUID)

One of the critical requirements of a FIPS 201 PACS application is the use of a standardized data model for cardholder identification data. This data model, represented by the cardholder unique identifier (CHUID), was first defined by PACS 2.2 and subsequently expanded in NIST SP 800-73. NIST SP 800-73 adds to the CHUID a field for expiration date.

The CHUID must be written to the FIPS 201-compliant card chip or chips and be available from both the contact and contactless interfaces. All of the CHUID elements must contain values. The reason for including all of this information in the CHUID is to identify each card uniquely within the Federal government. It is expected that the access control panel will therefore need to be able to use 14 digits, at a minimum, of the Federal Agency Smart Credential Number (FASC-N), a field within the CHUID. In the future, the requirement that each card be uniquely identified may make it necessary to migrate from use of the FASC-N to the global unique identifier (GUID).[7]

The FASC-N will be the main identifier used by a PACS and is a 25-byte data element composed of different fields. The FASC-N is likely to be much larger than identification numbers currently used in many legacy Federal access control systems. As a result, agencies may have to retrofit or install new readers to accommodate the larger number. In addition, access control system providers may need to modify their hardware and software to use the FASC-N.

While the FIPS 201 standard and related documents explain the methodology for transactions between the card and reader, they do not specify how the reader and the access control panel should communicate. This is to allow for an easier transition to FIPS 201 compliance by legacy access control systems and also allow for future bidirectional communications capabilities (e.g., IP-based readers).

Table 3-1 describes the data elements within the CHUID[8].

Table 3-1: CHUID Data Model Definition[9]

Data Element (TLV)	Tag	Type	Max. Bytes[10]
Federal Agency Smart Credential Number (FASC-N)	0x30	Fixed text	25
Agency code (optional)	0x31	Fixed text	4
Organization identifier (optional)	0x32	Fixed text	4
DUNS (optional)	0x33	Fixed text	9
Global unique identifier (GUID)	0x34	Fixed numeric	16
Expiration date	0x35	Date (YYYYMMDD)	8
Authentication key map (optional)	0x3D	Variable	512
Issuer asymmetric signature	0x3E	Variable	2816
Error detection code	0xFE	LRC	1[11]

[7] NIST Special Publication 800-73 (SP 800-73), April 2005: *Interfaces for Personal Identity Verification.* The Global Unique Identifier (GUID) field must be present, and may include either an issuer-assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials.

[8] The CHUID is defined as 0x3000, always read.

[9] Sources: *Technical Implementation Guidance: Physical Access Control Systems, Versions 2.2 and 2.3 [PACS 2.2 and PACS 2.3];* NIST Special Publication 800-73: *Interfaces for Personal Identity Verification*.

[10] The number of bytes listed for each data element is provided as maximum number of bytes. For example, a 4-digit agency code will never take up more than 4 bytes, but it may be stored in 2 bytes if encoded as 4 bits per digit. The data in the FASC-N (described in Figure 3-1 and Table 3-2) requires over 32 digits, but is stored in just 25 bytes due to the encoding technique employed.

[11] PACS 2.2 and 2.3

3.1 FASC-N Data

The FASC-N is the successor to the SEIWG-012 numbering scheme that was previously used by some Federal PACS. Use of the FASC-N is the key to incorporating credibility, non-repudiation, and reciprocity into a standardized Federal identification numbering system.

The FASC-N is a unique number assigned to one PIV card and individual only. Figure 3-1 illustrates the fields that compose the FASC-N and Table 3-2 describes the content of each field in the FASC-N.

Figure 3-1: FASC-N Fields

SS	**AGENCY CODE**	FS	**SYSTEM CODE**	FS	**CREDENTIAL NUMBER**	FS	**CS**	FS	**ICI**	FS	**PI**	**OC**	**OI**	**POA**	ES	LRC

SS = Start Sentinel
FS = Field Separator
ES = End Sentinel
LRC = Longitudinal Redundancy Check – a means of detecting bit errors in the reading process.

Table 3-2: FASC-N Field Descriptions

Field	Length	Description
Agency Code	4 digits	Identifies the government agency issuing the credential. This assumes an all-numeric code. If an alphanumeric format is used, the value of the organizational identifier field is set to 1 and the agency code is extracted from the agency code data element in the CHUID, not from the FASC-N.
System Code	4 digits	Identifies the system in which the card is enrolled and is unique for each site.
Credential Number	6 digits	Encoded by the issuing agency. For any particular system, no duplicate numbers are active.
Credential Series (CS) (series code)	1 digit	Available to reflect major system changes.
Individual Credential Issue (ICI)	1 digit	Initially encoded as a "1," this will be incremented if a card is replaced due to loss or damage.
Person Identifier (PI)	10 digits	Numeric code that can be used by the issuer/agency to uniquely identify the person.
Organizational Category (OC)	1 digit	Possible values are: 1 = Federal government agency 2 = State government agency 3 = Commercial enterprise 4 = Foreign government
Organizational Identifier (OI)	4 digits	Coded as If OC=1, Agency code[12] If OC=2, State code If OC=3, Company code If OC=4, Numeric country code

[12] In early 2005, NIST withdrew FIPS 95-2, which standardized agency codes, but has since released its replacement, Draft NIST Special Publication 800-87 (SP800-87): *Codes for the Identification of Federal and Federally-Assisted Organizations*, August 9, 2005.

Field	Length	Description
Person/Organization Association Category (POA)	1 digit	Possible values are 1 = Employee 2 = Civil 3 = Executive staff 4 = Uniformed service 5 – Contractor 6 = Organizational affiliate 7 = Organizational beneficiary

3.2 Required Biometric Data

Draft NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, is referenced in FIPS 201 and currently states that, at a minimum, two compressed fingerprint images must be stored on the PIV smart card contact chip. At this writing, a final decision has not been reached as to whether the fingerprint data will be in a compressed image form, template form, or both formats. The fingerprint data is required to support interoperability (use of the card for authentication between different Federal agencies and departments). FIPS 201 states that the required fingerprint data can only be accessed through the contact interface on the card and only after the card has been "activated" with a PIN. Privacy is the underlying reason for requiring PIN activation and should be kept in mind in designing and implementing biometric alternatives.

Since all 10 fingerprints must be collected for the FBI National Criminal History Fingerprint Check (in association with the FIPS 201 identity proofing process), it is recommended that at least the two index fingerprint images be retained so that an agency has the flexibility of generating either two fingerprint images, two fingerprint templates, or both for storage on the PIV card, subject to the final decision on the required format.

3.2.1 Issues Raised by Biometric Data Requirements

NIST SP 800-76 currently specifies the use of fingerprint images rather than templates, because there is no current test data that proves the interoperability of standards-based fingerprint templates. When using fingerprint images, agencies should carefully consider their throughput and performance requirements before implementing biometric authentication in their physical access control system's operational environment. Because of the size of compressed fingerprint images, the data transfer rates of smart cards and readers, and the additional processing steps needed to manipulate fingerprint images, agencies may find that the resulting authentication process exceeds the expected elapsed time for physical access transactions. Employee wait times might be unacceptable for physical access control applications that require rapid authentication, for example, during shift changes or at high throughput access points. Other applications, such as authenticating a visiting employee from another agency or department may be less sensitive to wait times.

The storage of two fingerprint images may also require a larger capacity smart card. This could present cost and commercial availability issues that should be carefully considered.

3.2.2 Other Biometric Considerations

Given the performance concerns raised above, agencies may want to consider the use of alternative biometric data representations and methods for those physical access control environments that require rapid authentication. Today's commercial physical access control products that support fingerprints for user authentication typically use templates of the biometric data (algorithmic or mathematical models of the data) rather than the fingerprint image data itself. These stored templates are efficient because they are only a fraction of the size of the

compressed fingerprint image data and require no additional preprocessing for matching purposes. A single fingerprint template can be as small as 200–500 bytes, while a single compressed fingerprint image is 7–12 Kbytes. While the fingerprint images may be required to support interoperability between agencies and departments, an organization is free to choose to use alternative biometric implementations to achieve more efficient internal operations.

FIPS 201 allows for other information, such as biometric templates, to be stored on the PIV card chip or chips and accessed through both the contact and contactless interfaces, but provides no additional information on this topic. Therefore, the storage of biometric templates on the PIV card must be considered an allowable but non-interoperable application.

In addition, FIPS 201 does not prohibit using the PIV card and CHUID to act as a pointer to biometric templates stored in a local database. This permits an agency or department to not only consider using more efficient fingerprint templates on the card, but also off-card template storage and alternative types of biometrics (other than fingerprints). For example, biometrics such as iris recognition, face recognition or hand geometry could be used in addition to fingerprints for physical access control. Hand geometry might be appropriate for use at facility entry portals that are directly exposed to the weather. In addition, there may be environments where employees may be required to wear protective gloves that make fingerprints impractical. In such circumstances, iris or face recognition might be an appropriate alternative biometric technology to use. Such biometrics could only be used to support the agency's PACS, not to support interoperability between agencies.

In summary, it appears to be acceptable for an agency or local facility to incorporate biometric templates on the contact or contactless portion of a card or in a local database. The incorporation of such templates would not affect the data that comprises the CHUID and therefore would not affect the interoperability of the card. Such templates would simply represent an additional application stored on or outside of the card. If an agency chooses to use fingerprint templates, it is highly recommended that these templates conform to the INCITS 378-2004 Finger Minutiae for Data Interchange Format standard[13].

Agencies also have the option of implementing biometrics using on-card matching. On-card matching is often viewed as enhancing security and privacy by eliminating the need to transfer the cardholder's stored biometric information off the card to other devices or systems for matching. On-card matching also eliminates the need for administering a separate off-card database of biometric templates.

If biometric templates are to be stored on the card, agencies need to decide whether the biometric data should be written to the card during the card issuance process or after card issuance. For added security, the data should be written to the card and digitally signed when the card is issued.

[13] A .pdf version of INCITS 378-2004 *Finger Minutiae for Data Interchange Format* can be ordered from the INCITS web site at http://www.incits.org/standards.htm.

4 Physical Access Rights and Privileges

Physical access rights and privileges at a Federal government facility for an individual PIV cardholder are defined by the local PACS manager. The local PACS manager grants access privileges to a PIV cardholder by registering/enrolling the PIV card's CHUID data (e.g., FASC-N, GUID, expiration date) in the local PACS. The cardholder can then access areas controlled by that PACS as authorized by that cardholder's registered access level. Access to highly sensitive areas may require the use of multiple identification elements as determined by the organization's policies and assurance level requirements. Combinations of a card and PIN, biometric checks, and/or digitally signed challenges may be required. All of these parameters are registered, processed, and verified by the local PACS.

Possession of a FIPS 201-compliant PIV card does not automatically permit the cardholder to access any Federal government facility that is FIPS 201 compliant. A cardholder must be enrolled in the PACS for every facility to which the cardholder needs access. Each agency will have to create policies that govern how to accept and authenticate cardholders who require access to an agency's facilities but who are not enrolled in that agency's home system. For example, a cardholder may have to see the security officer at the receiving agency's facility, at which time the card can be checked for authenticity. The cardholder can be asked to provide biometric verification (a live image to be compared to the image stored on the card), and the validity of the credentials can be checked. If all is in order and the visitor has legitimate reasons for being on site (a local sponsor, for example), then the PIV card CHUID data can be added to the local PACS.

The right to access a facility through a specific control point or group of control points can be controlled locally or remotely. Remote control requires multiple facilities to be linked using an enterprise-level access control system that shares information in a common database or IDMS. Agency policies will determine the requirements for management of physical access rights and privileges. Access privileges can be denied using different methods ranging from suspension to, in extreme circumstances, PIV card and associated certificate(s) revocation. Denial of physical access privileges may be managed from a local PACS, from the agency's central database and/or IDMS, or through checks against a certificate revocation list (CRL) or on-line certificate status protocol (OCSP) responder.

System processes that update and synchronize PIV card status in affected databases are essential to maintaining accurate PIV card status information. In addition to CRLs and OCSPs, a PIV card hotlist could be maintained that includes some or all revoked or terminated PIV cards. This hotlist could be made accessible online or could be distributed on a scheduled basis (e.g., hourly, daily). For added security, the hotlist could be digitally signed by its issuer/maintainer. Additional information on revocation processes can be found in section 6.3.

5 PACS Assurance Levels

FIPS 201 uses assurance terminology drawn from OMB Memorandum M-04-04 [OMB 404], *E-Authentication Guidance for Federal Agencies* and NIST Special Publication 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*. Both OMB 404 and FIPS 201 discuss assurance in terms of an agency's degree of certainty that the cardholder has presented a credential that references that cardholder's identity. "Assurance" means the following:

- The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued.
- The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.[14]

Since a PACS interacts with an issued credential, only the second part of the definition is relevant to physical access control operations.

5.1 Assurance Level Terminology

The assurance terminology in FIPS 201 is different than the terminology that became common with the publication of PACS 2.2. Table 5-1 summarizes the terminology used in the two documents. Appendix A discusses these differences in detail, as well as differences with OMB 404.

Table 5-1: Correlation of PACS 2.2 and FIPS 201 Assurance Levels

PACS 2.2 Assurance Level	FIPS 201 Assurance Level
Low	Some confidence
Medium	Some confidence
High (without PIN)	Some confidence
High (with PIN)	Very high confidence

5.2 Assurance Levels and Authentication

FIPS 201 and the associated documents define three types of authentication, which can take place in different combinations:

- Cardholder verification (HolderV). The person presenting the PIV card is verified through some mechanism (such as a PIN or biometric).
- Card verification (CardV). The PIV card is not counterfeit, and it has not been tampered with.
- Credential verification (CredV). The information on the PIV card has not been altered.

According to FIPS 201, HolderV by itself is only sufficient to provide some confidence. CredV by itself is also only sufficient to provide some confidence. It is critical that agency staff responsible for defining their agency FIPS 201 migration plan have an understanding of how PACS 2.2 relates to FIPS 201 assurance levels.

The PACS 2.2 Low Assurance Profile does not require any authentication of the card, cardholder, or credential. The card reader simply performs a free read of the CHUID and passes data to the panel for validation of the presumed cardholder's access rights. The PACS uses data such as FASC-N or GUID with the CHUID expiration date to match the presumed cardholder to records within the access control database. This process is very basic and not very secure. The data from the card could be skimmed or sniffed through covert means and copied onto a counterfeit

[14] See NIST SP 800-79: *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.*

card. The Low Assurance Profile neither protects data from being changed on the card nor provides any indication that such a change has taken place.

The PACS 2.2 Medium Assurance Profile requires that the system check to ensure that none of the information within the CHUID has been modified since the card was issued (CredV). The card reader obtains specified information from the CHUID and the card unique identifier (chip serial number). A site-specific encryption algorithm within the reader computes a hashed message authentication code (HMAC). This HMAC, along with the FASC-N, is passed to the access control panel to grant or refuse access. In most cases, the HMAC would be compared with the HMAC stored in the system at the time of enrollment. It can also be computed at the time of the transaction between the card and reader. If anyone changed the data within the CHUID after enrollment, the calculated HMAC would not match the originally encoded information registered and stored in the access control system, and access would be refused.

The PACS 2.2 High Assurance Profile requires symmetric or asymmetric encryption keys in both the card and the reader. It is highly recommended that each card have a unique diversified key if symmetric keys are used. The card is capable of storing multiple cryptographic keys in the authentication key map. The card reader for an agency would read this "key table," find the entry for its key, and then use the key to authenticate the card and the data on the card.

To support interoperability between agencies using the High Assurance Profile, it is important to coordinate the generation and storage of encryption keys so that keys from each agency are stored on the card during issuance. In a high assurance environment, keys would typically be generated on the card. As an alternative, agencies will need the ability to encode new encryption keys after cards are issued. Department/agency policy is required to determine which approach to take.

Appendix A includes additional detail on FIPS 201 assurance levels and PIV card authentication mechanisms.

6 PIV Card Life Cycle

The following discussion describes three major phases in the PIV card life cycle to assist agencies in understanding some of the broader implementation requirements:

- Identity proofing and registration of the individual applying for a PIV card
- Enrollment in local physical access control systems
- PIV card revocation

6.1 Identity Proofing and Registration

Meeting the control objectives for secure and reliable identification specified in HSPD-12 PIV I requires agencies to:

- Perform identity proofing
- Perform identity binding
- Determine identity trustworthiness
- Register identity with access privileges

6.1.1 Identity Proofing Background

The FIPS 201 identity-proofing process constitutes a standard policy that Federal agencies must follow when they provide official government identification to the following categories of employees:

- New employees, contractors, and affiliates
- Current employees
- Foreign service nationals (i.e., citizens of foreign countries who are working for the Federal government overseas)

Following the policy consistently helps ensure that cardholders are who they claim to be. Adherence to a uniform identity-proofing process that includes a threat/risk assessment (in accordance with HSPD-11[15]) for all employees and contractors across the Federal government provides a basis for trust among agencies. HSPD-12 and FIPS 201 require Federal agencies to comply with the PIV I standard for identity proofing by October 2005.

Note that compliance with the PIV I identity proofing requirements does not necessitate issuance of a PIV II compliant card. Where feasible, however, it is highly recommended that agencies strive to adopt technologies that fast track them toward a PIV II compliant card as early as possible. PIV II compliance will require that all new PIV cards conform to the technical and interoperability specifications for smart cards and related products found in NIST SP 800-73 and SP 800-76.

Included in OMB M-05-24 is the schedule for agencies and departments to comply with FIPS 201 requirements. Table 6-1 summarizes the actions and OMB timeline.

[15] Homeland Security Presidential Directive/HSPD-11: *Comprehensive Terrorist-Related Screening Procedures*, August 27, 2004

Table 6-1: Agency Actions for FIPS 201 Compliance[16]

Date	Agency Action
6/27/05	Implementation plans submitted to OMB
8/26/05	Provide list of other potential uses of the Standard
10/27/05	Comply with FIPS 201, Part 1
10/27/06	Begin compliance with FIPS 201, Part 2
10/27/07	Verify and/or complete background investigations for all current employees and contractors
10/27/08	Complete background investigations for all Federal department or agency employees employed over 15 years

Verifying an individual's identity is the first step. FIPS 201 mandates processes and provides guidance on both the source documents required to validate an individual's identity and the process for issuing a Federal PIV card, as well as the PIV credential itself.

6.1.2 Identity-Proofing and Registration Requirements

FIPS 201 and the GSA draft *Federal Identity Management Handbook* provide detailed information about identity-proofing, registration, and card issuance requirements.

The general requirements for PIV identity proofing and registration are as follows:

1. Agencies must use an approved identity-proofing and registration process.
2. The process must begin with the initiation of a National Agency Check with Inquiries (NACI) or another Office of Personnel Management (OPM) or National Security investigation required for Federal employment. For current employees, this requirement may be satisfied if a completed and successfully adjudicated NACI is on file for the employee.
3. Before a PIV credential is issued, a National Agency Check (NAC) should be completed and properly adjudicated.
4. The applicant must appear at least once in person in front of a PIV official before a credential can be issued.
5. During identity proofing, the applicant must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in I-9, OMB No. 1115-0136, *Employment Eligibility*. One of the documents must be a valid (unexpired) picture ID issued by a state government or the Federal government.

The PIV identity-proofing, registration, and issuance process must adhere to the principle of separation of roles. No single individual shall have the power to issue a PIV credential without the cooperation of another authorized person.

6.1.3 Temporary Access and Access-Pending Authorization

According to OMB Memorandum M-05-24, before issuing a PIV card to a new employee or contractor, agencies should receive notification of results of the National Agency Checks. If

[16] *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB Memorandum M-05-24, August 5, 2005

agencies do not receive the results in 5 days, the PIV card can be issued based on the FBI National Criminal History Check (fingerprint check).[17]

Employees may require access to buildings and systems pending the completion of their NAC. Also, certain individuals (such as individuals who fill vending machines) do not require a PIV card but do need access to facilities. Individual agency policies for temporary visitor access should be applied in both of these situations. Although it is the responsibility of each agency to design its temporary badges, as a best practice it is recommended that agencies design temporary and visitor badges that are unique and not similar to an official PIV card. This practice eliminates the possibility of mistaking temporary and visitor badges for valid PIV cards. The exact specifications for a PIV card can be found in Section 4.1 of the *Federal Identity Management Handbook*.

6.1.4 Agency Affiliates and Agency Partners

Many agencies have affiliates or partners who require physical access to do their jobs and who are not employees or contractors. For example, an affiliate or partner might be a visiting professor, guest faculty member, fellowship recipient, intern, temporary help, or a task force member. Each agency must determine whether these individuals require PIV cards. If so, then all identity-proofing and issuance requirements in FIPS 201 must be met. When affiliates or partners do not require a PIV card, agencies are encouraged to implement agency-specific visitor policies for these individuals. Agencies must be careful not to develop policies that overlap or contradict the FIPS 201 processes for identity proofing and credential issuance.

6.1.5 Identity Source Documents

Applicants are required to provide two forms of identification when applying for a PIV card.[18]

Acceptable forms of identification are also listed in I-9, OMB No. 1115-0136, *Employment Eligibility*. According to FIPS 201, applicants must also provide a completed SF 85, *Questionnaire for Non-Sensitive Positions*, or equivalent.

6.1.6 Notifications and Document Management

Agencies should develop a workflow for the identity-proofing process that includes notification when each step of the process is completed (for example, notification that a credential can be issued). The workflow should:

- Be secure
- Be auditable
- Protect the applicant's privacy

It is the responsibility of the PIV registrar and the IDMS to maintain the following documentation:

- Completed and signed PIV request
- Completed and signed SF 85 (or equivalent)
- Information related to the applicant's identity source documents
- Results of the applicant's background check
- Copies of an applicant's photograph and fingerprints
- Any additional documents used to prove the identity of the applicant

[17] OMB Memorandum M-05-24
[18] Acceptable forms of identification can be found at: http://uscis.gov/graphics/formsfee/forms/files/i-9.pdf.

6.1.7 Background Checks

Background checks in the form of a NACI/NAC[19] are required for employees and contractors to receive a PIV card. At a minimum, before a PIV card can be issued, a NAC has to be completed and adjudicated. The results of the NACI/NAC should be kept either electronically or in physical form while the individual is employed. Agencies should store the NACI/NAC in a secure location (logical or physical).

For PACS implementation, it is important to note that the CHUID data model in SP 800-73 is in the process of being modified by NIST to include a NAC/NACI status element. This is being done to comply with guidance included in OMB Memorandum M-05-24, which states: "Identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable (i.e., information is stored in the data on the card) from identity credentials issued to individuals who have a completed investigation." At the time of this writing, this has not been completed and the post-issuance process for updating the CHUID has not been determined.

6.1.8 Considerations for PIV I Implementation

Table 6.2 lists some implementation considerations, highlighting issues that may arise when working through the model to achieve PIV I compliance.

Table 6.2: PIV I Identity Proofing Considerations

Requirements	Considerations
Enrollment	• Scan documents for records retention. Verify scanned documents using electronic means to determine that they're valid and not counterfeit. • Capture a full set of 10 fingerprint images electronically using a multi-finger imaging platen reader device that records flat (or slap) images with no rolling movement required. • Design standard forms for the PIV application process if not using the system-based model (as required beyond SF 85). • Sign off approval forms if not using the system-based model. • Define enrollment agent role and process. Determine who is qualified (e.g., security officer, human resources), what training is needed and what function runs the process (e.g., human resources, security, CIO). This is analogous to FBI training for fingerprints. • Develop a non-confrontational enrollment policy. • Determine the enrollment auditing process.
Approval Process Requirements	• Designate signature authority. • Identify required turnaround times. • Develop adjudication procedures/processes to be used during identity vetting. For example, what should be done for individuals with questionable or false identities or with validated identities but who have NAC/NACI issues?
Issuance Requirements	• Determine if centralized or decentralized card printing/personalization will be used. • Develop materials-handling security requirements for card stock. • Define activation policies.

[19] An example NACI and NAC can be found at: http://www.opm.gov/extra/investigate/IS-15.pdf.

Requirements	Considerations
Revocation Requirements	• Develop the policies and procedures for revocation (e.g., staleness). • Determine how local physical and logical access control systems will be integrated with revocation mechanisms.
Cross-Agency Interoperability Requirements	• Determine who defines the policies and procedures for interoperability with other agencies. • Determine what servers must be installed. • Determine what messaging transactions must be supported.
Maintenance/Life Cycle Requirements	• Determine how to handle changes in status during the life cycle of the PIV card (e.g., expiration, renewals, privilege changes).

6.2 PACS Enrollment and Privilege Granting

An individual's PIV card must be enrolled in an agency's PACS before the individual can use the card for access. Agencies and departments will have different implementation approaches to PIV card enrollment, depending on their security requirements, their PACS, and their use of credential data. Different approaches can be taken in a variety of areas, ranging from how cards are enrolled and registered for physical access privileges to what data is entered in the PACS server database, to what data is used at the control points (e.g., doors, gates).

For example, one department may require data to be "pushed down" from the central identity management system to the PACS server's user database, with pre-registration for physical access privileges. Another agency may simply need to know that the new PIV card will work in the current system, while a third agency may want simply to read the serial number of the PIV card.

All of these implementations reflect different realities and unique agency perspectives. The only requirement common to all implementations is that they include the capability to remove and revoke registered access privileges centrally, should a person move or leave the organization. Manufacturers will therefore face a wide variety of implementation and operational requests.

In general, enrollment into a PACS requires the following activities:

1. Cardholder demographic data must be entered into the PACS as required by the local security manager.
2. The CHUID or a portion thereof must be entered into the PACS.
3. The PIV chain of trust must be validated to the level required by the agency.
4. Access privileges must be assigned.

Each of these activities can be accomplished in different ways, depending upon factors such as the following:

1. Was the PIV card issued by the organization that owns the PACS?
2. Was the PACS used as part of the PIV issuance process, or was issuance done as part of a separate IDMS?
3. Was the PIV card issued by a different agency or department?
4. What are the data input/output/sharing capabilities of the specific PACS?

For enrollment within an agency, the necessary demographics and PIV card information can be entered into the PACS by either pushing the information from the agency's IDMS to the PACS at

time the PIV card is issued, or by the PACS pulling the information from the IDMS when the individual presents himself to the security manager for assignment of access privileges following card issuance. The data could also exist in the PACS prior to issuance, if the PACS is used as a front-end for card issuance.

For cardholders from outside the agency (visitors), the local security manager could receive the needed data in advance of the visit by e-mail and then import it into the PACS or read it directly from the PIV card when the person arrives. As an alternative, visitors could upload the information themselves through a secure web site, using their PIV card PKI certifications for validation. In any case, the individual and the card are validated and local access privileges are assigned. The level to which the chain of trust for a card is validated is determined by the security and risk policies for a particular agency and a specific facility.

The data types and communications protocols necessary to perform validation between agencies for "visitor" PIV cards are still undefined. The minimum demographics and authentication data elements needed to ensure the HSPD-12 control objective, that the PIV be "rapidly verifiable electronically," would seem to be the CHUID and PKI certification, but these elements still need to be defined to ensure both system interoperability and mutual trust in the verification process.

6.3 PIV Card Revocation

Reliance on a trusted PIV card in a physical access setting requires that the applicant for a PIV card satisfactorily complete identity proofing and background checks prior to card issuance. Issuance includes vetting processes against the issuer's records and external data sources before a card is created and incorporated into the agency's database and/or IDMS. Continued trust in the PIV card requires that the issuing agency support the card's validity by distributing or providing access to pertinent status change information.

It is important for agencies to recognize the difference between revoking a PIV card and denying privileges. The PIV card is intended to establish trusted identity authentication across Federal agencies. Privilege denial simply halts an otherwise permitted activity. Privilege management lies outside of the scope of HSPD-12 and agencies have wide latitude in establishing the policies and methods for granting or denying access. Revocation of a PIV card means that the card is no longer valid and should not be used for identity authentication of a Federal government employee or contractor.

The PIV card standards require specific data for use in authentication. The standards allow agencies to add additional data (attributes) for use in determining access privileges. It is important for PACS to recognize and distinguish identity data used for authentication from other attributes used to determine privileges. This attribute information enables other interested organizations to evaluate whether certain attribute changes affect the granting of privileges to the identity (CHUID) recorded on the PIV card.

For example, deleting, changing or revoking an attribute pertaining to the person's job assignment may prevent the cardholder from accessing a particular IT application but not deny local physical access. Revocation of a CHUID or authentication certificate, however, will halt authentication processing in a typical PACS, preventing physical access. In certain situations it may be desirable to deny a privilege without revoking the PIV card.

6.3.1 Revocation Implementation Issues

A cardholder, agency or department initiates revocation processes if the PIV card has been compromised, lost, stolen, or damaged, if the cardholder no longer needs access to Federal buildings or IT networks, if employee status or attribute (e.g., name) changes or if any condition occurs that meets a policy criteria requiring revocation. It is up to the agency to define how the local PACS system obtains information about revocation. Four potential approaches are provided below:

- The PACS manager could maintain a directory of PIV card authentication certificates (contained on the contact chip of each PIV card) that are active in the PACS and perform a regularly scheduled (e.g., hourly, daily) check against a certificate revocation list (CRL) or on-line certificate status protocol (OCSP) responder. If a PIV card authentication certificate is revoked, then the access privileges of the associated PIV cardholder should be revoked. This process could be automated.
- A direct link could be established between an agency's IDMS and the PACS. Once a card is revoked, a message could be sent from the IDMS to the PACS flagging the revoked card. The PACS would then deny access based on the agency security policies for the PACS.
- An agency's IDMS could send a list of revoked PIV card serial numbers to the PACS manager's workstation. The implementation of this revocation list would be agency-specific. The security manager would be responsible for updating the PACS access control lists with information from the revocation list.
- The PACS manager could go to a web portal populated by an agency's IDMS and download an updated list of revoked PIV cards.

Any of these options may be used, depending on the need or preference of the agency or facility. For added security, the lists and messages mentioned above could be digitally signed and the digital signatures could be verified and validated against a CRL or OCSP responder. There is no requirement that each access point triggers a credential status request, as long as the PACS is updated according to agency-specific FIPS 201-compliant procedures (like the examples described above).

Upon revocation, FIPS 201 recommends that the old PIV card, if available, be collected and destroyed. If the card cannot be collected, normal operational procedures should complete within 18 hours of notification. In some cases where 18 hours is an unacceptable delay, previously defined emergency procedures must be executed to disseminate this information as rapidly as possible.

6.3.2 PIV Card Termination

The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. The PIV card should be terminated under the following circumstances:

- An employee separates (voluntarily or involuntarily) from Federal service.
- An employee separates (voluntarily or involuntarily) from a Federal contractor.
- A contractor changes positions and no longer needs access to Federal buildings or systems.
- A PIV cardholder is determined to hold a fraudulent identity.
- A PIV cardholder passes away.

Similar to the situation in which the card or a credential is revoked, normal termination procedures must be in place to ensure that the PIV card is collected, destroyed and revoked and that revocation information is made available to those systems that need to be informed.

7 Acquisition Process

OMB[20] requires that all departments and agencies acquire only products and services that are approved to be compliant with the standard (FIPS 201 and associated specifications) and included on the approved products list. A forthcoming Federal Acquisition Regulation (FAR) will require the use of only approved products and services.

GSA has been designated as the "executive agent for Government-wide acquisitions of information technology" under section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. § 11302(e)) for the products and services required by the Directive. GSA will report to OMB annually on the activities undertaken as an executive agent.

To ensure standard compliant products and services are available, NIST is issuing test suites in SP 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines (SP800-73 Compliance)*, and will publish National Voluntary Laboratory Accreditation Program (NVLAP) accredited validation services for demonstrating conformance for products. Providers of products and services that are determined to conform to the standard will be eligible to offer approved products and services on a new GSA procurement vehicle, which will be established to align all agency acquisitions with policy.

GSA[21] will make federally approved products and services (as described above) available that are compliant with FIPS 201 and associated specifications to agencies as they become available. In the interim, GSA recommends that agencies that have not begun deployment of smart cards as identity badges for employees and contractors should not begin or make procurements until End Point products, as defined in NIST Special Publication 800-73, are available. End Point products employ a unified card edge interface that is technology-independent and compliant with current international standards. Full technical specifications for these products can be found in SP 800-73.

GSA also recommends that agencies that have initiated a large-scale deployment of smart cards as identity badges prior to July 2005 may acquire Transitional products and services, also defined in NIST Special Publication 800-73, as part of a migration strategy. In so doing, these agencies should weigh benefits and costs of such a strategy over moving directly to an End Point smart card.

OMB acquisition guidance was issued before finalization of NIST Special Publication 800-76: *Biometric Data Specifications for Personal Identity Verification*, and allows agencies to defer the capture of biometrics for the identity credential until NIST guidance on biometrics is finalized.

The acquisition process described above is current as of the date of this publication. Additional up-to-date information on the status of FIPS 201 implementation can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org.

[20] OMB Memorandum M-05-24

[21] GSA Memorandum, *Acquisitions of Products and Services for Implementation of HSPD-12*, August 10, 2005

8 Conclusions and Observations

FIPS 201 and the associated NIST special publications were developed to provide additional guidance for implementing the HSPD-12 requirements for a common Federal identification credential that is to be used to access both physical and logical facilities and information systems. These standards and specifications signal a momentous change in how the Federal government manages physical access control and information security. While FIPS 201 and its associated special publications define many aspects for an interoperable Federal identity card, the standard also provides a variety of options for implementation and permits individual agencies to define their own approaches to meeting agency-specific access requirements.

As of the publication date of this white paper, many of the questions about PIV card implementation have been addressed by NIST special publications and by OMB and GSA guidance. However, work is still being done in the following key areas:

- **Biometrics**. The format for prescribed fingerprint data is still undecided. If the decision is made to store interoperable fingerprint templates on the PIV card, these templates would provide an appropriate interoperable biometric technology to use for rapid authentication in a PACS. It is important to remember that Federal agencies and departments are not precluded from implementing any alternative biometric data formats and modalities that may be required for their unique physical access control operations and do not need to be interoperable with other agencies.
- **CHUID definition**. Work is ongoing on the CHUID definition. Key open items include use of the expiration date, additional data elements that may be required (e.g., NAC/NACI status), GUID issuance and use, and replacement of FIPS 95-2 with SP 800-87. Agency PACS implementations may be affected by any changes to the CHUID definition.
- **Post-issuance updates**. Work is still being done to define the policies for updating PIV cards after the cards are issued. Key issues include policies for writing data to the contactless interface and for writing data to a PIV card issued by a different agency. Agencies will also need to be aware of the requirements for FIPS 201 and FIPS 140 re-certification if any applets are added post-issuance.
- **Revocation processes**. A variety of approaches can be taken to implement PIV card revocation depending on the capabilities of an agency's PACS. How revocation is to be handled across multiple agency systems is a major consideration during implementation.
- **Acquisition process**. Both OMB and GSA have issued initial memoranda outlining the acquisition process, with guidance to agencies about the use of End Point and Transitional products and services.
- **End Point vs. Transitional products.** Agencies need to be aware of whether they are using End Point or Transitional card systems when they implement their PACS to ensure that the system meets their needs. Card and reader vendors are now making Transitional products available and are working toward End Point products as End Point system specifications are finalized. Physical access control system vendors have also begun the process of implementing FIPS 201, focusing on Transitional smart cards. As FIPS 201 End Point cards are better defined and other specification ambiguities are resolved, PACS vendors will move to meet the requirements of End Point cards.

The impact of FIPS 201 is not restricted to the Federal government. State and local governments are being encouraged to adopt the provisions of FIPS 201, and businesses that provide goods and services to the Federal government will find that a substantial segment of their workforce will need to be credentialed. While this paper focuses on the impact of FIPS 201 on government, the private sector is also leaning toward the use of similar technologies and controls. Over the past 2 years, large leading-edge enterprises such as Boeing, Microsoft, Sun Microsystems and Johnson & Johnson have been migrating toward the use of smart cards for both physical and logical

access control authentication. Other enterprises have watched their progress carefully and are now planning their own implementations.

FIPS 201 and other initiatives that are being implemented to improve identity authentication are driving a paradigm shift for government agencies, businesses and smart card and PACS product and service providers. This shift is forcing a convergence of physical and logical access, requiring the adoption of new processes and technologies and forcing organizations to rethink their approach to managing access and authentication. It is critically important for industry and customers to work together to develop and implement standards-based solutions that address the new market realities and facilitate this transition.

The migration of the Federal government to FIPS 201-compliant PACS, the move by industry to combine physical and logical access systems, and the work on supporting standards are all ongoing efforts. To support the industry, the Smart Card Alliance Physical Access Council has created a resource on the Smart Card Alliance web site that maintains up-to-date information about the status of FIPS 201 and provides information that is relevant to both government agencies and other enterprises implementing new PACS.[22] The Physical Access Council recommends that organizations implementing new physical and logical access systems follow the industry activities closely and use this Alliance resource as they select new systems.

[22] See http://www.smartcardalliance.org/about_alliance/councils_pa.cfm.

9 References and Resources

Acquisitions of Products and Services for Implementation of HSPD-12, General Services Administration (GSA) memorandum, August 10, 2005 (available at http://www.cio.gov/ficc/documents/GSAacquisitionHSPD12.pdf)

E-Authentication Guidance to Federal Agencies, OMB Memorandum M-04-04, December 16, 2003 (available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf)

Federal Identity Credentialing Interagency Advisory Board (IAB) web site, http://www.smart.gov/IAB

Federal Identity Management Handbook (Draft), GSA publication, July 2005. (available at http://www.smartcardalliance.org/pdf/industry_info/FedIdentityMgmtHandbook_July_2005.pdf)

Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors,* NIST, February 25, 2005 (available at http://www.smartcardalliance.org/pdf/industry_info/FIPS_201_022505.pdf)

General Services Administration smart card web site, http://www.smart.gov/whats_new.cfm

GSA Memorandum: *Acquisitions of Products and Services for Implementation of HSPD-12*, August 10, 2005 (available at link to http://www.cio.gov/ficc/documents/GSAacquisitionHSPD12.pdf)

Homeland Security Presidential Directive/HSPD-11: *Comprehensive Terrorist-Related Screening Procedures*, August 27, 2004 (available at http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html)

Homeland Security Presidential Directive/HSPD-12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004 (available at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html)

"Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," Office of Management and Budget Memorandum M-05-24, August 5, 2005 (available at to http://csrc.nist.gov/piv-program/memo/m05-24.pdf)

INCITS web site, http://www.incits.org/standards.htm

International Biometric Industry Association (IBIA) web site, http://www.ibia.org

NIST PIV Program web site, http://csrc.nist.gov/piv-program/

NIST Special Publication 800-63 (SP 800-63), June 2004: *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology* (available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf)

NIST Special Publication 800-73 (SP 800-73), April 2005: *Interfaces for Personal Identity Verification* (available at http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf)

NIST Special Publication 800-73 Supplemental Information: *Namespace Management for Personal Identity Verification (PIV) Applications and Data Objects*, May 17, 2005 (available at http://csrc.nist.gov/piv-program/fips201-support-docs/Namespace-Management-PIV-Data-Objects.pdf)

NIST Draft Special Publication 800-76 (SP 800-76), January 2005: *Biometric Data Specification for Personal Identity Verification* (available at http://csrc.nist.gov/piv-program/fips201-support-docs/SP800-76-Draft.pdf)

NIST Special Publication 800-78 (SP 800-78), April 2005: C*ryptographic Algorithms and Key Sizes for Personal identity Verification* (available at http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf)

NIST Special Publication 800-79 (SP 800-79), July 2005: *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations* (available at http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf)

NIST Draft Special Publication 800-85 (SP 800-85), August 2005: *PIV Middleware and PIV Card Application Conformance Test Guidelines (SP 800-73 compliance)* (available at http://csrc.nist.gov/publications/drafts/800-85/draft-SP800-85.pdf)

NIST Draft Special Publication 800-87 (SP 800-87), August 2005: *Codes for the Identification of Federal and Federally-Assisted Organizations* (available at http://csrc.nist.gov/publications/drafts/Draft-SP800-87.pdf)

Office of Management and Budget (OMB) Federal Identity Credentialing Committee web site, http://www.cio.gov/ficc

Open Security Exchange web site, http://www.opensecurityexchange.org

Security Industry Association (SIA), http://www.siaonline.org

Smart Card Alliance web site, http://www.smartcardalliance.org

Smart Card Alliance Physical Access Council FIPS 201 resources, http://www.smartcardalliance.org/about_alliance/councils_pa.cfm

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2, Physical Access Interagency Interoperability Working Group (PAIIWG) of the Interagency Advisory Board (IAB), July 30, 2004 (PACS 2.2) (available at http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf)

X.509 Certificate and CRL Profile for the Common Policy, Version 1.1, July 8, 2004 (available at http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf)

10 Publication Acknowledgements

This report was developed by the Smart Card Alliance Physical Access Council to provide an overview of how FIPS 201 affects government physical access control systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Physical Access Council members for their contributions. Participants from 36 organizations were involved in the development of this report including: ADT Federal Systems, AMAG Technology, Anteon, Booz Allen Hamilton, Competech Smart Card Solutions, Condortech Services, Inc., CoreStreet, Ltd., EDS, Fargo Electronics, GTSI Corp., HID Corporation, HIRSCH Electronics Corporation, IBM, Identity Alliance, Identification Technology Partners, Inc. (IDTP), Indala, InfoGard, Integrated Engineering, International Biometric Industry Association (IBIA), LEGIC Identsystems, Lenel Systems International, Inc., Lockheed Martin, MAXIMUS, MDI, NASA, Northrop Grumman Corporation, Oberthur Card Systems, Precise Biometrics, SAFLINK Corporation, SAIC, SCM Microsystems, Shane-Gelling Company, SPAWAR, Tyco Safety Products, U.S. Department of Homeland Security (DHS), XTec, Inc.

Special thanks go to the individuals who wrote, reviewed and edited this report.

John Attala, InfoGard
Tom Baker, IDTP
Kirk Brafford, SAFLINK Corp.
Tom Caddy, InfoGard
Tom Casey, DHS
Salvatore D'Agostino, CoreStreet, Ltd.
Dave Engberg, CoreStreet, Ltd.
Paul Evans, Booz Allen Hamilton
Bob Fee, LEGIC Identsystems
Ken Gregory, Precise Biometrics
Walter Hamilton, IBIA/SAFLINK Corp.
Steve Hopper, InfoGard
Steve Howard, IDTP
Nick Ingerto, Anteon
Russ Kent, EDS
Gary Klinefelter, Fargo Electronics
Kevin Kozlowski, XTec, Inc.
Lolie Kull, DHS
Eric Larsen, Lenel
Mark McGovern, Lockheed Martin
John McKeon, IBM
Cathy Medich, Smart Card Alliance
Bob Merkert, SCM Microsystems
Mike Miley, SAIC
Ram Mohan, GTSI Corp.
LJ Neve, MAXIMUS
Dwayne Pfeiffer, Northrop Grumman Corp.
JC Raynon, SCM Microsystems
Steve Rogers, Integrated Engineering
Jim St. Pierre, MDI
John Schiefer, XTec, Inc.
Adam Shane, AMAG Technology
Dale Shane, Shane-Gelling Company
Jeffrey Stephens, EDS
Lars Suneborn, HIRSCH Electronics
Radu Tenenbaum, Tyco Safety Products
Greg Thornton, Competech Smart Card Solutions
Jim Valentine, Anteon
Eric Widlitz, HID Corp.

About the Smart Card Alliance Physical Access Council

The Physical Access Council is one of several Smart Card Alliance Technology and Industry Councils, a new type of focused group within the overall structure of the Alliance. These councils have been created to foster increased industry collaboration within a specified industry or market segment and produce tangible results, speeding smart card adoption and industry growth.

The Physical Access Council is focused on accelerating the widespread acceptance, usage, and application of smart card technology for physical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the physical access industry and that will address key issues that end user organizations have in deploying new physical access system technology.

The Physical Access Council is managed by a combined government/industry steering committee. Current steering committee members are:

Tim Baldridge, NASA
Craig Diffie, Axalto
Jeremy Grant, MAXIMUS
Lolie Kull, U.S. Department of Homeland Security
Bob Merkert, SCM Microsystems & Council Chair
Dwayne Pfeiffer, Northrop Grumman Corporation & Council Vice Chair
Joe Pilozzi, Philips Semiconductors
Steve Rogers, Integrated Engineering & Council Secretary
Adam Shane, AMAG Technology

The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software and reader vendors; physical access control systems vendors; and integration service providers. Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

11 Glossary

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).
Access Right	The privilege or permission for an individual to access areas controlled by a physical access system.
Applicant	An individual applying for a PIV card/credential. The applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.
Application	A hardware/software system implemented to satisfy a particular set of requirements. In the context of FIPS 201, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.
Assurance Level	The degree of certainty that the user has presented an identifier (e.g., a credential) that refers to his or her identity. In the context of FIPS 201, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Asymmetric Cryptography	A type of cryptographic system that uses a pair of mathematically related cryptographic keys. The public key can be made available to anyone and can be used to encrypt information or verify a digital signature. The private key is kept secret by its holder and can be used to decrypt information or generate a digital signature.
Asymmetric Keys	Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence of authenticity; for FIPS 201, in the validity of a person's identity and the PIV card.
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
Biometric Information	The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).
Biometric System	An automated system capable of the following: - Capturing a biometric sample from an end user - Extracting biometric data from that sample - Comparing the extracted biometric data with data contained in one or more references

	- Deciding how well they match - Indicating whether or not an identification or verification of identity has been achieved.
Capture	The method of taking a biometric sample from an end user. [INCITS/M1-040211]
Card	An integrated circuit card, also known as a smart card.
Cardholder	An individual to whom a PIV card was issued.
Card Reader	An electronic device that connects an integrated circuit card and the card applications therein to a client application. Also known as a card interface device.
Certification	The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.
Chain of Trust	An attribute of a secure ID system that encompasses all of the system's components and processes and assures that the system as a whole is worthy of trust. A chain of trust should guarantee the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust must also ensure that information within the system is verified, authenticated, protected and used appropriately.
CHUID	Cardholder Unique Identifier. Part of the standardized data model for cardholder identification data for FIPS 201.
Component	An element of a larger system, such as an identity card, PIV Issuer, PIV Registrar, card reader, or identity verification support, within the PIV system.
Confidence Level	The degree of likelihood that an identifier refers to a specific individual.
Control Point	Any device which is controlled by a physical access system (for example, doors, turnstiles, gates, lights, cameras, elevators). There may be multiple control points for a single access requirement.
Credential	Evidence attesting to one's right to credit or authority; in FIPS 201, it is the PIV card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. A smart card can store multiple digital credentials.
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.
Digital Signature	Method for authenticating digital information analogous to ordinary physical signatures on paper (i.e., "wet" signatures), but implemented using techniques from the field of cryptography. A digital signature method generally defines two complementary algorithms, one for signing and the other for verification, and the output of the signing process is also called a *digital signature*. By contrast, an *electronic signature* is simply a digital scan of a "wet" signature.

End Point Products	As defined in NIST SP 800-73, products that employ a unified card edge interface that is technology independent and compliant with current international standards.
FASC-N	Federal Agency Smart Credential Number. The data element that is the main identifier on the PIV card that is used by a physical access control system.
Federal Information Processing Standard (FIPS)	A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS publication covers some topic in information technology to achieve a minimum level of quality or interoperability.
FIPS 201	Federal Information Processing Standard Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.
GUID	Global Unique Identifier. Data element within the CHUID that must be present, and may include either an issuer-assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials.
Hash-Based Message Authentication Code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function. This is a means of digitally signing a block of data.
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. **One-Way. I**t is computationally infeasible to find any input that maps to any pre-specified output. 2. **Collision Resistant. I**t is computationally infeasible to find any two distinct inputs that map to the same output.
IAB	Government Smart Card Interagency Advisory Board.
ICC	Integrated circuit chip
Identification	The process of discovering the true identity of a person from the entire collection of similar persons.
Identifier	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
Identity Management System (IDMS)	System composed of one or more computer systems or applications that manages the identity registration, verification, validation, and issuance process, as well as the provisioning and deprovisioning of identity credentials.

Identity Proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV registrar when attempting to establish an identity.
Identity Registration	The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.
Identity Verification	The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV card or system and associated with the identity being claimed.
Interoperability	For the purposes of FIPS 201, interoperability allows any government facility or information system, regardless of the PIV issuer, to verify a cardholder's identity using the credentials on the PIV card.
Issuer	The organization that is issuing the PIV card to an individual. Typically this is an organization for which the individual is working.
Key	See "Cryptographic Key."
Match/Matching	The process of comparing biometric information against previously stored biometric data and scoring the level of similarity.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Model	A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.
NAC	National Agency Check. Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check. The NAC is part of every NACI.
NACI	National Agency Check with Inquiries. The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).
NIST	National Institute of Standards and Technology
Off-Card	Refers to data that is not stored within the PIV card or to a computation that is not performed by the integrated circuit chip (ICC) of the PIV card.
On-Card	Refers to data that is stored within the PIV card or to a computation that is performed by the integrated circuit chip (ICC) of the PIV card.

PAIIWG	Physical Access Interagency Interoperability Working Group
Personal Identification Number (PIN)	A secret that an individual memorizes and uses to authenticate his or her identity or to unlock certain information stored on the PIV card (e.g., the biometric information). PINs are generally only decimal digits.
PACS	See physical access control system.
Personal Identity Verification (PIV) Card	A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains printed and stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
Physical Access Control System (PACS)	A system composed of hardware and software components that controls access to physical facilities (e.g., buildings, rooms, airports, warehouses).
PIN	See Personal Identification Number.
PIV	See Personal Identity Verification
PIV Registrar	An entity that establishes and vouches for the identity of an individual to a PIV issuer. The PIV registrar authenticates the individual's identity by checking identity source documents and identity proofing, and ensures a proper background check has been completed, before the credential is issued.
Population	The set of users for the application. [INCITS/M1-040211]
Private Key	The private part of an asymmetric key pair that is protected by the owner and used to decrypt data or create a digital signature.
Public Key	The public part of an asymmetric key pair that is typically used to encrypt data or verify a digital signature.
Public Key Infrastructure (PKI)	A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.
Registration	See "Identity Registration."
Secret Key	A cryptographic key used in symmetric cryptography that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution.
Smart Card	A device that includes an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card

	connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are available in a variety of form factors, including plastic cards, SIMs, and USB-based tokens.
Standard	A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.
Symmetric Cryptography	A type of cryptographic system that uses the same secret key to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).
TLV	Tag-Length-Value. A commonly used means of storing multiple fields of digital data in a single block. A **tag** for the first field is stored with a specified and fixed length; following that is another fixed length data item describing the **length** of the data to follow; the **value** follows.
Transitional Products	As defined in NIST SP 800-73, products that meet the Transitional interface specification. Transitional products can be used as part of a migration strategy by agencies that have already initiated a large-scale deployment of smart cards as identity badges.
Trustworthiness	Security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]
Verification	See “Identity Verification.”

12 Appendix A: PIV Card Authentication and Assurance Levels

For PIV cards issued by different agencies to be accepted throughout the Federal government, every agency must have confidence in the PIV cards issued by every other agency. To support PIV card interoperability among Federal government agencies, NIST has defined a set of identity authentication assurance levels in FIPS 201.

12.1 Identity Authentication Assurance Levels

Identity authentication assurance levels define how much confidence an agency can have in the established identity of a cardholder presenting a PIV card. Each assurance level refers to a degree of confidence that an agency can have in a PIV card, even if the PIV card is issued by a different agency. Each level is achieved by using specified methods to authenticate a cardholder and validate a card. The authentication process determines whether the cardholder is actually who the cardholder claims to be through the following:

1. The rigor of the identity proofing process conducted prior to issuing the PIV card;
2. The security of the PIV card issuance and maintenance processes; and
3. The strength of the technical mechanisms used to verify that the cardholder is the owner of the PIV card.

All Federal agencies are responsible for authenticating the identities of employees, contractors, and other authorized personnel to whom they issue PIV cards. Once a chain of trust is established between the agency and its cardholders, the agency selects an assurance level that will be compatible with its security needs.

Each agency is also responsible for determining what assurance level is required to safeguard its physical and logical resources. The transaction between a PIV card and card reader can be more or less reliable, and an agency may have varying requirements for transaction reliability. These requirements reflect the value of the assets that the agency's PACS is protecting. After agencies have assigned an assurance level to each resource, they must apply the appropriate PIV card authentication mechanisms to guarantee that access to these resources is granted only if the required level of assurance has been achieved.

12.1.1 FIPS 201 Assurance Levels

FIPS 201 defines three assurance levels:

- Some: A basic degree of assurance in the identity of the cardholder
- High: A strong degree of assurance in the identity of the cardholder
- Very high: A very strong degree of assurance in the identity of the cardholder

Each level is associated with one or more basic PIV card authentication mechanism. Other authentication mechanisms could be implemented based on optional logical credential elements (e.g., symmetric authentication key) that could be implemented on a PIV card.

12.1.2 OMB's E-Authentication Assurance Levels

The levels of assurance defined by FIPS 201 align with the levels defined in Section 2 of OMB memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* (OMB 404).

Table 12-1 correlates the OMB assurance levels with the FIPS 201 assurance levels.

Table 12-1: Correlation Between OMB E-Authentication and FIPS 201 Assurance Levels

OMB Level	Description	FIPS 201 Level
1	Little or no confidence in the asserted identity's validity	No equivalent
2	Some confidence in the asserted identity's validity	Some confidence
3	High confidence in the asserted identity's validity	High confidence
4	Very high confidence in the asserted identity's validity	Very high confidence

OMB 404 addresses "identity assurance for electronic transactions requiring authentication" and prescribes a methodology based on the risks and potential impact of errors in identity authentication. FIPS 201 requires owners of logical resources to apply the methodology defined in OMB 404 to identify the assurance level required for electronic transactions. Agencies may use a methodology similar to that defined in OMB 404 to determine the FIPS 201 assurance level required to access their physical resources; they may also use other applicable methodologies to determine the required level of identity assurance for their physical resources.

The PIV card can be used to authenticate a cardholder's identity for physical access. Table 12-2 summarizes the PIV-card-supported authentication mechanisms for a PACS. A PIV card authentication mechanism that is suitable for a higher assurance level can be used to meet the requirements for a lower assurance level.

Table 12-2: Authentication for Physical Access

FIPS 201 Assurance Level	Applicable Authentication Mechanism
Some confidence	Visual, CHUID
High confidence	Biometric
Very high confidence	Biometric-Attended, Public Key Infrastructure

Each authentication mechanism described in Table 12-2 can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the department or agency's network infrastructure.

12.1.3 Smart Card Interagency Advisory Board (IAB) Assurance Levels

The Government Smart Card Interagency Advisory Board's Physical Access Interagency Interoperability Working Group (PAIIWG) publication, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2,* July 30, 2004 (PACS 2.2) also defines assurance levels (profiles). Each level provides a different degree of confidence that the PIV card is valid and that the person presenting the PIV card is the assigned cardholder. The levels (profiles) are as follows:

- Low: Provides none of the true security benefits of a smart card, because there is no way to determine whether the card presented is genuine or whether the data is genuine or altered.
- Medium: Provides no assurance that the card is genuine but does guarantee that the data is valid. It assures that the data presented has not been altered, but it does not protect against the data being cloned or played back.
- High: Provides assurance that the card is genuine and that the data has not been altered. A cryptographic challenge/response validates that the card has been issued by the authorized agency. This level uses the security features of a smart card.
- High with PIN: Provides the same high assurance with the addition of a PIN to verify the cardholder.

Table 12-3 correlates the PACS 2.2 assurance levels and the FIPS 201 assurance levels.

Table 12-3: Correlation of PACS 2.2 and FIPS 201 Assurance Levels

PACS 2.2 Assurance Level	FIPS 201 Assurance Level
Low	Some confidence
Medium	Some confidence
High (without PIN)	Some confidence
High (with PIN)	Very high confidence

12.2 PIV Card Authentication Mechanisms

Table 12-2, above, lists the PIV card authentication mechanisms that can be used to authenticate cardholders to the different FIPS 201 assurance levels. This section describes each mechanism in greater detail.

12.2.1 Authentication Using Visual Credentials

Authentication using visual credentials, or VIS, can achieve some confidence (the "some assurance" level) in the identity of a cardholder. Because it is prone to human error, visual authentication provides the lowest level of identity assurance. Agencies may want to implement visual authentication when they cannot install electronic PIV card readers at all physical access locations or where it may not be feasible for them to have connectivity to the PACS at all physical access locations.

Several visual elements can be used for VIS, including a photograph, name, employee affiliation/employment identifier, expiration date, agency card-serial number, and issuer identification. An agency may also choose to implement and use optional elements such as a cardholder signature or cardholder physical characteristics (e.g., height, weight and hair color).

The visual authentication process should at a minimum follow these steps:

1. The security officer at the physical access entry point confirms that the PIV card presented appears to be valid and unaltered.

   For a security officer to check the validity of a PIV card and determine whether it is unaltered, the officer will need training on the physical characteristics of the PIV card.

2. The security officer compares the photograph on the PIV card to the face of the individual presenting the card.
3. The security officer checks the expiration date on the PIV card to ensure that the card is still valid.
4. One or more of the other visual data elements are used to determine whether the PIV cardholder should be granted access.

If agencies choose to implement any optional visual elements, the officer could also do the following:

- Check the physical characteristics on the card to ensure that they describe the individual presenting the card.
- Collect the cardholder's signature and compare it with the signature on the card.

People never sign their signature the same way twice. Therefore, if the visual authentication process includes evaluating the cardholder's signature with the signature on the card, security officials need proper training in detecting false signatures.

12.2.2 Authentication Using the CHUID

Implementation of PIV II requires that all PIV cards contain a CHUID. A PIV cardholder can be authenticated electronically using the CHUID, which is stored in the card chip(s). Because the CHUID is a free-read data element, it provides only some confidence (the "some confidence" assurance level) in the identity of the cardholder.

If authentication is to be accomplished using the CHUID, a FIPS 201-compliant PIV card reader must be installed at the access point. Both contact and contactless readers can read the CHUID. The CHUID can be used to authenticate a PIV cardholder using the following process:

1. The CHUID is read electronically from the card.
2. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Number System) are used to determine whether the PIV cardholder should have access.
3. In addition, the following CHUID data elements can be used:
    - The digital signature of the CHUID, which can be checked to ensure that it was signed by a trusted source and is unaltered.
    - The expiration date of the CHUID, which can be checked to ensure that the PIV card has not expired.

12.2.3 Authentication Using Biometric Data

A PIV card contains, at a minimum, two digitally signed fingerprint images stored on the PIV card chip and accessed through the contact interface. These images can be used to authenticate the cardholder with high confidence (the high assurance level) or very high confidence (the very high assurance level), depending on the situation. Unless an alternative use of biometric templates is implemented (as described in Section 3.2.2), only contact readers can accomplish biometric authentication.

The biometric authentication process can be unattended or attended. When there is no security guard or attendant at a physical access point, the cardholder enters a PIN and provides a biometric without supervision. Unattended biometric authentication provides only high confidence in the identity of the cardholder, because the cardholder could be providing the PIN and biometric under duress. When there is a security guard or attendant at a physical access point, the PIV cardholder enters a PIN and provides a biometric under supervision. Attended biometric authentication provides very high confidence in the identity of the cardholder, because a security guard or attendant witnesses the transaction.

Agencies can choose to use one or both of the two biometric fingerprint images stored on a PIV card for authentication purposes. FIPS 201 does not mandate whether the match takes place off the card (e.g., on a reader, panel or server) or on the card. Performance considerations may dictate that biometric templates be used rather than the draft NIST SP 800-76-prescribed fingerprint images to meet PACS rapid authentication requirements. Consideration should also be given to adding biometric templates to the PIV card for access through the contactless interface; however, due to proprietary implementations, biometric templates cannot support inter-agency interoperability.

12.2.4 Authentication Using Asymmetric Cryptography (PKI)

A PIV card carries mandatory and optional asymmetric private keys and corresponding certificates on the PIV card chip, which are accessed through the contact interface. This data can be used to authenticate the cardholder with very high confidence (the very high assurance level).

The process for using asymmetric cryptography to authenticate a cardholder is as follows:

1. The cardholder is prompted to enter a PIN. By entering the PIN, the cardholder activates the PIV card and allows a card reader to access it.
2. The card reader issues a challenge request to the card and requests an asymmetric operation in response.
3. The PIV card signs the challenge request with the PIV authentication private key and attaches the associated certificate.
4. The card reader verifies the response signature and PKI path validation is conducted in compliance with X.509 certificate policy. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure that the certificate has not been revoked.
5. The subject distinguished name and FASC-N are extracted from the authentication certificate and passed to the authorization function. This step requires connectivity to the PKI network. Standalone access control systems will not be able to perform this step.

12.2.5 Authentication Using Card Authentication Key

The PIV card may include additional symmetric keys, asymmetric keys and certificates, which can be used to authenticate the cardholder with very high confidence (the very high assurance level).

FIPS 201 defines requirements for digital signature and key management keys. Where digital signature keys are supported, the PIV card is not required to implement a secure hash algorithm. Message hashing may be performed off-card. Cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a card authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES)-based challenge-response protocols for physical access, the PIV card must contain storage for the AES key and support AES operations through the contactless interface. If the contactless interface uses asymmetric cryptography (e.g., elliptic curve cryptography), the PIV card may also require storage for a corresponding public key certificate.

FIPS 201 and the PKI Common Policy support the use of both RSA and elliptic curve cryptographic algorithms. Where an asymmetric card authentication key is accessible through the contactless interface, the elliptic curve algorithm offers compelling performance advantages. Private key operations can be performed with fewer operations than with RSA, and the encrypted challenge and the public key certificate will be smaller. To maximize performance, agencies should consider the 163-bit elliptic curve algorithms for the asymmetric card authentication key. However, agencies should note that elliptic curve authentication mechanisms are not widely implemented at this time. Agencies should not assume that the cards issued by other agencies will support elliptic curve card authentication keys.

All cryptographic operations using the PIV keys must be performed on the card. Therefore, the card need not implement any additional cryptographic functionality, such as hashing or signature verification on the card itself. Algorithms and key sizes for each PIV key type are specified in SP 800-78.

The PIV card carries a single mandatory key and four types of optional keys. One of these optional keys is the card authentication key. This key can be either a symmetric (secret) key or an asymmetric private key for physical access. Like all PIV cryptographic keys, the card authentication key must be generated by a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV card must provide Level 3 physical security to protect the PIV private keys in storage.

FIPS 201 also includes requirements specific to storage of and access to the card authentication key. The PIV card must not permit the card authentication key to be exported. The card must support the performance of private/secret operations using the key without explicit user action

(e.g., without supplying a PIN). FIPS 201 does not specify key management protocols or infrastructure requirements.

The required contents of the X.509 certificates associated with PIV private keys are based on specifications in "*X.509 Certificate and CRL Profile for the Common Policy.*"[23] The certificates containing the public key associated with an asymmetric card authentication key must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension and must assert id-PIV-cardAuth in the extended key usage extension.

[23] *X.509 Certificate and CRL Profile for the Common Policy*, Version 1.1, July 8, 2004. Available at http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf.