Considerations for the Migration of Existing Physical Access Control Systems to Achieve FIPS 201 Compatibility

A Smart Card Alliance Physical Access Council White Paper

Publication Date: September 2006

Publication Number: PAC-06001

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 a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of 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

Introduction

Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, mandated 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.

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*, issued on February 25, 2005, and a number of special publications that provide more detail on the implementation of the standard. This standard has far-reaching effects on Federal agencies in providing specifications that govern the entire chain of trust of the identity system and in specifying a single smart card – the PIV card – to be used for both physical and logical access, as well as other applications as determined by the individual agencies.

Both Federal agencies and enterprises are now implementing FIPS 201-compliant identity (ID) programs.

Purpose of this White Paper

There are many considerations for physical access control systems (PACS) under HSPD-12 and FIPS 201. One important consideration affecting organizations is the migration from existing PACS to new FIPS 201-compatible systems. What happens when some employees have PIV cards and some do not? How can the existing PACS accommodate the migration to FIPS 201 compatibility? Can systems be upgraded or must new systems be acquired? What security considerations are there?

The focus of this document is to consider the current security environment for physical access and, through a series of questions, make recommendations for how agencies can migrate and upgrade their current PACS to align them with the requirements of HSPD-12 and FIPS 201 end state compatibility. This document is informative and provides guidance for implementing a FIPS 201-compatible PACS. It is designed as a simple tool to assist agencies in planning for the initial deployment of FIPS 201-compatible PIV systems and issuance of PIV cards. This document is intended to contribute to best practices and to be used to simplify the procurement process and help reduce acquisition costs.

Scope of this White Paper

The use of a smart card is only the tip of the iceberg in a secure ID system implementation. Identity verification and management processes range from enrollment and issuance to usage in logical and physical access control systems and authentication with back-end systems.

In considering FIPS 201 migration steps, this document covers the PACS from the card reader to the access control server as well as the PACS registration process. Also included within the scope of this white paper is the use of a back-end certificate revocation list (CRL) or online credential status protocol (OCSP) responder for checking if a PIV card has been revoked.

The specific protocols and physical connections that link the PACS readers with PACS servers are also within this scope. Since a FIPS 201-compliant PIV card must present a standard interface to a FIPS 201-compliant PIV card reader, this is the PIV system's point of interoperability. The method and protocol used to connect PACS readers to control panels and servers, as well as the PACS data and access control policies, are at the discretion of the agency. It is in the scope of this document to promote best practices and convergence of technologies. The PACS reader-to-server interface is covered by few existing standards;

therefore, implementation guidance is needed to create PACS solutions that are FIPS 201-compatible and meet operational and security requirements.

The following technologies and processes are not included within the scope of this white paper:

- Enrollment and issuance systems and processes
- Back-end authentication beyond revocation status
- Security policies
- Specific configurations
- Operation of and data in the PACS server, and its link to the agency information technology (IT) infrastructure
- Cardholder and access status updates to the issuer and host agencies
- Reader-to-control panel link protocols and technology, both of which are at the discretion of the agency.

How to Use the Tools in this White Paper

Organizations implementing FIPS 201-compatible PACS can use the tools in this white paper to develop the plan and approach to upgrading or replacing existing PACS equipment.

Section 1 includes two tools:

- A worksheet to assist with documenting the current PACS configuration, and
- A detailed flow chart with assessment questions. Agencies should use this flow chart to walk through key PACS migration considerations and determine what hardware and software can be upgraded and what will need to be replaced.

Section 2 provides additional explanation for questions included in the assessment flow chart. Section 3 provides guidance on alternative processes that can be used for registering a PIV card into a PACS.

The appendices include additional information on scenarios for using biometrics during PIV card registration and PACS use and external IT infrastructure subsystems that are needed for FIPS 201 compatibility. Also included are a FIPS 201 PACS site survey worksheet and glossary of terms.

1 FIPS 201 PACS Assessment Worksheet

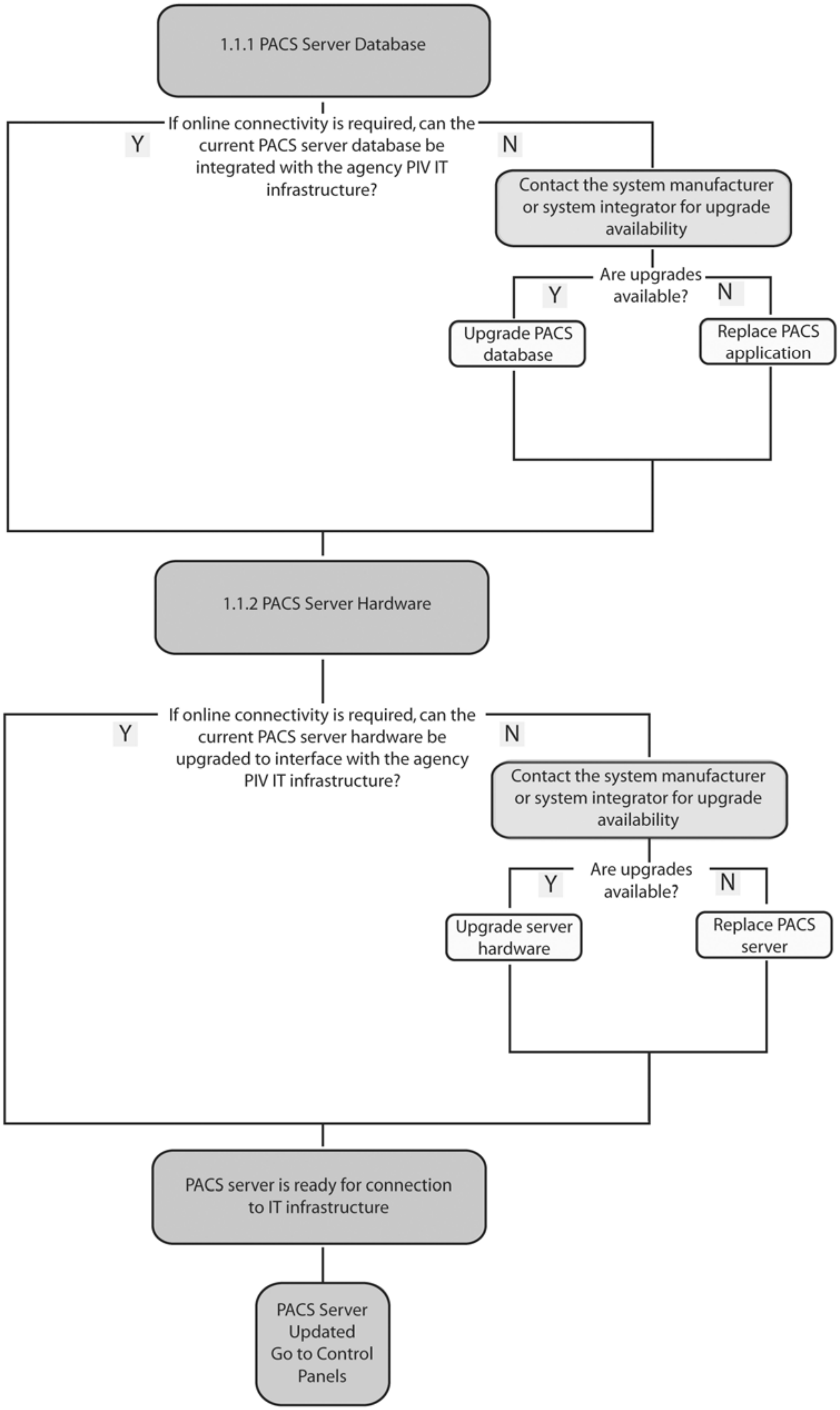
The tools in this chapter and in Appendix D were designed to help organizations plan for the migration of existing PACS to FIPS 201 compatibility.

An important first step is the development of a detailed understanding of the capabilities of the current PACS components. Appendix D includes a detailed PACS site survey worksheet that can be used to compile an inventory of the PACS equipment currently in use. This information can then be incorporated into the worksheet below summarizing the information that is needed to assess the system's ability to work with FIPS 201-compliant PIV cards and back-end authentication systems.

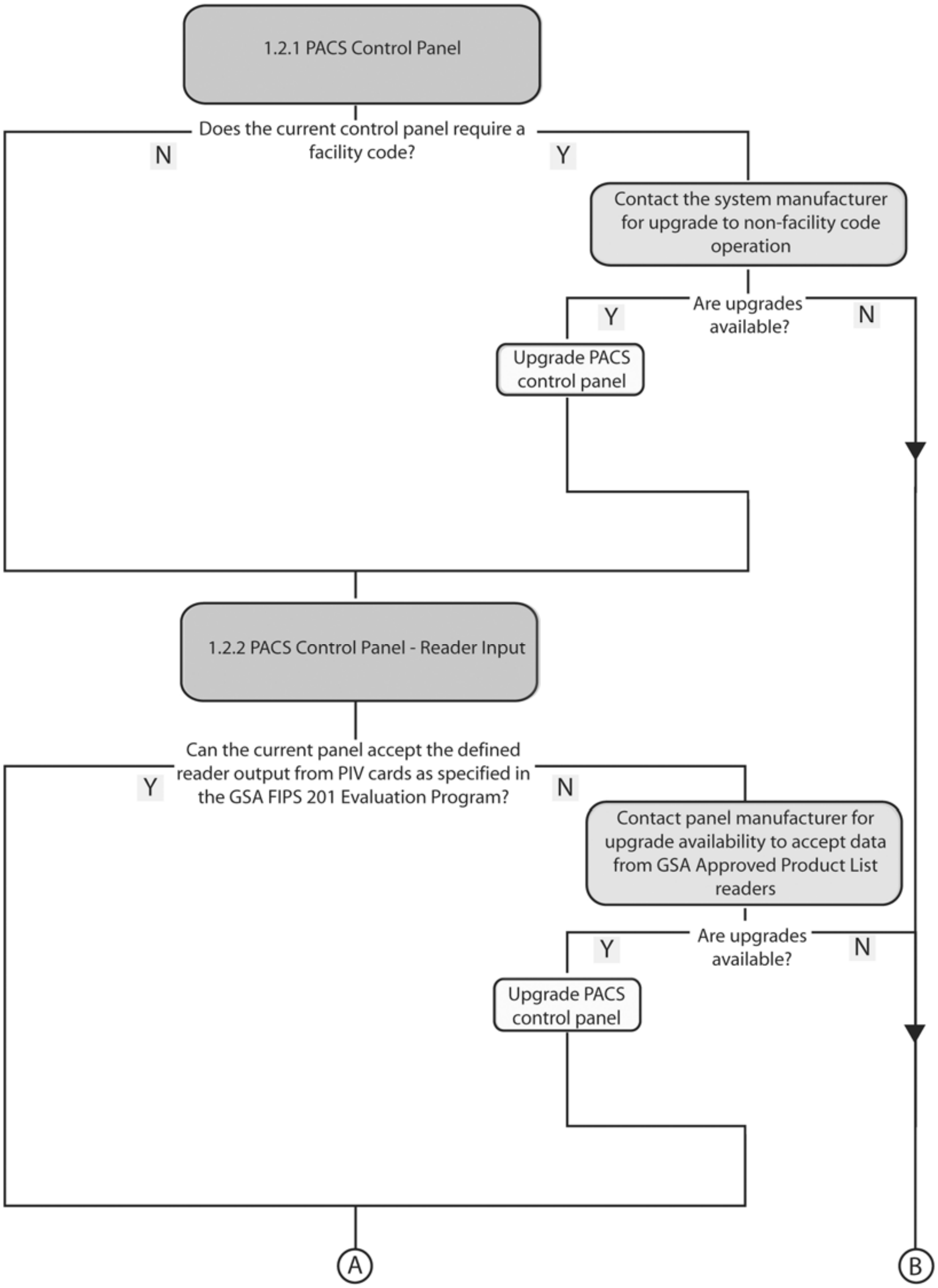
With this information, each component can be assessed for its ability to meet FIPS 201 requirements. The flow charts shown in sections 1.1, 1.2 and 1.3 step through key assessment questions to determine whether the PACS server, control panels and readers can be upgraded or whether they will need to be replaced. Section 2 includes additional information to explain the importance of the questions that are included in this flow chart.

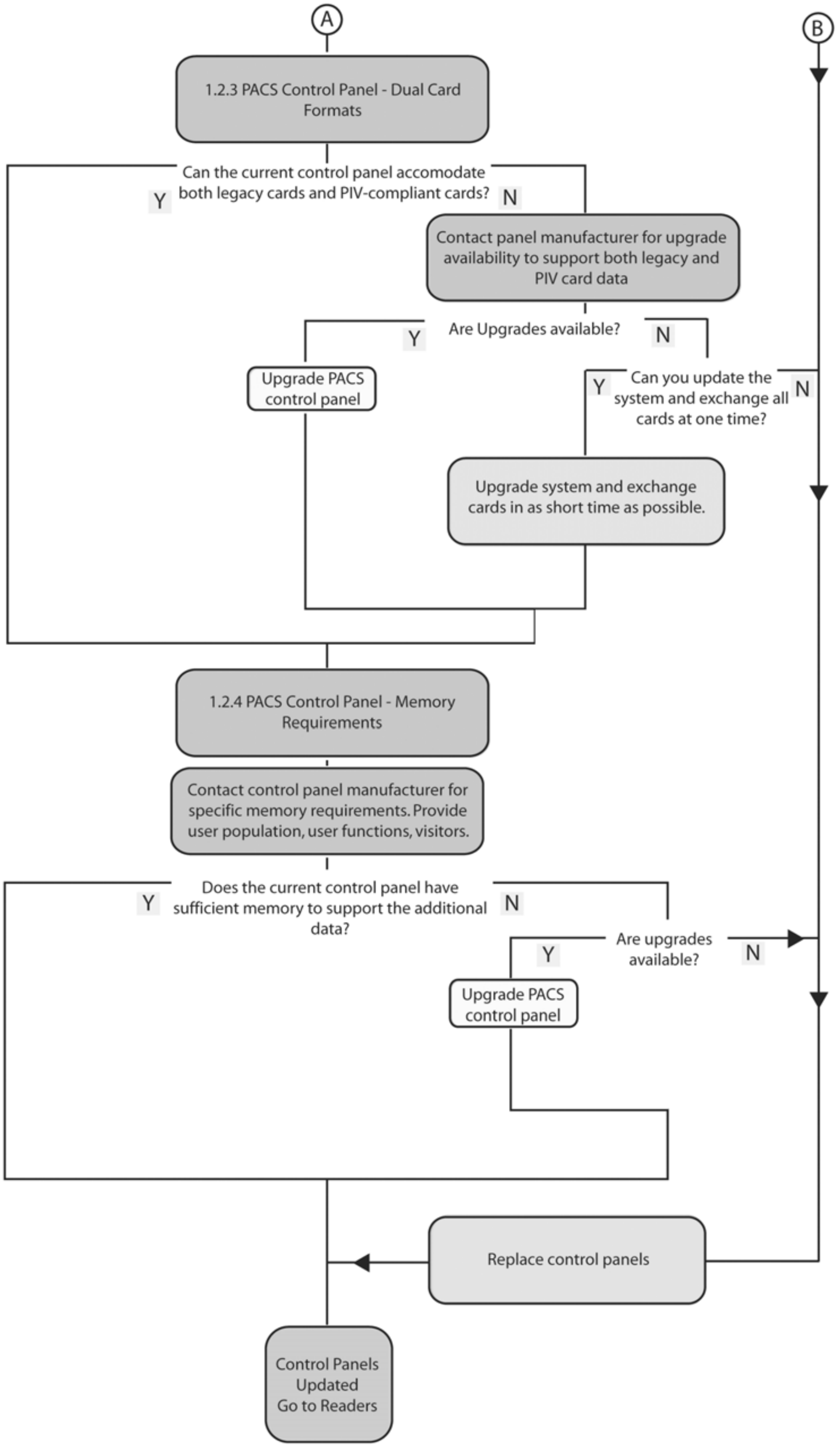
Local PACS Components	Site Equipment Summary
Local PACS Server	
• Hardware:	
• Manufacturer:	
• Model:	
• Operating system:	
• Database:	
• Hard disk drive capacity:	
• Number of clients:	
Door Control Panel	
• Manufacturer:	
• Model:	
• Firmware version:	
• Control panel – server communication:	
• Control panel – reader interface:	
Door Reader	
• Number of readers:	
• Reader technology (e.g., magnetic stripe, 125Khz proximity):	
• Number of card-only readers:	
• Number of multi-factor readers (e.g., card and PIN; card and biometric):	
• Biometric type:	
• Biometric reference storage (reader, card, server):	
• Available cabling:	
Door Security Levels	
• Number of access control points – attended:	
• Number of access control points – unattended:	

1.1 PACS Server Upgrades for IT Infrastructure Interfaces

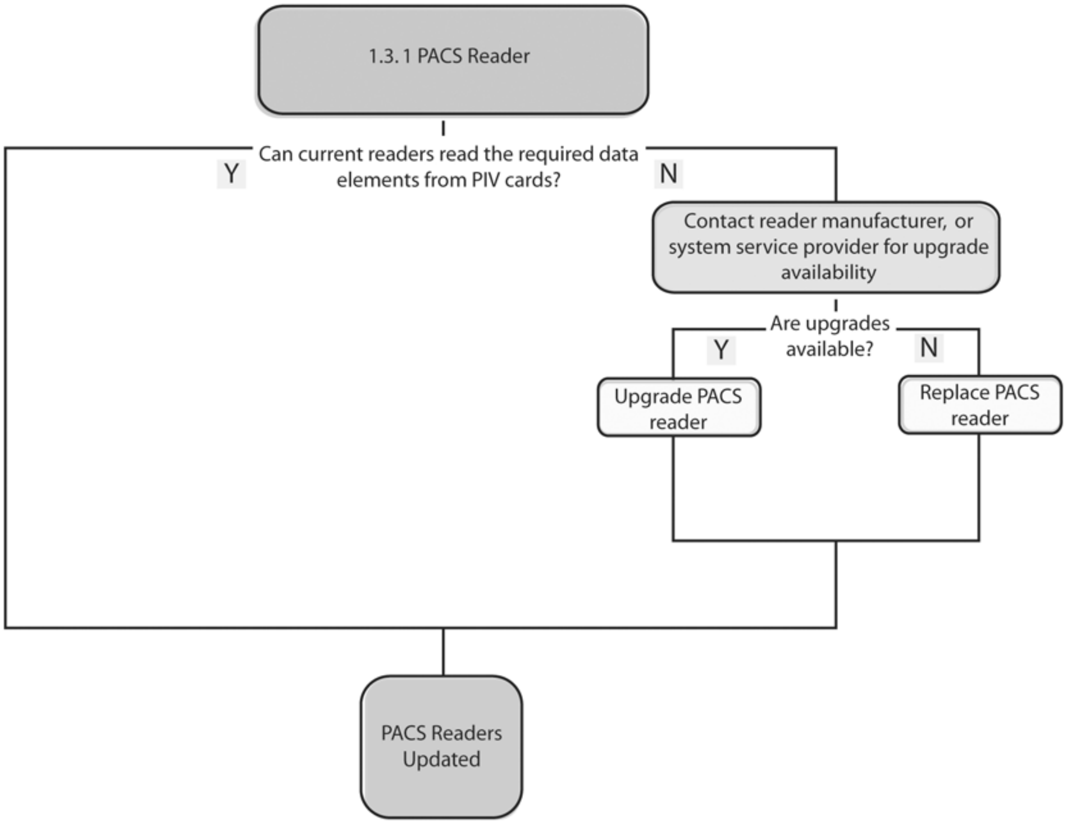

1.1.1 PACS Server Database
If online connectivity is required, can the current PACS server database be integrated with the agency PIV IT infrastructure?
Y
N
Contact the system manufacturer or system integrator for upgrade availability
Are upgrades available?
Y
N
Upgrade PACS database
Replace PACS application
1.1.2 PACS Server Hardware
If online connectivity is required, can the current PACS server hardware be upgraded to interface with the agency PIV IT infrastructure?
Y
N
Contact the system manufacturer or system integrator for upgrade availability
Are upgrades available?
Y
N
Upgrade server hardware
Replace PACS server
PACS server is ready for connection to IT infrastructure
PACS Server Updated Go to Control Panels

1.2 PACS Control Panel Upgrades


1.2.1 PACS Control Panel
Does the current control panel require a facility code?
N
Y
Contact the system manufacturer for upgrade to non-facility code operation
Are upgrades available?
Y
N
Upgrade PACS control panel
1.2.2 PACS Control Panel - Reader Input
Can the current panel accept the defined reader output from PIV cards as specified in the GSA FIPS 201 Evaluation Program?
Y
N
Contact panel manufacturer for upgrade availability to accept data from GSA Approved Product List readers
Are upgrades available?
Y
N
Upgrade PACS control panel
A
B


A
B
1.2.3 PACS Control Panel - Dual Card Formats
Can the current control panel accomodate both legacy cards and PIV-compliant cards?
Y
N
Contact panel manufacturer for upgrade availability to support both legacy and PIV card data
Are Upgrades available?
Y
N
Upgrade PACS control panel
Can you update the system and exchange all cards at one time?
Y
N
Upgrade system and exchange cards in as short time as possible.
1.2.4 PACS Control Panel - Memory Requirements
Contact control panel manufacturer for specific memory requirements. Provide user population, user functions, visitors.
Does the current control panel have sufficient memory to support the additional data?
Y
N
Are upgrades available?
Y
N
Upgrade PACS control panel
Replace control panels
Control Panels Updated Go to Readers

1.3 PACS Readers


1.3.1 PACS Reader
Can current readers read the required data elements from PIV cards?
Y
N
Contact reader manufacturer, or system service provider for upgrade availability
Are upgrades available?
Y
N
Upgrade PACS reader
Replace PACS reader
PACS Readers Updated

2 *Clarification of the Assessment Questions*

This section provides additional information to clarify the importance and relevance of the questions that are included in the Section 1.1, 1.2 and 1.3 flow charts.

At sites where the local PACS server and PIV IT infrastructure are or will be connected, Section 2.1, questions 1.1.1 and 1.1.2 are relevant.

2.1 *Local PACS Server*

Question 1.1.1: Can the current PACS server database be integrated with the agency PIV IT infrastructure?

For physical access to facilities, an individual's identity has traditionally been authenticated locally by using paper or other non-automated, hand-carried credentials, such as driver's licenses and ID badges. With few exceptions, PACS servers and cardholder databases are updated manually by a local PACS operator. FIPS 201 defines procedures for the PIV card lifecycle activities including identity proofing, enrollment, PIV card issuance, and PIV card usage. A wide range of mechanisms are employed to authenticate identity, maintain identity information and certificates, and implement revocation procedures to ensure that only authorized individuals have access to government resources. To automate FIPS 201 processes, PACS server databases must be integrated with the other components of agency PIV IT infrastructure.

Modern PACS databases are often upgradeable. Several PACS suppliers and system integrators offer upgrade packages and services to facilitate integration to external IT resources.

Agencies may also require the development of procedures to comply with the Federal Information Security Management Act (FISMA) before allowing a local PACS server to be connected to the agency IT network. The primary concerns that need to be addressed are:

- Database structure
- Administrator and operator access policies
- Implementation of operating system security patches
- System upgrades and change management

Agencies should contact the IT department for policy clarification prior to initiating PACS server upgrades.

A list of related reference documentation is included in Appendix C.

Question 1.1.2: Can the current PACS server hardware be upgraded to interface with the agency PIV IT infrastructure?

FIPS 201 provides detailed technical specifications to support interoperability among Federal departments and agencies. It is important to note, however, that the link from the reader to the server and server functionality is not specified; user agencies have the responsibility to implement the reader-to-server link and PACS server functions, as long as compatibility with FIPS 201 is achieved.

Question 1.1.5: Does the current PACS server database support multiple card formats for one single user?

During a transitional period, existing as well as new FIPS 201-compliant readers may co-exist in one system. Until all existing equipment (e.g., cards and readers) is updated or replaced, one person may have both an existing card and a PIV card.

The consequence in a PACS server is that each cardholder may have to be entered into the PACS database twice, once with the data read from the existing card and once with the data read from the PIV card (the FASC-N). Some PACS server databases are capable of registering multiple credentials for the same individual, while others may require a separate record for each card, even when they belong to the same individual.

2.2 PACS Control Panel

Question 1.2.1: Does the current control panel require a facility code?

PACS manufacturers often embed an 8-bit facility code number, 0-255, in their system control panels. The facility code precedes a 16-bit sequential or unique number, 0-65535, for the card. As a user presents the card to a PACS card reader, the card's facility code and sequential, or unique, number are read and transmitted to the PACS control panel for verification and authentication. When the facility code from the card matches the facility code stored in the PACS control panel, the sequential, or unique, number is verified and the system makes a decision to grant or deny access.

When the facility code does not match, the PACS regards the card as alien to the system. The PACS then generates an error message and denies access. No further processing occurs.

The FIPS 201 standard does not specify existing facility codes for PACS. The PIV card uses a Federal Agency Smart Credential Number (FASC-N). As a result, existing numbering systems must either be modified or replaced.

Question 1.2.2: Can the current control panel accept the defined reader output from PIV cards as specified in the GSA FIPS 201 Evaluation Program?

The most common data stream produced by PACS readers for current access cards is 26 bits of Wiegand data (8-bit facility code, 16 bits of data, 2 parity bits). A reader included on the GSA Approved Product List (APL) must produce 75 bits of data (48-bit FASC-N, 25-bit expiration date, 2 parity bits). An approved PIV reader must, at a minimum, transmit the 75 bits of data to the control panel. The PACS reader, panel, or server must process the 75 bits of data received from the card and reader. The 48-bit FASC-N (the unique ID number) and 25-bit expiration date must be checked for every access transaction. However, the expiration date may be parsed out of the data and checked either at the reader using card data or at the panel or server using the PACS database.

The reader to control panel communication protocol and link are not specified by FIPS 201 and may be specific to a control panel. However, the GSA FIPS 201 Evaluation Program requires that PIV card data only be sent using Wiegand, RS232, RS485 or TCP/IP protocols.

Existing PACS control panels must be updated to receive and process the longer data streams, or must be replaced.

Question 1.2.3: Can the current control panel accommodate both existing cards and PIV compliant cards?

Initially, the card population at each site will consist primarily of existing PACS cards. As the number of people who are issued PIV cards increases, the number of existing cards will gradually decrease until all are replaced with PIV cards.

During this transition period, it may be necessary for the PACS to process data from existing cards as well as from PIV cards.

Question 1.2.4: Does the current control panel have sufficient memory to support the additional data?

Cardholder records stored in the control panel will require additional memory space to accommodate the larger amount of data required for each user in FIPS 201-compatible systems. In many cases, this may not cause a problem since control panels are seldom used to capacity.

However, the difference between current memory consumption per cardholder record and memory required in a FIPS 201-compatible environment is significant. Each manufacturer has its own unique method for storing, accessing and utilizing cardholder-specific data. Control panels with complex feature sets also require additional memory space for each cardholder. The PACS system manufacturer should be contacted to determine the capacity offered in the specific PACS environment.

2.3 PACS Readers

The GSA FIPS 201 Evaluation Program defines contactless PACS readers in two categories: Card Holder Unique Identifier (CHUID) and Transparent. A "CHUID reader" reads the CHUID and validates the expiration date of a presented PIV card. A "Transparent" reader reads the CHUID from a card, then extracts and sends FASC-N data and expiration date to a PACS control panel. As this reader type is most compatible with traditional PACS, this document covers only the "Transparent" reader type.

Question 1.3.1: Can current readers read the required data elements from the PIV cards?

For contactless operation, FIPS 201 and SP 800-73 specify the use of ISO/IEC 14443 contactless smart card technology (readers and cards) for Federal agency PACS applications.

The GSA FIPS 201 Approved Products List (APL) (http://fips201ep.cio.gov/apl.php) includes approved readers. If the existing readers' make and model are not listed on the GSA APL, then the readers must be upgraded or replaced.

According to the GSA Evaluation Program’s test protocol, all GSA APL-listed readers must be capable of producing a minimum of 75 bits of data (48-bit FASC-N, 25-bit expiration date, 2 parity bits), when reading a PIV card. It is important to note that, for PIV cards, the reader produces the same minimum 75 bits of data (48-bit FASC-N, 25-bit expiration date, 2 parity bits) whether it is a card-only reader or a multi-factor reader (card plus personal identification number (PIN)d, card plus biometric, or card plus PIN and biometric).

For the past few years, several reader manufacturers have produced ISO/IEC 14443-compliant smart card readers that are upgradeable to support FIPS 201 requirements.

The service company should be contacted for more information.

2.4 Biometric Implementation for Access Control

FIPS 201 Section 6 (PIV cardholder authentication) does not differentiate between a FASC-N produced by a card-only PIV card reader and a FASC-N produced by a reader where the identity verification process requires the use of card, PIN and/or biometric. Therefore, from a PACS system perspective, there is no difference in the submission of the FASC-N among readers supporting one-, two- or three-factor authentication. According to FIPS 201 and SP 800-73, all readers produce the same FASC-N. As a result, adding a reader that supports a biometric or one that supports card and PIN is no different from adding a PIV card-only reader. Processing the FASC-N produced by a three-factor biometric reader is the same as processing a FASC-N produced by a PIV card-only reader.

Below are some considerations for implementing biometrics for access control.

FIPS 201 requires contact smart card readers with PIN entry to release the standard fingerprint templates from the PIV card for matching. Use of contact readers with PIN entry and fingerprint biometrics may not meet throughput requirements for entry points requiring high-volume, rapid access. In addition, contact readers may not be practical for an outdoor environment where the reader is exposed to the weather.

Consider one of the following alternative biometric implementations that are permitted in FIPS 201, SP 800-76 (see Section 1.2), but which may not be interoperable with other agencies:

- Storing the biometric off-card.
- Storing the biometric on-card in an agency-specific container.

Appendix A includes use case scenario details for these biometric implementations.

3 PACS Registration

3.1 PACS Registration: PACS Connected to External IT Infrastructure

A PIV card can be registered into a PACS in one of two ways: automatically from an authoritative source or manually. When a PIV card is manually registered into a PACS system, it is recommended that the site check the validity of the PIV card with the issuer and authenticate the user with the biometric before registering the user into the PACS. Registration could be performed on a third-party system or in an integrated PACS system component. Appendix B includes additional information on external IT infrastructure systems used for authentication.

During PACS registration, the PIV card is inserted into a contact reader connected to an administrative workstation. The cardholders are prompted to enter their PIN and place one of their two index fingers on a sensor for comparison with one of the two fingerprint biometric templates stored on the PIV card; this authenticates the cardholder to the card. As an option, the system administrator could also download the user's biographical data, photo (if present on the card), and fingerprint template (if the site plans to store biometrics on the PACS as an alternative biometric implementation) from the PIV card. The system administrator then enters the cardholder’s access permissions into the PACS.

Below is an example procedure for registering physical access privileges to a PIV cardholder.

- The PIV cardholder is escorted to the local PACS operator. The operator searches the PACS server cardholder database for the correct name that has been downloaded from the agency central identity management system (IDMS) or shared service provider (SSP). Once located and selected, the specific user data is displayed.
- The operator then asks the cardholder to insert the PIV card into a contact PIV reader connected to the PACS server, to enter the PIN, and to place a finger on the fingerprint sensor to authenticate that the person physically present is the same person to whom the PIV card was issued.
- If the person is authenticated as the valid holder of the PIV card, the PIV authentication certificate is checked through the external IT infrastructure to confirm that it is still a valid credential (e.g., not revoked). This is accomplished by accessing a certificate revocation list (CRL) or using an online certificate status protocol (OCSP) server.
- The reader reads the CHUID and the PIV authentication certificate from the credential and transmits these to the PACS.
- The PACS extracts the FASC-N from the CHUID and maps the FASC-N components (agency code, system code and credential number) to the proper locations of the cardholder record in the PACS.
- The PACS system extracts the expiration dates from both the CHUID and PIV authentication certificate. Whichever date is earlier is mapped to the proper locations of the PACS cardholder record.
- Next, the server concatenates the 4-digit agency code (AC), 4-digit system code (SC) and 6-digit credential number (CN), to form a new and unique 14-digit number. As an example, AC 1111, SC 2222, and CN 333333 may be converted to the 14-digit number, 11112222333333. This card number is downloaded to the proper control panels as determined by the physical access authorization rights for this cardholder.
- The PACS operator selects the authorized access control point (e.g., door) records in the PACS server and registers this card to a set of physical access privileges. The server

downloads the 14-digit number to the relevant control panels as the number that will be used to identify the PIV cardholder's record and access privileges.

During operational use of these enrolled credentials, readers located at each access control point read the PIV card. According to the GSA test protocol, the reader transmits the entire FASC-N or 14-digit number from the FASC-N and expiration date to the PACS for authorization. An alternative is to have the reader transmit only the 14-digit number derived from the FASC-N. The PACS compares the previously enrolled expiration date against the system clock. This allows the PACS system to honor the correct expiration date, whichever is earlier between the PIV authentication certificate and the CHUID.

Some PACS can be configured to suspend physical access privileges registered to an individual as opposed to deleting them. This simply means that any access requests attempted with a suspended card are archived and properly logged in the history file.

This approach enables an IDMS operator to easily suspend a card by simply changing the expiration date of the PIV card from the registered date to the current date and time. The modification is then downloaded to the PACS server. As soon as the PACS server receives the modification, the new date is downloaded to the control panel and access privileges are suspended for the specific PIV card. Alternatively, a PACS operator may change the expiration date for a user.

This method eliminates the need for a real-time clock in the PACS readers.

3.2 PACS Registration: Standalone PACS (Not Connected to External IT Infrastructure)

A visitor or new employee may have physical access privileges registered for the PIV card without the system being connected to the agency IT infrastructure (until such an infrastructure is in place). The following steps describe this process:

- The host agency receives notification of the visit before it occurs.
- The visitor or new employee is escorted to the PACS operator.
- The PACS operator asks the visitor or employee to insert the PIV card into a contact reader, enter the PIN, and place a finger on the fingerprint sensor to authenticate that the person is the valid holder of the PIV card.
- If authentication is confirmed, the reader reads the CHUID FASC-N and sends the FASC-N and expiration date to the PACS server.
- The PACS server extracts the agency code, system code and credential number from the CHUID FASC-N and concatenates the numbers to create the 14-digit card number.
- The PACS operator verifies the access level and areas where the visitor or new employee needs access and selects the authorized access control point(s) from the PACS door list.
- The PACS server creates a new cardholder record with an expiration date and downloads the FASC-N to the relevant control panels.

The visitor or new employee can now use the PIV card at access control points equipped with PIV readers until the expiration date occurs, or until access privileges are manually suspended by the PACS operator.

3.3 PACS Registration: PKI Pre-Validation for Standalone PACS (Not Connected to External IT Infrastructure)

Agencies may choose to implement PACS registration in a variety of ways; these are policy decisions and not dictated by FIPS 201. This section presents a registration scenario that allows PIV card validation for a standalone PACS.

If the agency uses a standalone PACS (that is not connected to an external IT infrastructure), an alternative approach can be used to validate the visitor's PIV card. In this scenario, a URL is stored on the PIV card; this URL is used to locate the issuing authority server to which the card's authentication certificate can be sent for validation. This process can be performed from a separate visitor verification station located at the visitor entrance and connected to an external IT infrastructure.

An online visitor verification station would consist of the following components:

- Contact PIV card reader
- Biometric sensor (fingerprint)
- Keypad
- Display
- IP port

If this approach is used, the visitor arrives and walks to an attended visitor desk. The visitor inserts the PIV card into the contact reader. The card and reader communicate and the visitor is prompted to enter the PIN. PIN verification opens the biometric container. The visitor is then prompted to place a finger on the fingerprint sensor for comparison with the stored biometric. Based on the result of the biometric verification, the unit will display a message that indicates if the match was successful. If the match is successful, the station sends the PIV card certificate number to the server located at the URL stored on the PIV card.

The result of this external IT system authentication is returned to the visitor verification station. When the response is positive, a message is displayed indicating that the visitor's card has been validated. The visitor is then allowed to enter the facility based on site or agency policy.

The visitor may proceed to the local PACS operator to have physical access privileges registered to the PIV card as described in sections 3.1 and 3.2.

4 Conclusions

Migrating to a FIPS 201-compatible PACS is a significant undertaking that will be a long process for most Federal agencies. Smart cards and readers are just the tip of the iceberg in FIPS 201 deployments. Government agencies need to consider new enrollment and issuance systems, as well as PACS changes and integration with back-end authentication systems. This white paper is designed to assist government agencies with the first phases of PACS migration to provide support for the new PIV cards that are being issued. By assessing current system capabilities and understanding the changes needed to support FIPS 201, agencies can develop a plan for migration – including what components can be upgraded and what components need to be replaced. The tools in this white paper help agencies to develop a solid foundation for their migration plans.

5 Publication Acknowledgements

This report was developed by the Smart Card Alliance Physical Access Council to assist government agencies with the development of the initial PACS migration plan to support new PIV cards. 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 18 organizations were involved in the development of this report including: Actcom Security Solutions, a Diebold Company; BearingPoint; Booz Allen Hamilton; CoreStreet; Fargo Electronics; HID Corporation; Hirsch Electronics; Honeywell; ID Technology Partners; Integrated Engineering; LEGIC Identsystems; Lenel Systems International; Northrop Grumman; Precise Biometrics; Saflink; SCM Microsystems; U.S. Department of Defense/Defense Manpower Data Center (DMDC); U.S. Department of State.

Special thanks go to the individuals who wrote, reviewed and edited this report and to Lars Suneborn, Hirsch Electronics, who managed the project.

Sal D'Agostino, CoreStreet
Tony Damalas, Actcom Security Solutions
Paul Evans, Booz Allen Hamilton
Bob Fee, LEGIC Identsystems
Marty Frary, HID Corporation
Bob Gilson, U.S. Dept. of Defense/DMDC
Mike Grady, Saflink
Marlin Grarino, U.S. Dept. of Defense/DMDC
Walter Hamilton, Saflink
Scott Hanson, Precise Biometrics
Stephen P. Howard, ID Technology Partners
Gary Klinefelter, Fargo Electronics
Cathy Medich, Smart Card Alliance
Bob Merkert, SCM Microsystems
Ram Mohan, Northrop Grumman
Dwayne Pfeiffer, Northrop Grumman
Roger Roehr, BearingPoint
Paul Russell, Lenel
Steve Rogers, Integrated Engineering
Mike Sulak, U.S. Dept. of State
Lars Suneborn, Hirsch Electronics
Beth Thomas, Honeywell
Robert Van Spyk, U.S. Dept. of Defense/DMDC
Eric Widlitz, HID Corporation
Greg Yarus, Saflink

About the Smart Card Alliance Physical Access Council

The Physical Access Council is one of several Smart Card Alliance Technology and Industry Councils, which are focused groups 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 AMAG Technology, BearingPoint, CoreStreet, General Services Administration (GSA), Hirsch Electronics, Identification Technology Partners, Integrated Engineering, LEGIC Identsystems, NASA, Northrop Grumman, Saflink, and SCM Microsystems. 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.

A Appendix A: Use Case Scenarios for Alternative Biometric Implementations

The scenarios in this appendix illustrate additional ways in which the identity of the cardholder can be authenticated during access by using the alternative biometric paradigms or methodologies as described in SP 800-76 Section 1.2. FIPS 201 allows a wide range of security policies, from simple visual inspection of the card to multi-factor authentication using a PIN and biometric. Thus, actual implementation approaches are determined by individual agency policy. The policy for access to a library may, for example, specify minimum requirements, whereas policy for a secure location may specify several levels of security

The scenarios below only apply to using the PIV card for physical access. This document and FIPS 201 are silent on other applications that agencies may place on the card for their own use. FIPS 201 specifies that only the PIV applets are inviolate.

NIST presents basic authentication use cases in SP 800-73, Appendix C as follows:

PIV Authentication Mechanism	Card Validation Steps (CardV)	Credential Validation Steps (CredV)	Cardholder Validation Steps (HolderV)
PIV Visual Authentication	1. Counterfeit, tamper and forgery check	1. Expiration check	Possession of card Match of card visual characteristics with cardholder
PIV CHUID		Expiration check CHUID signature check (optional)	Possession of card
PIV Biometric (Unattended)		Expiration check CHUID signature check (optional) PIV biometric signature check (optional)	Possession of card Match PIN Match holder's biometric with PIV biometric
PIV Biometric (Attended)		Expiration check CHUID signature check (optional) PIV biometric signature check (optional)	Possession of card Match PIN Match of holder's biometric to PIV biometric *in view of attendant*

A.1 Alternative Use Case 1: Store Biometric Off-Card

In this scenario, agency-specific enrolled biometric data (e.g., face, fingerprint, iris, hand geometry) for each employee or contractor is stored in an agency-controlled data repository (e.g., PACS server, control panel or reader) and the biometric is matched off of the PIV card in a device or server. The CHUID read from the contactless PIV card acts as a reference pointer to the specific biometric data to be matched for user authentication. Matching can take place at the PACS server, control panel or reader, all of which may be at a different location from where the biometric data is stored.

In this case, no card-resident biometric data is used during the authentication process although it will be present in the PIV container on the card. Thus, any biometric technology may be used in this scenario. Interoperability is achieved since any agency-issued PIV card can be used for access control once the user has been registered in the agency's PACS along with the user's agency-specific biometric data.

For those agencies that choose to use biometrics stored off of the PIV card for access control, the scenario steps would be as follows:

1. The cardholder places the PIV card in close proximity to the contactless entry control device.
2. The CHUID is read from the PIV card contactless interface.
3. CHUID identifiers are passed to the reader and control panel for the authorization check.
4. The biometric sample is collected from the cardholder. (Any type of biometric may be used.)
5. The biometric sample is matched with enrolled biometric data stored in the agency data repository. Matching takes place outside of the PIV card (either on a server, control panel or other device).
6. If authenticated, access is granted based on access rights assigned to the cardholder.

If a server or control panel is used to store the enrolled biometric data, network connectivity is required to transmit the biometric data for matching. It is recommended that the biometric data repository reside within each facility to avoid delays from network latency or service interruptions that may affect a wide area network.

There is a related scenario for initially processing visitors with PIV cards issued by other agencies, where the visitor is seeking unescorted facility access at the host agency. The visitor arrives at a visitor control center to be verified and registered into the PACS. This scenario assumes that the visitor has a host agency sponsor who has notified the security office in advance that the visitor should be granted unescorted facility access. This scenario could use the following process:

1. The cardholder places the PIV card in the contact reader in the security office.
2. The cardholder enters the PIN on the keypad or keyboard.
3. A fingerprint sample is collected from the cardholder.
4. The fingerprint sample is matched with the enrolled fingerprint templates stored in the PIV card. Matching takes place outside of the PIV card in the security office computer.
5. The PIV certificate is checked with issuing agency to determine if the PIV card is still valid.
6. If the fingerprint is authenticated and the PIV card is still valid, selected data from the CHUID is entered into PACS access control list.
7. The visitor's biometric is enrolled into the PACS (e.g., face, fingerprint, iris, hand geometry). If the agency uses FIPS 201-standard fingerprint templates as the agency-specific biometric data, then the visitor does not have to enroll the biometric. The templates from the visitor’s PIV card can be copied and placed into the PACS data repository.
8. The visitor can now use the PIV card for unescorted facility entry.

The above scenario provides a high level of access control assurance using biometrics while protecting the privacy of the biometric data. It also avoids the requirement for contact reader use and PIN entry to access the fingerprint data stored on the PIV card. Agency policy may also allow lower levels of access control.

A.2 Alternative Use Case 2: Store Biometric On-Card in an Agency-Specific Container

In this scenario, agency-specific biometric data (e.g., face, fingerprint, iris, hand geometry) for each employee or contractor is stored on the PIV card in an agency-specific non-PIV-applet data container. Biometric matching can take place either on the PIV card (match-on-card) or off of the PIV card in a device such as the smart card reader. Any biometric technology can be used in this scenario. However, this approach is <u>not</u> interoperable with cards issued by other agencies since it is assumed that the visiting agency will not permit the host agency to write its biometric data container to the visiting agency employee's PIV card. This alternative biometric paradigm is permitted under FIPS 201 as referenced in Section 2.1 of SP 800-76.

This scenario could use the following process:

1. The cardholder places the PIV card in close proximity to the contactless entry control device
2. The CHUID is read from the PIV card contactless interface.
3. CHUID identifiers are passed to the reader and control panel for the authorization check.
4. The biometric sample is collected from the cardholder.
5. The biometric sample is matched with biometric data stored in the agency-specific container on the PIV card. Matching can take place outside of the PIV card (e.g., at the card reader) or within the smart card chip using match-on-card algorithms also stored in the agency-specific container on the PIV card.
6. If authenticated, the FASC-N is assembled and sent to the PACS for the access decision based on access rights assigned to the cardholder.

It is important to note that it is recommended that biometric data transferred between the card and the reader be cryptographically protected to ensure the privacy of the cardholder's biometric data.

There is a related scenario for initially processing visitors with PIV cards issued by other agencies where the visitor is seeking unescorted facility access at the host agency. The visitor arrives at a visitor control center to be verified and registered into the PACS. This scenario assumes that the visitor has a host agency sponsor who has notified the security office in advance that the visitor should be granted unescorted facility access. This scenario could use the following process:

1. The cardholder places the PIV card in the contact reader in the security office.
2. The cardholder enters the PIN on the keypad or keyboard.
3. A fingerprint sample is collected from the cardholder.
4. The fingerprint sample is matched with the enrolled fingerprint templates stored in the PIV card. Matching takes place outside of the PIV card in the security office computer.
5. The PIV certificate is checked with issuing agency to determine if the PIV card is still valid.
6. If the fingerprint is authenticated and the PIV card is still valid, the cardholder is issued a visitor smart card that has its own unique identifier number or that uses the visitor’s PIV card CHUID data.
7. The visitor-unique number is entered into the PACS access control list.
8. The visitor's biometric is enrolled (e.g., face, fingerprint, iris, hand geometry) and the resulting biometric templates are stored in an agency-specific container in the visitor smart card. If the agency uses FIPS 201-standard fingerprint templates as the agency-specific biometric data, then the visitor does not have to enroll the biometric. The templates from the visitor’s PIV card can be copied and placed into the agency-specific container on the visitor smart card.
9. The visitor can now use the visitor smart card for unescorted facility entry.

The above scenario provides a high level of access control assurance using biometrics while protecting privacy of the biometric data. It also avoids the requirement for contact reader use and PIN entry to access the fingerprint data stored on the PIV card. However, this scenario is not interoperable with PIV cards issued by another agency and requires the use of a visitor PIV card for access control.

B Appendix B: External IT Infrastructure Systems

HSPD-12 requires secure smart card issuance and usage as defined in the FIPS 201 standard. FIPS 201 consists of two parts – PIV I and PIV II – and is being implemented in two phases. The standards in PIV I support the control objectives and security requirements described in HSPD-12. These describe a set of procedures to establish the true identity of each Federal employee and contractor. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal PIV system. In this second phase, a fully operational system is required to produce PIV cards with PIN-protected biometric data and PKI certificate, as well as other user and agency specific data.

Components of the PIV-compliant identity system are:

- The identity management system (IDMS)
- The card management/issuance system (CMS/CIS)
- PIV card
- The public key infrastructure (PKI), providing information security
- The online credential status protocol (OCSP) server and the credential revocation list (CRL), providing assurance that only users with valid certificates can use the system
- The local physical access control system, PACS, which uses the PIV card to determine physical access rights for cardholders based on agency policy

This appendix is intended to provide a high-level overview of these systems and the data flow. Other industry and government groups are creating interoperability standards for these back-end system processes.

HSPD-12 and FIPS 201 create a chain of trust for the identity proofing and verification processes and require the deployment of an identity credential – the PIV card – that can be rapidly authenticated electronically. In order to maintain this chain of trust, the status of a PIV card must be verified with the issuing organization before the cardholder is enrolled in the PACS. The status should be verified at regular intervals.

PIV cards are used by cardholders during registration, authorization, and daily use to access facilities. Card issuance systems (CIS) and relying party usage systems need to be in constant communication since the issuer needs to be able to change or revoke the card, and the relying party must be able to determine that the card has not been revoked. Thus, both the issuer and relying party depend on a complex set of networked systems to provide the level of security required by FIPS 201.

The Federal Smart Card Interagency Advisory Board (IAB) has established the Backend Authentication Scheme Work Group (BASWG) and assigned it the task of addressing the issues of back-end authentication among PACS, other entities and the PIV card issuer. The BASWG has also been tasked to develop the proposed technology infrastructure to support this requirement. This group has proposed different methods for accomplishing the status verification process among systems, including:

- Use of the online certificate status protocol (OCSP). With this methodology, the PIV card PKI authentication certificate is used to check the status of the card. A copy of the credential certificate can be stored locally in the PACS or other system and periodically verified with the issuing authority OCSP responder.

- Use of a gateway with online, networked XML-based infrastructure. With this more robust approach, web services and XML-based documents are used to check the status of the PIV card. This check could be done independent of the card and would require the PACS to contact the issuer's hosting site.

B.1 PIV Card Issuance Considerations

This section includes some of the first questions that need to be answered to prepare the IT infrastructure for FIPS 201-compatibility.

PIV cards must be personalized with identity information for the individual to whom the card is issued. Federal departments and agencies may use other accredited issuers to personalize and produce identity credentials for Federal employees and contractors until a government-wide PIV accreditation process is established

High-level considerations include the following:

1. Does the agency want to be an issuer or want to join with other agencies for card issuance? For in-house issuance, is there an existing public key infrastructure in the agency? Can the existing PKI components (certificate authority, validation authority, application plug-ins, desktop OCSP client software, OCSP responder infrastructure) be identified?
2. Should the agency create an agency-specific issuance system or should a commercial CMS/CIS be acquired? Creating a unique CMS/CIS has proven to be difficult and complex. Being an early adopter of CMS/CIS systems can create uncertainties since these are new systems that are still evolving.
3. Should the agency use its own data source or another's data source? Few authoritative personnel data repositories exist, and biometric data, in particular, has not been captured consistently.
4. Does the agency have the management and operational expertise to operate and maintain complex secure systems?

For outsourced card production and issuance, a qualified and approved shared services provider (SSP) can be selected from the government's approved list located at http://idmanagement.gov/.

By using an SSP, the agency does not have to host the PKI infrastructure (or at least the parts of it that produce private keys). Most equipment used in producing private keys require a hardware security module, need to be physically and electronically protected, must operate to a service level agreement (SLA), and need hot, geographically dispersed back-up systems. The value proposition of an SSP to an agency is the ability to provide a full range of PKI services, 24x7x365, year after year.

PKI shared service providers can provide Federal agencies the following services:

- Certificate authority (CA) services supporting certificate issuance, suspension and revocation.
- Certificate lifecycle management services including registration authority (RA) services that work with the agency's card management system (CMS).
- Certificate revocation status publication in accordance with the Federal PKI Common Policy Framework.
- Online certificate status service, which includes the OCSP service and certificate lookup service, allowing PKI relying parties within Federal agencies to inquire about the status of PIV certificates as mandated by FIPS 201 and the Federal PKI Common Policy Framework.
- Key recovery services, including escrow services, as required by agencies.
- Provision of digital signatures for some of the non-certificate components on the card. The CHUID, fingerprint templates and facial image all require digital signatures to establish and maintain the integrity of the data.

In addition, using the optional card authentication certificate (which could be used for high assurance by the PIV card's contactless interface) could be generated by the SSP's certificate authority. The SSP is valuable for providing these certificates for PACS applications, in addition to providing the PIV authentication certificate and the related certificate status information.

There are two types of SSP, the original set of SSPs and those that are now being selected by GSA. The new SSPs will support end-to-end credential issuance that includes all of the capabilities outlined in this section.

B.2 PACS Connection to PIV Infrastructure Example

Figure 1 illustrates an example of the PIV infrastructure and connection to support PACS. These capabilities include:

- Secure servers for personnel enrollment and registration
- PACS readers and their components for daily access
- Communication with the external PIV IT infrastructure
- Secure internal network

B.3 Usage Considerations

The details of how the PACS will be implemented should be considered. Key questions include:

1. What is the visitor management process and is there an automated system?
2. What is the process for physical access authorization?
3. What is the process for access usage and usage revocation?
4. What is the process for reporting problems to the issuer if the card was not issued by the host agency?
5. What is the process for back-end validation of PIV card status?

Figure 2 illustrates the process that an issuer can use to parse a request for credential validation from a relying party. The issuer, at top left, processes the request. The issuer is the only entity that knows the validity of a PIV card. The result is a yes/no decision, shown at the right top of the illustration.

Figure 1: Example of IT Capability Supporting a Physical Access Control System

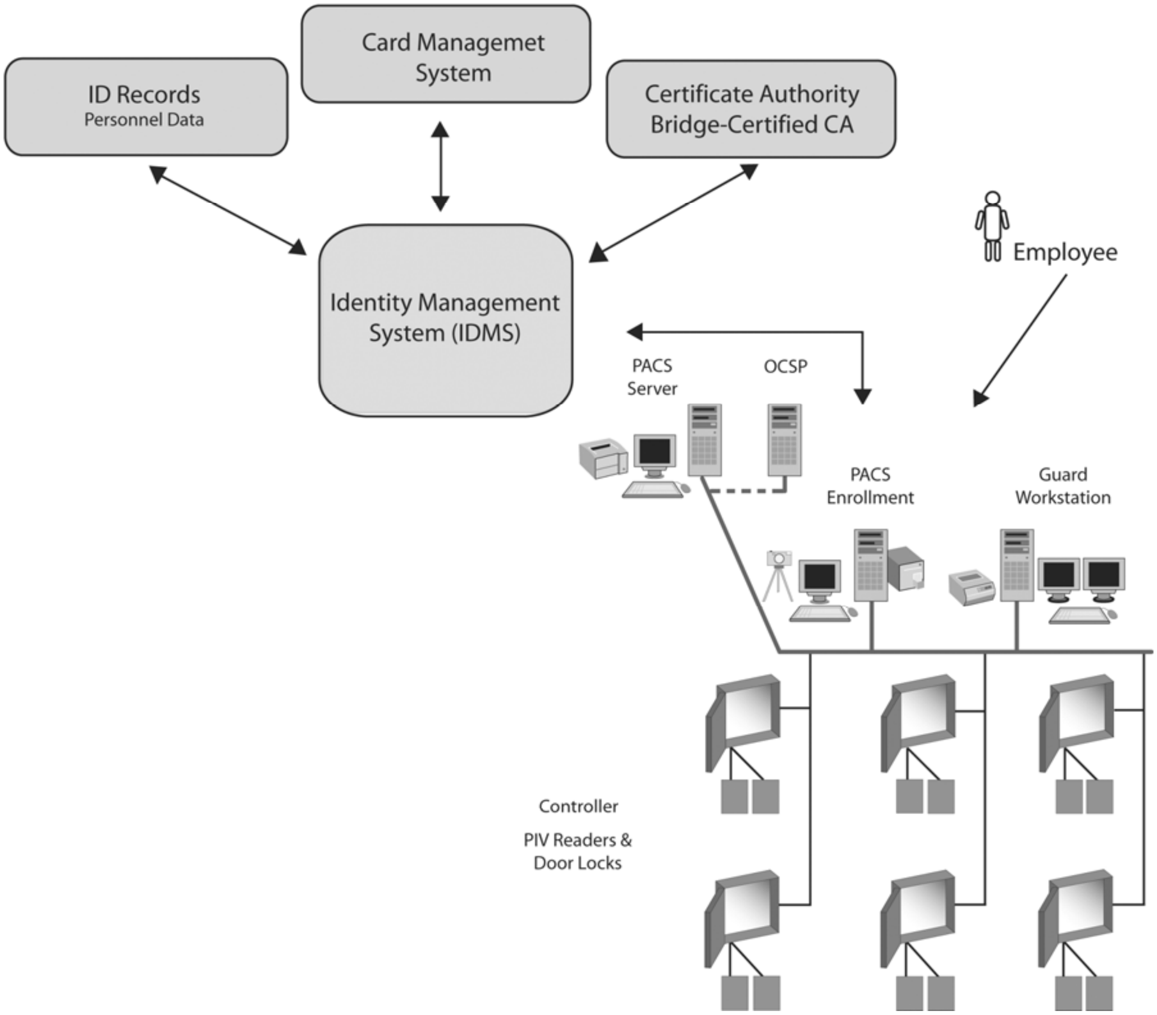
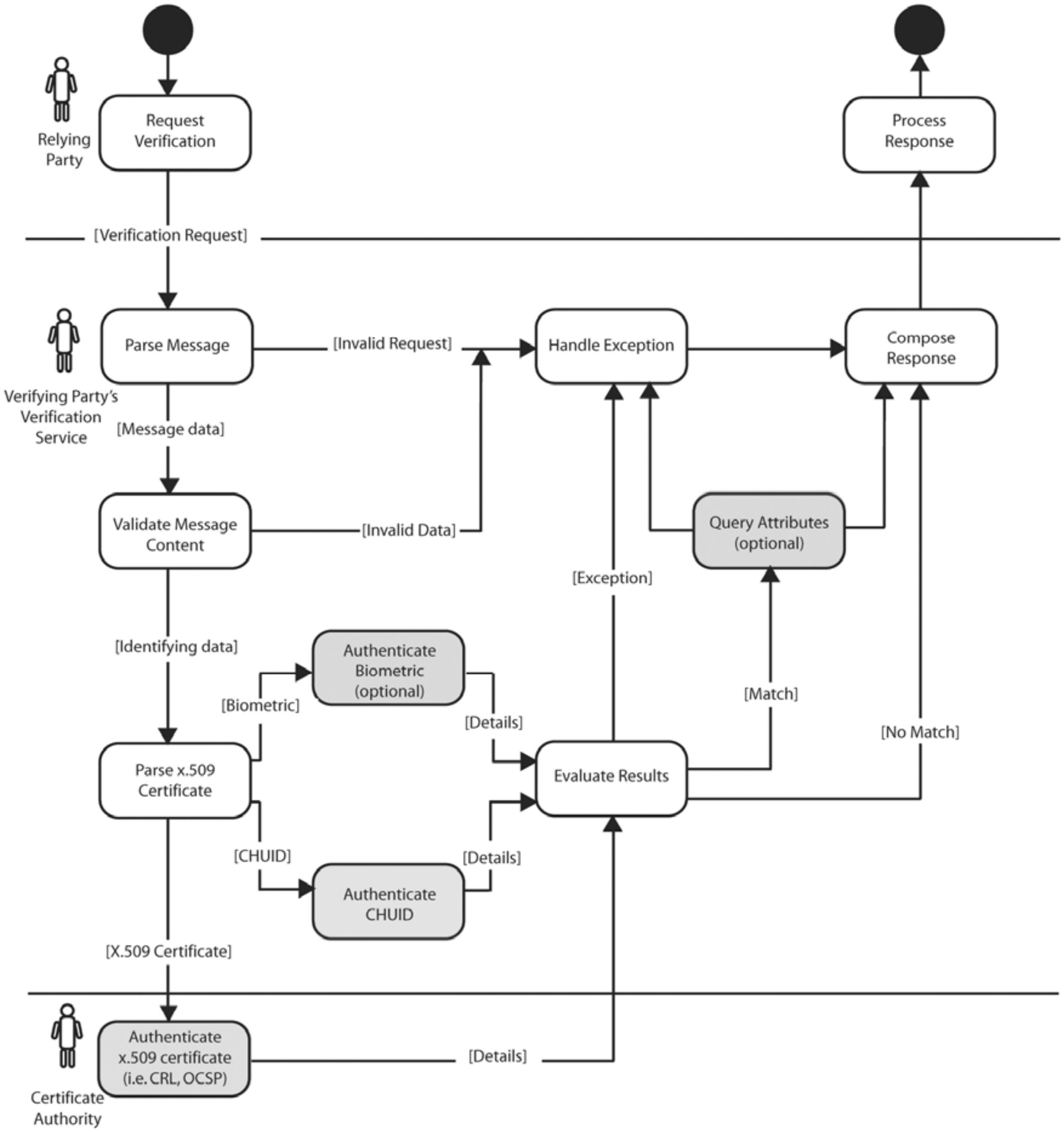


Figure 2: PIV Issuer Verification Process



UC A.2.1	Verifying party may choose to receive and authenticate biometric data or return biometric data which the relying party's system can assess
UC A.2.2	Authentication of the x.509 certificate
UC A.2.3	Authentification of the CHUID at the verifying party's authoritative data source

C Appendix C: References

Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004). Mandates the establishment of a standard for identification of Federal government employees and contractors and requires the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems.
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

Federal Information Processing Standard (FIPS) 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors (June 2006)
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004). Provides a process for achieving FISMA compatibility.

- NIST SP800-37: Security Control Assessment. Determines the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of SP800-53A.
- NIST SP800-37: System Authorization. Determines the risk to agency operations, assets, or individuals and authorizes information system processing.
- NIST SP800-37: Security Control Implementation. Implements security controls in new or existing information systems.

http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

NIST SP 800-53: Recommended Security Controls for Federal Information Systems (February 2005). Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system.
http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1

NIST SP 800-53 Revision 1: Scheduled for publication in late 2006. Establishes methods and procedures to assess security controls.
http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf

NIST SP 800-70: Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers (May 2005). Provides an overview of the security requirements for the information system in a security system plan and documents the security controls planned or in place.
http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf

NIST SP 800-73-1: Interfaces for Personal Identity Verification, 2006 Edition (April 2006). Technical support documentation for FIPS 201.
http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf

NIST SP 800-76: Biometric Data Specification for Personal Identity Verification (February 2006)
http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf

NIST SP 800-78: Cryptographic Algorithms and Key Sizes for Personal identity Verification (April 2005).
http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

NIST SP 800-96 (second draft): PIV Card / Reader Interoperability Guidelines (July 2006).
http://csrc.nist.gov/publications/drafts/800-96/2nd_draft-SP800-96-072706.pdf

OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

OMB M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf

OMB M-03-22: OMB Guidance for Implementing the Privacy Provisions the E-Government Act of 2002
http://www.whitehouse.gov/omb/memoranda/m03-22.html

OMB M-04-04: E-Authentication Guidance for Federal Agencies and NIST Special Publication 800-63, **Electronic Authentication Guideline**: Recommendations of the National Institute of Standards and Technology
http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3, Physical Access Interagency Interoperability Working Group (PAIIWG) of the Government Smart Card Interagency Advisory Board (IAB) (December 2005)
http://www.smart.gov/iab/documents/PACS.pdf

GSA FIPS 201 Evaluation Program: Attestation Form for Transparent Reader. Form used to assert that the reader product being submitted for FIPS 201 conformance evaluation is accurately meeting the requirements stated in the standard.
http://fips201ep.cio.gov/index.php

GSA FIPS 201 Evaluation Program: Transparent Reader Approval Procedure Version 3.0.0 (June 30, 2006)
http://fips201ep.cio.gov/index.php

D Appendix D: FIPS 201 Physical Access Control System Site Survey Worksheet

DOOR DESCRIPTION: ________________________________

DOOR CONTROL PANEL DATA

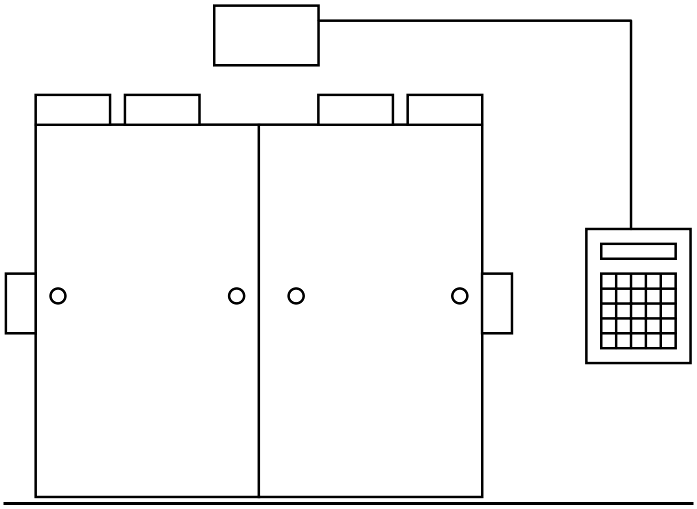
Manufacturer	Location	Panel Lock Code
Panel Type	Primary Communication Type	Reader Interface
Firmware Version	Backup Communication Type	
Serial Number	Panel Database	

DOOR READER DATA

# of Readers	PIN Keypad	Reader Footprint (size)
Reader Type	Biometrics	Mounting (mullion, box, surface)
Reader Technology	Wiring Available	
Reader Output	Wiring Used	

DOOR SECURITY LEVEL

Card Only	Assurance Level	CCTV
Card + PIN	Duress	Guard Post
Card + Biometrics		Intercom Station



Draw Hardware Locations and Notes Above

High Frequency Usage
Medium Usage
Low Usage
Access One Side
Access Both Sides
Door Position Switch
Power Supply
- Mains
- Battery
Lock
- Electric Strike
- Magnetic Lock
- Electrified Lock
Exit Device
- Egress Switch
- Motion Detector
Existing Wiring
- Plenum
- Shielded

NOTES:

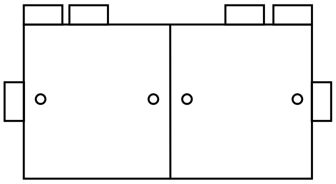
1)
2)

Date:	Building:
Survey By:	Floor:
Contact:	Room:
Phone #:	Door #:
Page:	Of:

READER #1

Recommendations: ____

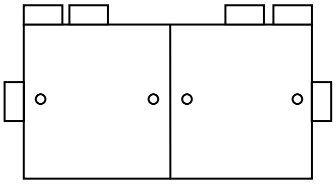
Usage:
High_____ Medium_____ Low______
Day _____ Night________ Weekends_____
Security Level _____________
Free Exit______ Need Card to Exit__________
Fire Exit (Refer to local codes) _________________
Photo Attached_____________________________



READER #2

Recommendations: ____

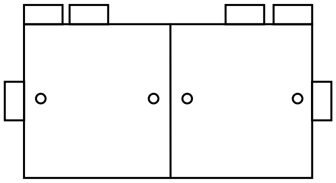
Usage:
High_____ Medium_____ Low______
Day _____ Night________ Weekends_____
Security Level _____________
Free Exit______ Need Card to Exit__________
Fire Exit (Refer to local codes) _________________
Photo Attached_____________________________



READER #3

Recommendations: ____

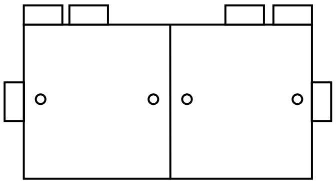
Usage:
High_____ Medium_____ Low______
Day _____ Night________ Weekends_____
Security Level _____________
Free Exit______ Need Card to Exit__________
Fire Exit (Refer to local codes) _________________
Photo Attached_____________________________



READER #4

Recommendations: ____

Usage:
High_____ Medium_____ Low______
Day _____ Night________ Weekends_____
Security Level _____________
Free Exit______ Need Card to Exit__________
Fire Exit (Refer to local codes) _________________
Photo Attached_____________________________



E Appendix E: 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).

Application programming interface (API)
The interface a computer system, library or application provides in order to allow requests for services to be made by other computer programs, and/or to allow data to be exchanged.

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.

Authentication
The process of establishing confidence of authenticity; in the context of 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.

Card
Under FIPS 201, an ID badge that contains within it an integrated circuit chip. Also known as a smart card.

Cardholder
An individual to whom a PIV card was issued.

Card management system (CMS)
A Web-based smart card/token and digital credential management solution for enterprises that is used to issue, manage, and support cryptographic smart cards and PKI certificates for identity-based applications throughout the organization.

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.

Certificate
See digital certificate

Certificate authority (CA)
A trusted entity that issues and revokes public key certificates.

Certificate revocation list (CRL)
A time-stamped list of certificates that have been revoked by a certificate authority (CA). A certificate that is found in a CRL might not be expired, but is no longer trusted by the certificate authority that issued the certificate. The certificate authority creates the CRL that contains the serial number and issuing CA distinguished name of the certificate that has been revoked. The CA might add the certificate to the certificate revocation list if it believes that the client certificate is compromised. The certificate revocation list is maintained and issued by the certificate authority.

Certification
The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

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 rights, privileges or evidence of 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
A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Digital certificate
A portable block of data, in a standardized format, which at least identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certificate authority issuing it.

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*.

IAB
Government Smart Card Interagency Advisory Board.

ICC
Integrated circuit card

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, the ability for 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 (or issuing authority)
The organization that issues the PIV card to an individual after identity proofing, background checks and related approvals have been completed. 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.

Model
A 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.

NIST
National Institute of Standards and Technology

OCSP
Online Certificate Status Protocol. An online protocol used to determine the status of a public key certificate.

Off-card
Refers to data that is not stored on the PIV card or to a computation that is not performed by the integrated circuit on the PIV card.

On-card
Refers to data that is stored on the PIV card or to a computation that is performed by the integrated circuit chip on 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
The 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.

Population

The set of users for an application.

Public key certificate (**or digital certificate**)
A certificate which uses a digital signature to bind together a public key with an identity (e.g., information such as the name of a person or an organization and their address). The certificate can be used to verify that a public key belongs to an individual.

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.

Smart card
A device that includes an embedded integrated circuit 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.

Template
Biometric data after it has been processed from its original representation (using a biometric feature extraction algorithm) into a form that can be used for automated matching purposes (using a biometric matching algorithm). Biometric data stored in a template format cannot be reconstructed into the original output image.

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.

Validation
The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification
See identity verification.