Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials

Developed by the
Smart Card Alliance Physical Access Council
in collaboration with the Open Security Exchange,
Security Industry Association, and
International Biometric Industry Association

V17 – September 5, 2007
FINAL DRAFT - SUBJECT TO BOARD APPROVAL

- Includes final edits discussed during the 9/5 review call
- Logos of all 4 orgns to be added. Final layout to be done in parallel with approval process

Table of Contents

1 Introduction

All federal government employees and contractors are now transitioning to FIPS 201-1 compliant credentials (the Personal Identity Verification card, known as the PIV card). This presents unique challenges to security directors with currently-deployed ID badges and existing systems for building access management and control. Key questions that may be asked by all security directors and those responsible for physical access control systems are:

- Will what I have today work with the new directives and requirements? If not, what can I do to comply?
- How do I take advantage of the enhanced security technology in a FIPS 201-1 credential to improve my organization's security profile?

The answers to these common questions depend on many factors. Compliance methods range from visual presentation and validation of the new PIV card (a minimal process with high risk), to the trusted process using the PIV card for fast, electronic authentication through the public key infrastructure (PKI) and a multi-factor reader or handheld device. Beyond reading the PIV card, field devices, the associated network and cabling, intermediary hardware or control equipment, host computers, and processes may be affected by new technologies used by the PIV card.

Given the scope of an enterprise, federated and converged security system, it is thus very important for a security director, facilities manager or systems manager to understand the changes introduced by PIV cards and determine how to manage change for success. Understanding what will maximize the return on investment and mitigate the risks going forward of “failure of operation” or “failure to comply” is critical to success. It is expected that corollary questions are “how much of my existing system can I reuse” – i.e., how can I mitigate costs, permitting a migration strategy to be implemented – and optionally “how can I use the same method of authentication for physical access and logical access?”

Simply stated, a migration strategy is a series of steps in a particular direction leading to a final objective or goal. The final migration goal for Federal agencies is to achieve FIPS 201-1 compatibility and interoperability by fully using the PIV card within a physical access control system (PACS). There are a number of migration steps that an agency can take to move toward this goal, while also improving security for the organization. The PIV card enables agencies to implement a range of identity authentication methods, allowing the method appropriate to an agency's risk assessment and security requirements.

This white paper describes key elements of a typical access control system, identifies migration considerations relative to each, and outlines different migration options and their benefits and challenges. The white paper also discusses options for integration, PACS enrollment and registration, and biometrics.

2 PACS Migration Considerations

The PIV card uses smart card technology and a data model that is significantly different from traditional physical access tokens. These differences may require changes to the PACS and related components as described in this section.

Whether the facility is considering upgrading an existing PACS or procuring a new system, certain operational parameters are crucial for a successful outcome. These are discussed in detail in the white paper, "Considerations for the Migration of Existing Physical Access Control Systems to Achieve FIPS 201-1 Compatibility," published September, 2006 by the Smart Card Alliance Physical Access Council.[1]

Today, a PACS consists of four major components. Starting from the center and working toward the edge, the first component is a PACS server, the second component is the access or area control panel, the third is a reader or combination multi-factor reader with keypad and/or biometric that can read the card, which is the fourth component.

Any migration strategy must consider that the PACS solution in place may already be tightly integrated with other control technologies, such as: intrusion detection systems, video monitoring and alarm/response management.

Each of these system components is affected by the introduction of HSPD-12 and FIPS 201-1. This section includes a short explanation of the basic functions of each of these vital components and important factors that must be considered when migrating from an existing physical access solution to the use of a PIV card for physical access.

It is also important to remember that these activities involve several stakeholders, each with some level of jurisdiction in the process. Facilities, IT, and security staff members must co-operate as a team to ensure the migration process is as smooth as possible.

With FIPS 201-1, PACS must now work in coordination with the credential issuance infrastructure in those cases where the PACS does not issue the credential. This requires interfaces with new identity system components, pulling information into the PACS as opposed to creating information about identities. This also requires a separation of the functions around creating an identity with those around assigning associated privileges with identities and tracking the actions of individuals associated with those credentials.

2.1 PACS Server

Traditionally the access control server is an administrative tool used by the PACS operator to provision a variety of physical and logical access control resources, journal all system activities, and execute business logic related to alarms and other events collected via data sensors. The access control server is also typically the primary means to register and enroll a cardholder's name, access privileges, and expiration date in the physical access control system. The server downloads cardholder unique identification data, access level and authorized function(s) to the relevant access control panel. It also allows a system operator to temporarily assign a credential and access privileges to a visitor or to an employee who accidentally forgot or misplaced the permanent credential.

For physical access to facilities, an individual's identity has traditionally been authenticated locally by using paper or other hand-carried credentials, such as driver's licenses and ID badges. Once confirmed, identity data about the individual is entered into the PACS database and management authorizations are confirmed for access to areas in the facility. With few exceptions, a local PACS operator registers and revokes user access privileges manually at the PACS server. FIPS 201-1 defines tools for automated authentication, validation and revocation procedures for a PIV

[1] "Considerations for the Migration of Existing Physical Access Control Systems to Achieve FIPS 201-1 Compatibility," is available on the Smart Card Alliance web site at http://www.smartcardalliance.org.

credential. A PACS may be connected to the federated IT infrastructure, enabling automation for these processes using federated ID services. Alternatively, an agency may define compliant manual validation and revocation procedures.

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

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

The consequence in a PACS server is that each user may be entered twice, once with the data read from the legacy card and once with the data read from the PIV card. Some PACS server databases are capable of registering multiple credentials for the same individual, while others may require a separate user record for each credential, even when they belong to the same individual.

Key considerations for migration of PACS servers include:

- Determine if the currently installed server database can be integrated with the agency IT systems to enable federated ID services (including smart card log-on).
- Determine if the PACS server database supports, or can be upgraded to support both existing cards and PIV cards simultaneously.
- Determine if the PACS server can be upgraded to communicate with an online certificate status protocol (OCSP) or certificate revocation list (CRL) service to check the validity or revocation status of credentials.

2.2 Area Control Panels

The control panel is clock synchronized and connected to the access control server, card reader/ keypad and door hardware. It contains a number of user records, usually one per cardholder. Content of the user records varies greatly from one manufacturer to another; however, the basic information is similar among most systems. The panel receives the information from the card reader and compares this to data stored in its local database. Once the control panel determines that the data is valid, it compares this against access privileges registered to the cardholder and makes an access decision. This decision is based on credential revocation status, day of the week, time of day, door location and so on. The control panel sends the decision result to the access control server for display and archiving. When the panel makes an access grant decision, it sends a signal to release the locking mechanism and disarm associated alarm sensors, such as door position monitors.

Numbering systems. The FIPS 201-1 specification does not allow locally-defined or vendor-defined facility codes or system codes commonly used in legacy PACS. The PIV card uses a government-wide Federal Agency Smart Credential Number (FASC-N) that enables cross agency interoperability without credential number conflicts among agencies. As a result, PIV cards will not work unless legacy numbering associated with the cardholder is modified to replace the facility code and system code numbering method with the FASC-N system. During a transition period it may be necessary for the PACS controller to process data from legacy cards as well as from PIV cards.

User records. PIV user records stored in the control panel require additional memory space to accommodate the larger amount of data required for each user in FIPS 201-1 compliant systems.

Details on the data required are found in *section 8.3 The Card Holder Unique Identifier (CHUID) as the Card Credential Number.*

Key considerations for migration of control panels include:

- Determine if the currently installed control panel can operate, or be updated to operate without facility and system codes.
- Determine if the currently installed control panel is capable of, or can be upgraded to process the data from a reader included on the GSA Approved Products List (APL).
- Determine if the currently installed controller can, or can be updated to process multiple card technologies (existing cards and PIV cards).
- Determine if the currently installed controller can, or may be updated to support the expected user population.

2.3 PACS Readers

The GSA FIPS 201-1 Evaluation Program defines 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 the FASC-N and expiration date to a PACS control panel. This section discusses only the "Transparent" reader type.

The PIV card produces the same output to the reader regardless of what transparent reader type is installed at an access control point. From a practical interoperability perspective, the process of connecting a contactless, contact, or three-factor (card, personal identification number (PIN), biometric) reader to the PACS control panel is greatly simplified as one reader type may simply replace another.

For the past few years several reader manufacturers have produced card readers that are upgradeable to support FIPS 201-1 requirements.

Key considerations for migration of PACS readers include:

- Determine if the currently installed readers are capable of, or may be updated to read, process and send the required data.

2.4 PACS Cards

Essential to the understanding of a PACS is an understanding of the card used to request physical access. In a FIPS 201-1-compatible PACS, the PIV card is the physical artifact issued to an individual that allows the claimed identity of the cardholder to be verified.

FIPS 201-1 requires that the PIV card be a smart card. The card body is similar to a bank credit card and conforms to the ISO 7810 specification. The card must contain both contact and contactless interfaces to a single integrated circuit chip (ICC), known as a dual-interface ICC. The contact interface must conform to the ISO 7816 specification, and the contactless interface must conform to the ISO 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.

The PIV card stores a cardholder photograph, PKI certificates and associated cryptographic keys, biometric data and the cardholder's unique identifier (CHUID). The card enables 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.

Key considerations for using PIV cards with PACS:

- Determine operational use of the card. See section 4.2 for additional detail.
- Determine how to use data stored on the PIV card. Details on the PACS-related data available on the PIV card are found in section 8.3, "The Card Holder Unique Identifier (CHUID) as the Card Credential Number."

- Determine how to take advantage of all of the information on a card including photos, certificates, biometrics and other information.

3 Risk Assessment Related to PIV

Prior to developing a migration plan, a risk assessment must be conducted for each individual Federal government facility or site, taking into account unique missions, threats, crime and surrounding environment. This risk assessment supports the determination of the appropriate DOJ Facility Security Level -- Level V being the highest risk level and Level I being the lowest. In many cases this may already have been established, in which case the servicing security director should possess this information.

Based on the established security level for the given facility, the security director must implement the appropriate security measures for protection. HSPD-12 and FIPS 201-1 support this requirement for varying levels of security or "graduated security." FIPS 201-1 defines graduated security as a security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

3.1 Levels of Authentication

The PIV card supports three factors of authentication to allow security directors to determine what level of authentication they want to use to confirm the identity of a person before they are granted access to an asset:

1. Something you have - PIV card
2. Something you know - PIN presented to the PIV card and/or presented to the PACS system
3. Something you are - Facial photo verified by a human
4. Something you are - Fingerprint verification using the PIV minutiae templates

3.1.1 Something You Have

The PIV card (possession) is the first authentication factor in PIV. The credential FASC-N is available as a free read through the contact or contactless interface. A free read of the CHUID and FASC-N is the fastest method to use for electronic checking, but this information could also be copied to a fraudulent credential. To ensure that a credential is authentic, it is recommended that the readers use a challenge response protocol involving either the PIV authentication certificate or the card authentication certificate. At a minimum, certificate status should be verified to ensure the card is not revoked. The PIV authentication certificate is mandatory and is only available through the contact interface after user PIN verification to the credential. The card authentication certificate is optional, but is available through both the contact and contactless interfaces as a free read. At this writing, some issuers include the card authentication certificate, but it is optional and may not be on all cards.

In order to validate a PIV certificate, the certificate must be checked to confirm that it was issued by a certificate authority that is trusted and that it has not been revoked.

The security director will need to choose the level of authentication needed and balance that with the throughput to be achieved.

3.1.2 Something You Know

For physical access, the "something you know" is a PIN. This may be used to access the PIV contact interface and associated PKI services, or for PACS system verification. When used to access the PIV contact interface, the PIN is tied as an additional factor for electronic authentication based on a mutual authentication protocol involving the PIV authentication certificate.

3.1.3 Something You Are

In a FIPS 201-1 credential two factors determine "something you are:" the facial photograph and fingerprint minutiae templates stored on the PIV card.

Facial photographs (digitally signed) are assumed to be authenticated by humans; the fingerprint minutiae will be authenticated automatically by a fingerprint sensor and related matching software. To access the fingerprint templates, the reader must present a PIN to the card (something you know) enabling "something you are" based on the fingerprint verification.

3.2 Assurance Levels and Authentication Methods

The levels of identity authentication assurance defined within FIPS 201-1 and supported by the PIV card are closely aligned with OMB's E-Authentication Guidance for Federal Agencies, M-04-04.

M-04-04 addresses "identity assurance for electronic transactions requiring authentication" and prescribes a methodology based on the risks and potential impacts of errors in identity authentication. FIPS 201-1 states that those responsible for controlling access to physical resources may use a similar methodology to determine the PIV assurance level required for access to their physical resources. It also allows for the use of other applicable methodologies to determine the required level of identity assurance for their application or system.

For example, the PIV card can be used to authenticate the cardholder in a physical access control environment as a "flash pass" with human guards at checkpoints or through electronic access control points. FIPS 201-1 discusses authentication methods for physical access control systems. Each authentication method can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the federated identity service. These various authentication methods are described in more detail in later sections.

4 Migration Options -- Cards

Each agency will have to determine the PACS infrastructure that is in place today and the needs identified from their risk assessment as defined in Section 3. The next step is to determine the desired agency's end state physical access solution based on the risk assessment. The framework for migration for each agency will be established based on the end state solution and the assurance level required.

There are a number of migration options that could be considered in determining the path for using a PIV card.

4.1 Use the PIV Card as a Flash Pass

FIPS 201-1 includes visual cardholder authentication with the PIV card as an acceptable authentication method. However, it is the lowest level of assurance, "SOME Confidence," which provides only a basic degree of assurance in the identity of the cardholder. Another common term for this visual authentication method is "flash pass." The steps required in this visual authentication process are as follows:

1. The human guard at the access control entry point determines whether the PIV card appears to be genuine and has not been altered in any way.
2. The guard compares the cardholder's facial features with the picture on the card to ensure that they match.
3. The guard checks the expiration date on the card to ensure that the card has not expired.
4. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)
5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)
6. One or more of the other data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Benefits of using the PIV card as a flash pass are as follows:

- Easy to implement because it is the method currently used at many facilities today.
- No need to invest in new technology for physical access control systems and card readers.

Challenges with using the PIV card as a flash pass are as follows:

- Not suitable for rapid or high volume access control.
- No support for the HSPD-12 directive that the PIV card be rapidly authenticated electronically.
- Low resistance to tampering and forgery, which is counter to the HSPD-12 directive that the PIV card be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- High potential for human error.

4.2 Use the PIV Card for Rapid Electronic Verification

The PIV card is designed to enable a fully interoperable cross-agency solution for identity proofing and access control (both logical and physical). This focus on interoperability addresses many concerns that may be identified within an agency where systems are developed and

deployed over time in isolation from each other. The interoperable credential offers a common user experience, no matter what system it is used in, when using the full services of the PIV card.

The PIV card and the federated ID services that support it enable full lifecycle support in PACS for rapid electronic verification and operations. These include:

- Verification of identity and enrollment into the PACS system
- Daily use to enter a building or area
- Revocation of the credential

4.2.1 Enrollment Using PIV Card

Initial identity verification and enrollment are done using the contact interface of the PIV card. The following may be done using the PIV card to verify that the cardholder is who they claim to be:

- Verify the credential is still valid.
  Read the CHUID from the card and validate it is not expired. Read the PIV Authentication Certificate from the card and check its validity against an OCSP or CRL service. Verify the digital signatures of all objects read from the card.
- Verify the PIV card is unaltered/not forged/not copied.
  Use the PIV Authentication Key (and certificate) or the optional Card Authentication Key (and certificate) to perform a challenge response protocol with the card. This verifies that the PIV card actually has valid keys in accordance with their certificates.
- Verify that the individual presenting the credential is the rightful cardholder.
  Have the cardholder activate the card using a PIN and use the fingerprint templates and/or optional facial photograph.
- Acquire the credential number and identity information to be registered into the local PACS.
  Extract the information needed for the local system from the CHUID and the PIV Authentication Certificate (and the optional printed information buffer). Create the local credential number (from the FASC-N or GUID) to be registered into your PACS. Add the identity information to your records for that individual. Use a federated ID service to gain additional information about the individual from the issuing agency to make an access decision.
- Grant access privileges to the cardholder.

4.2.2 Daily Use of PIV Card

The PIV card offers both contact and contactless operations for PACS solutions. The contactless interface provides the mandatory CHUID as a free-read object as well as the optional Card Authentication Key (and certificate). The contact interface offers these same features along with the PIV Authentication Key (and certificate), fingerprint biometrics and facial photograph. Depending on the risk profile for the area or building being controlled by the PACS, all or some of these features may be used by the security director.

In all instances, the PIV card must be checked to see that it has not been revoked by the issuer and that it has not passed its expiration date. This may be done at the PACS server as required by the security policy of the security director. Once the PIV card has been verified as still valid, the following features provide a robust suite to verify that that particular card is being presented (not a copy, clone, forgery) and that the cardholder belongs to that PIV card.

- Contactless operation
  - Read the CHUID.
  - Extract the credential number (from the FASC-N or GUID).

- Optionally, perform a challenge response protocol with the Card Authentication Key (and certificate) if it is present.
- Optionally, verify the digital signatures from the CHUID and the Card Authentication Certificate to ensure they are unaltered.

- Contact operation
  - Read the CHUID.
  - Extract the credential number (from the FASC-N or GUID).
  - Optionally, perform a challenge response protocol with the Card Authentication Key (and certificate) if it is present.
  - Optionally, verify the digital signatures from the CHUID and the Card Authentication Certificate to ensure they are still valid.
  - Optionally, verify the biometric and PIN from the cardholder matches the PIN and fingerprint templates stored on the PIV card

- Per local policies of the security director, an additional PIN or biometric verification may be done by the PACS system, beyond that offered by the PIV card.

- If all operations are successfully confirmed as required for that particular gate/barrier, open the door strike.

4.2.3 Revocation of the PIV Card

There are three issues for revocation when using a PIV card:

- Revocation by the issuer
- Revocation locally when that individual no longer requires access to an area
- Expired card

A federated ID service, such as a validation authority, an OCSP responder, or a CRL mechanism, should be used to validate if the issuer has revoked a PIV card. If revoked, all access privileges should be removed for that individual. It is a local policy decision by the security director to delete the entire record for that individual, or simply remove privileges for that individual.

Local revocation and expiration of a PIV card are local processes that do not involve federated ID solutions. These are typically handled by policy in the local PACS head-end database.

4.2.4 Benefits and Challenges

Benefits of using the PIV card for rapid electronic authentication include:

- Provides full compliance with OMB policy implementing the HSPD-12 directive.
- Enables a single credential within all deployed agency access control systems.
- Protects against fraudulent credentials being used to gain access to buildings and controlled areas.
- Ensures the correct individual is using the credential.

Challenges with this approach include:

- Requirement for a PIV-compatible PACS solution or migration to be available. For example, two-way communications with readers may be required to accommodate the cryptographic challenge and response and other enhanced features.
- Potential for cloned or duplicated cards to be created from a free read of the CHUID. Security directors have the option to use other authentication methods to mitigate this risk (such as PIN to the PACS, biometric match to system, system picture verification and/or cryptographic challenge of the PIV card).

4.3 Issue Two Cards

In some cases, an agency may not have the funding to upgrade or replace their non-compliant card readers or existing PACS components. The agency should define the migration strategy and identify budget resources to enable a migration. Until such funding is available, an agency may continue to use existing cards for enrollment in the PACS. Once identity is confirmed according to the PIV I process, an agency may continue issuing and enrolling legacy technology cards in their PACS.

Benefits of this approach include:

- Continued use of existing PACS cards until funding is available to replace PACS components.

Challenges with this approach include:

- Additional cost of continued issuance of two cards.
- Issuance of PACS cards to partner agency personnel who already have a PIV card.
- The card numbering system commonly used in legacy PACS is designed for a relatively small number of cardholders within a single facility. As an example, a typical legacy card consists of a three digit "Facility Code" (000-255) and a five digit unique card number (00000-65000). The risk of conflicting card numbers within the system increases as the user population grows.
- Some older PACS are unable to process the full 14-digit FASC-N. To enable use of PIV cards, these systems may use a hashing process to reduce the number of digits produced from a PIV card to equal the number of digits produced by a legacy card. This approach greatly increases the probability of conflicts.

4.4 Issue the PIV Card with Additional Technologies

One migration option is to continue to use legacy ID card technology (magnetic stripe, bar code or 125 kHz proximity) by issuing a multi-technology PIV card. Note: at this time Wiegand wire swipe cards are not being supported in multi-technology cards.

PIV cards use 13.56 MHz based on ISO/IEC 14443. Interference can be created by adding multiple 13.56 MHz applications. FIPS 201-1 specifies that additional technologies cannot be added to a PIV card post-issuance.

4.4.1 ISO 7811 Magnetic Stripe

FIPS 201-1 provides a space on the back of the card for a magnetic stripe and most PIV card manufacturers can supply this type of card stock. A security director must coordinate with other sites and numbering sequences to create a numbering system that will not conflict with other legacy cards, or the PIV FASC-N. One solution is to use a different number of digits, such as 11, to ensure differential between legacy SEIWG-encoded magnetic stripes and the 14-digit FASC-N. Other options are to encode the legacy credential number or a new local facility credential number.

Benefits of this approach include:

- Legacy technology remains in place.
- Facilities can use local numbers or FASC-N.
- Facilities can create and encode their own numbering systems using different length numbers to minimize the risk of conflicting card numbers.

- Encoding in accordance with ISO 7811 can be read by any reader conforming to this standard providing a non-proprietary solution.
- Option supports automated checking of the credential.

Challenges with this approach include:

- Some older PACS systems are unable to process the full 14-digit FASC-N. To enable use of PIV cards, these systems may use a hashing process to reduce the number of digits produced from a PIV card to equal the number of digits produced by a legacy card. This approach greatly increases the probability of conflicts between cards of the two formats.
- A magnetic stripe requires physical contact and subjects both the reader and card to wear and tear from use. When the magnetic stripe wears out, card replacement costs are going to be significant for a PIV card.
- Magnetic stripe technology can easily be copied or altered, providing low resistance to cloning, tampering and forgery. This is counter to the HSPD-12 directive that the PIV card be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.

4.4.2 Barcode

The FIPS 201-1 standard retains space on the card for a PDF 417 barcode on the front of the card and 3 of 9 barcode on the back of the card.

Benefits of this approach include:

- Legacy technology remains in place.
- Barcodes conform to standards and provide a non-proprietary solution.
- Facilities can use local numbers or FASC-N.
- Facilities can create and encode their own numbering systems using different length numbers to minimize the risk of conflicting card numbers.
- Barcodes can provide quick non-contact reads for use with automated systems.
- Option supports automated checking of the credential.

Challenges with this approach include:

- Bar code technology can easily be copied or altered, providing low resistance to cloning, tampering and forgery. This is counter to the HSPD-12 directive that the PIV card be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- Tight printing quality control is required to produce a readable barcode. Card production quality check must include barcode testing.
- Barcode is subject to wear and tear and fading; this can be mitigated by laminating both sides of the card.

4.4.3 125 kHz Proximity Technology

125 kHz proximity technology is widely used for physical access. 125 kHz technology can be embedded in the PIV card. The contactless interface of the PIV card transmits at 13.56 MHz and does not interfere with the 125 kHz technology.

Benefits of this approach include:

- 125 kHz technology provides a rapid read with good read ranges.
- Technology required to produce 125 kHz cards is not readily available which makes it harder to duplicate credentials.

- 125 kHz technology is the most commonly installed technology according the Security Industry Association (SIA).

Challenges with this approach include:

- Some older PACS are unable to process the full 14-digit FASC-N. To enable use of PIV cards, these systems may use a hashing process to reduce the number of digits produced from a PIV card to equal the number of digits produced by a legacy card. This approach greatly increases the probability of conflicts between cards of the two formats.
- 125 kHz proximity technology is not standardized, with each manufacturer having a different method for transmitting data. Most manufacturers have different bit outputs that must be programmed in the PACS. Some manufacturers' proximity implementations require that cards and readers be matched, with cards and readers not even interchangeable from the same manufacturer.
- Some proximity technology manufacturers provide PACS integrators with proprietary card formats that require that a licensing fee be paid to the integrator for chips encoded in that format.
- Proximity chip embedding requires minimum orders which can significantly increase the lead time for PIV compliant card stock.
- Encoding the proximity chip may require a separate process in addition to personalizing the PIV card.
- Matching data between the two chips may not be feasible (FASC-N vs. proprietary encoding of proximity chip)
- Agencies with encoding that is copied from the FIPS 201-1 credential number on the smart card chip to 125 kHz chip will need to ensure that the 125 kHz credential numbers used with the 125 kHz proximity system do not collide with FIPS 201-1 credential numbers.
- If the agency does not have uniform agency-wide proximity solution, adding 125 kHz technology may not solve agency-wide deployment issues.

5 Migration Options -- Readers

5.1 Upgrade Firmware in Current Card Readers for FIPS 201-1 Compatibility

Agencies should determine if the currently installed readers are capable of reading, or may be updated to read, both the legacy cards and the PIV cards simultaneously. This would allow for a single reader to process both credentials during the migration process.

Some reader manufacturers offer readers that are designed to be updated in the field through a process that either replaces the firmware completely with an updated version or allows an update to the existing firmware version that would allow migration options for the technology in the reader to perform new capabilities.

Firmware is software encapsulated in hardware that provides instructions to the product on what and how to perform. Firmware updates can be performed in a variety of ways depending on the process selected by the vendor. Examples could include:

- Removing the reader and replacing the electronic chips containing the firmware with new firmware components;
- Removing the reader, electronically performing the update process with a handheld or mobile device, and then remounting the reader;
- Downloading updates electronically from a central point (typically the head-end PACS);
- Performing a contactless transfer process. In this case, a contactless control card is presented to the reader and instructs the reader to "get ready" to accept a new firmware set. The new firmware version is then presented with a card that uses contactless technology to transfer the new firmware version to the reader. The reader is then commanded to return to its normal state.

Whatever method is used, the net result is "new and updated" firmware in the reader which now allows new capabilities to be possible. When a firmware application is updated through a remote download or some other electronic means, it is referred to as "flashing." One note of importance when following this process is to be sure that the firmware version installed in the reader is supported and compatible with the access control panel and associated host software. Otherwise, the update may not work properly or even cause complications.

Benefits of this approach include:

- Reduced cost of not having to replace the readers.
- Assurance of system compatibility.

Challenges with this approach include:

- Logistics for updating the reader. Updating may require physically going to each reader and using a programming card or directly connecting the reader to a laptop or other programming device for the upgrades. Cycling power to the reader may also be required.
- Compatibility among PACS components. Access control panel firmware or software versions in both the access control panel and host software must be checked to confirm that they can support the new reader firmware.

5.2 Use the PIV Card with a Handheld or Desktop Reader for Authentication

Industry has demonstrated that a handheld device can be used not only for authentication of individuals but also to determine their authorizations/roles in order to grant access.

One way an agency may leverage their investment in FIPS 201-1 credentials involves the use of mobile device authentication for such functions as perimeter control, security guard desk, mutual aid and spot checks. The idea is that in lieu of or in parallel to an upgrade to a physical access control system, there exists a migration strategy that uses handheld devices as a means of high assurance authentication of individuals by security professionals. This is an alternative to a "guard and gun" and a "flash pass." Further the solution proposed can deal not only with a given organization's FIPS 201-1 credentials but also with those from other organizations.

Industry has demonstrated solutions that provide strong authentication using up to three different authentication factors found on FIPS 201-1 credentials. In addition these solutions have shown the ability to work with legacy U.S. government smart cards as well as a default credential that employs FIPS 201-1 technology (e.g., FIPS 201, CAC, FRAC, and TWIC).

Solutions have been shown where such handheld devices hold the status of all U.S. government and FIPS 201-1 technology credentials.

Benefits of this approach include:

- Immediate ability to do strong authentication (certificate plus multiple factors) based on PIV card technology.
- Scalability. A single device can hold all FIPS 201-1 technology credentials.
- Resilience. The device can operate without network connectivity in case of communications loss.
- Leverage of existing networks. This option does not require secure connections and can operate with any existing wide or local area networks for synchronization.
- Electronic verification of PIV cards.

Challenges with this option include:

- Requirement for the security officer to operate.
- No support for unattended physical access.

5.3 Replace Current Card Readers with PIV-Compliant Readers

One solution is to replace current PACS readers with readers that only read the PIV card. These could be either contact or contactless readers. Typical PACS readers will take the whole or part of the CHUID (see section 8.3) and send it to the field panel to adjudicate the request for access. For PIV, the minimum fields required to uniquely identify a credential within the FASC-N field of the CHUID are:

- Agency Code -- four (4) decimal digits;
- System Code -- four (4) decimal digits;
- Credential Number -- six (6) decimal digits

If each of these fields is represented in binary number, this would require 48 bits to uniquely identify a credential. Some legacy systems can not handle a credential number of this size.

Benefits of using a PIV reader include:

- This approach ensures that all personnel entering have a PIV card.
- Automated enrollment is simplified.

- Synchronization with the issuing authority for status checks is simplified.
- System installation and cardholder record maintenance is simplified.

Challenges of this approach include:

- All users of the system must be issued a PIV card.
- The PACS must be able to handle 48 bits to ensure unique identification of the Federal Agency Smart Credential Number (FASC-N). When the Global Unique ID (GUID) is used, the PACS will need to handle 128 bits.
- There is the potential for cloned or duplicated cards to be created from a free read of the CHUID. Security directors have the option to use other authentication methods to mitigate this risk (such as PIN to the PACS, biometric match to system, system picture verification and or cryptographic challenge of the PIV card).
- Visitor's cards, if issued to work on the PACS, will need to be encoded with a FASC-N.

5.3.1 Use PIV Card with an Intelligent Reader and Local PACS for Authentication

For those legacy systems that cannot handle the large number that comes from a PIV-compliant reader, two types of intelligent readers have been developed.

The first type of intelligent reader is a hash reader that takes the information from the CHUID and the Card Unique ID (CUID), hashes them, and then sends a small digest to the system. (Note: see Section 3.3 of *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems Version 2.3.)*

Benefits of this approach include:

- This approach allows a legacy system to be used with PIV cards. Hash readers can be of particular use to aid the migration of the PACS to PIV compliance where the perimeter entrances have been upgraded to ensure only unique PIV cardholders gain access, but allow internal PACS components to be changed to support PIV compliance as budget permits.
- The risk of cloning is reduced by using chip-specific information in addition to the FASC-N credential number. Note that the hash can be appended to the normal card read for additional security if so desired by security director and supported by the PACS.

Challenges with this approach include:

- This approach does not ensure unique identification -- i.e., there is a possibility that two credentials with different information will generate the same hash. The probability of collision is 1% with a 32-bit hash when the card population reaches 9,300 cards. As the card population grows or if a shorter hash is used, the risk for conflicts increases.
- All cards at enrollment will have to be read on a reader that performs the hash and the hash will need to be recorded in the cardholder record.

A second type of intelligent reader would take the FASC-N, look it up in a local table stored in the reader, and then send a different smaller number that will work with the installed PACS database.

Benefits of this approach include:

- The legacy system is preserved.
- The approach uniquely identifies the credential to the PACS.

Challenges with this approach include:

- This approach requires a sophisticated read with matching database that could limit the number of users.

- The system administrator will have to manage the CHUID in the reader and ensure that a unique ID is generated for the legacy system.
- This system will require real-time two-way communications to the reader normally done through an IP network.

5.4 Replace Current Card Readers with Multi-Technology Readers

A number of contactless RF reader manufacturers have released PACS readers that can read multiple card formats in 125 kHz (proximity) and 13.56 MHz (contactless smart cards) frequencies. This allows facilities to use their currently issued proximity or legacy contactless smart cards in concert with new PIV cards as they migrate their cardholders from legacy cards to PIV cards.

Benefits of this approach include:

- This option does not require addition of legacy technology to the PIV card. This keeps the card cost minimal and reduces production time.
- This approach allows for smooth transition from legacy technology to the PIV card.
- The cost of multi-technology readers usually adds only 25% or less when compared to the price of a PIV-only reader.

Challenges with this approach include:

- The other components of the PACS system must be able to support the CHUID card format that an agency chooses (see section 8.3).
- The card reader may require a separate power supply.
- A legacy card number could possibly conflict with PIV card number.
- There is the potential for cloned or duplicated cards to be created from a free read of the CHUID. Security directors have the option to use other authentication methods to mitigate this risk (such as PIN to the PACS, biometric match to system, system picture verification and or cryptographic challenge of the PIV card).

6 Integration Options

The security departments of Federal agencies today face the same challenge that commercial enterprises do: converge their information technology (IT), information security (IS), and physical or "traditional" security to jointly develop overarching security strategies. The need to comply with HSPD-12 is forcing Federal agencies to develop migration strategies toward compliance to FIPS-201-1 and adopt a converged solution. Compliance is the primary business driver for Federal agencies. However, there are additional business drivers that may have a greater influence for commercial businesses.

Each group will determine how to reach their desired "end state," by evaluating and prioritizing the various business processes and procedures which control their security functions. Both commercial business entities as well as Federal agencies will establish their priorities from these four categories:

- Compliance
- Asset and personnel protection
- Cost control and productivity
- Business continuity or workflow

Once this step is completed, agencies and business entities can establish a strategic roadmap with tactical goals and operational components.

This in turn enables a decision-making process for technology choices to be based on sound business reasons. Additional information about the business drivers for convergence can be found in the Open Security Exchange white paper, "Physical/IT Security Convergence: *What It Means, Why It's Needed, and How to Get There*"[2].

6.1 Connect PACS to IT Infrastructure

The long-term goal is to have a federated identity infrastructure with a PACS-vendor-agnostic interface capable of interfacing with different PACS databases and database structures across an IT network infrastructure. However, each PACS typically has its own unique method of formatting data and processing and handling user records. Some older systems may be proprietary and have no method to connect to the outside world. Older systems may not work with third party software or other means to manage connection to external system access. Today, no common standard exists to bridge these systems; however both the Security Industry Association (SIA) and other industry organizations are developing common criteria for such interfaces.

A solution to integrate the local PACS with the IT infrastructure should focus on the following areas:

- Confidentiality and integrity
- Scalability
- Flexibility
- Process flow
- Data content

6.1.1 Confidentiality and Integrity

Data security is paramount; information must be maintained securely and access to restricted data must be limited to authorized parties. This may require cryptographic protection for information both at rest and in transit, with policies and procedures in place defining who has rights to access of data. Data transferred and exchanged among the identity management

[2] "Physical/IT Security Convergence: *What It Means, Why It's Needed, and How to Get There*" is available on the Open Security Exchange website http://www.opensecurityexchange.org/.

system (IDMS), a card management system (CMS) and the PACS must be authenticated and validated to prevent a fraudulent system from impersonating a trusted PACS and then gathering secure data. PKI is one technology that can be used to validate the authenticity of the communicating parties.

6.1.2 Scalability

The solution must be able to accommodate a large number of PACS. Communications must exist to deliver the data between systems in a reliable, fault tolerant manner.

6.1.3 Flexibility

The integration solution must have one or more mechanisms to communicate to a wide range of disparate PACS servers. Today this type of integration is done on a project-by-project basis. No uniform standard exists based on accessing information in specific data cells using a standardized index (such as first name, last name, CHUID) As these standards develop they must be flexible enough to respond to a changing environment, including new cryptographic processes and transmission methods and different agency requirements to transmit additional information.

6.1.4 Process Flow

The process flow must be considered when developing a comprehensive integration solution. The information may flow from a central IDMS/CMS to a local PACS, or a local PACS may "reach" for required information. Specific issues for privacy and security must be identified and addressed when the IDMS/CMS is not owned by the agency operating the local PACS.

6.1.5 Data Content

The PACS only needs to receive and transmit the basic information necessary for physical access control purposes. CHUID, first name, last name and expiration date might be all the information needed. Local physical security officers most likely do not need to know a person's Social Security number, have images of their fingerprints, or have any other access to personal information. The photo and other cardholder information might be necessary, or required by specific agency policy. All data content sent to and from the PACS must be access-protected and controlled.

Although the integration solution will be delivered using modern communication technology, the above key points on privacy and security deserve the major focus. Current technology will inevitably be replaced by newer, better technology. Web services may extend current technology to achieve these requirements as they offer the flexibility to interface with different platforms in a secure manner.

Benefits of this approach include:

- Automated certificate validation.
- Automated change of physical access privileges of expired credentials.
- Driver for standardization of PIV IT data exchange processes.

Challenges with this approach include:

- Lack of ability for all PACS to integrate with the IT infrastructure.
- Unknown long-term sustainability, maintenance issues.

6.2 Use Full PKI Infrastructure for PIV-compliant PACS

The PKI infrastructure provides the security director with two core capabilities. First, the PKI infrastructure can be used to check the status of the PIV credential with the issuing authority.

Second, PKI can be used to ensure that the PIV card is genuine by using a cryptographic challenge and response. These checks may be performed together or in a separate process.

Credential authentication occurs when the PIV card is sent data to encrypt with its private key which is stored on the card. The PIV card is authenticated when the encrypted data is correctly decrypted using the card's public key stored in its certificate.

The PIV card includes 4 certificates: digital signature (optional), key management (optional), PIV authentication (mandatory) and card authentication (optional). Since there are three optional certificates and one mandatory certificate, it is important to know which certificates have been included in the PIV card by the issuer in order to take advantage of these features for enhanced security applications. At this time, some PIV card issuers are issuing all four certificates.

Note: Verification of the PIV authentication certificate is two-factor authentication because it requires the PIN. Verification of the card authentication certificate is only one-factor authentication since it is available during a free-read. FIPS-201 was written before SP 800-73-1; at the time of FIPS 201-1 publication, the authors did not know about the free-read card authentication certificate in SP 800-73-1. The PKI authentication definition in chapter 6, *PIV Card Holder Authentication,* of the FIPS 201-1 specification assumes that the PIN is being entered for all PKI authentications. This does not preclude the system from employing other authentication factors.

Benefits of this approach include:

- This approach provides the highest level assurance that a PIV card is genuine and not cloned or forged.

Challenges with this option include:

- The PKI challenge and response can take additional time; security must consider where this level of security is needed for each access point and each access attempt.
- A reader doing a PKI challenge and response could require two-way communications that is not support by the legacy communications infrastructure.

PKI is the only method that is currently defined by FIPS 201-1 for checking the revocation status of PIV credential with the issuer. Two methods for checking the credential's certificate status have been developed: Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). When connecting a PACS to the PKI, different systems will connect with different parts of the PACS. Security directors should understand what part of the PACS server, controller or reader will be connecting to the PKI and ensure that the network is configured to provide those components with the necessary network access.

The CRL is published by the certificate issuer and identifies those certificates that have been revoked. When a credential is enrolled in the PACS, the card PIV authentication certificate should be stored in the PACS or in a middleware program and the certificate's status should be periodically checked with the issuer PKI authority. If the certificate is revoked, privileges for that credential should be revoked.

Benefits of this approach include:

- Relatively inexpensive
- Simple integration to local PACS

Challenges with this approach include:

- Potential for large CRLs or integration with OCSP infrastructures
- A PIV card only supports PKI authentication on the contactless interface with an optional card authentication key that may not be available from all issuers.

7 Migration Options -- Registration and Enrollment

Agencies may choose to implement PACS registration and enrollment in a variety of ways; these are policy decisions and not dictated by FIPS 201-1. This section presents three models for registering or enrolling a PIV card into a PACS, depending on the level of integration that the PACS has with the IT infrastructure.

7.1 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. During registration, the PIV card is inserted into a contact reader connected to an administrative workstation. The user is asked to enter the PIN and place a finger on the sensor for comparison with the enrolled biometric template stored on the PIV card; this authenticates that the user is the valid cardholder. As an option, a fully connected PACS system could also receive a download of 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), including the proper access privileges as predetermined by agency policy.

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

- The new employee is escorted to the local PACS operator. The operator searches the PACS server user database for the correct name that has been downloaded from the agency central IDMS or shared service provider (SSP). Once located and selected, the specific user data is displayed.
- The operator then asks the employee to insert the PIV card into a contact PIV card reader (a PIV-enabled PACS registration station) 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 individual is not yet present in the PACS, the PIV card reader/enrollment station can automatically acquire attributes about the individual through a federated ID service. This would enable population of pertinent fields in the PACS automatically – such as name, title, address, photos, biometric, and policy-driven authorized access points.
- If the person is authenticated as the valid user 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 or using an online certificate status protocol server.
- The reader reads the CHUID components from the PIV card. The components that will create the unique credential number (FASC-N's agency code, system code and credential number or GUID) and expiration date are copied from the CHUID and mapped to the proper fields of the user record in the PACS.
- Next, the server concatenates the 4-digit agency code (AC), 4-digit system code (SC) and 6-digit credential number (CN), to form a unique 14-digit credential number. As an example, this may be AC 1111, SC 2222, and CN 333333 converted to the 14-digit number, 11112222333333. In the future, the server may simply use the 128 bit GUID as the credential number. This credential number is downloaded to the proper control panels as determined by the physical access authorization rights for this user.

- 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 in the case that systems are not connected and automated. The server downloads the credential number to the relevant control panels as the number that will be used to identify the PIV card user's record and access privileges.
- Readers located at each access control point read the PIV card and send the FASC-N and expiration date to the PACS for authorization.

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 credential are archived and properly logged in the history file.

This approach enables an IDMS operator to easily suspend a credential 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.

7.2 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 verifies the access level and areas where the visitor or new employee needs access.
- 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 user of the PIV card.
- If authentication is confirmed, the reader reads the CHUID and sends the CHUID and expiration date to the PACS server.
- The PACS server extracts the GUID or the FASC-N's agency code, system code and credential number.
- The PACS operator selects the authorized access control point(s) from the PACS door list.
- The PACS server creates a new user record with an expiration date and downloads the credential number 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.

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

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 the external IT infrastructure.

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

- Contactless PIV card reader, or
- 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 described above.

8 Other Migration considerations

8.1 Biometrics Authentication

This section describes the considerations and options for using biometric authentication for physical access control if required.

8.1.1 Considerations

Biometric authentication enhances physical security by providing a high level of assurance that the person presenting the PIV card for facility access is, in fact, the person that the card was issued to. This is accomplished by matching a presented biometric sample to an enrolled biometric template. Biometric authentication represents an additional authentication factor when compared to traditional authentication mechanisms, such as something that you have (the PIV card) and something that you know (the PIN). Biometric authentication represents something that you ***are*** and can be used in combination with the other authentication factors to achieve a higher level of assurance.

In FIPS 201-1, it is mandatory that the PIV card memory store two fingerprint templates for interoperability purposes. This fingerprint data can also be used for authentication in a physical access control system by incorporating a fingerprint sensor into the physical access reader. As previously stated, the advantage of biometric authentication is higher level access control assurance. The disadvantage is that biometric technology adds cost to the access control reader device and requires that personnel receive some orientation training in its proper use. Commercial PIV card reader products that incorporate biometric fingerprint sensors are available today and approved by GSA for use in HSPD-12 compliance.

FIPS 201-1 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 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 201-1 and SP 800-73-1, 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.

8.1.2 Implementation Approaches

Option 1 – Use Standard Fingerprint Template on PIV Card

Based on FIPS 201-1 requirements, if the standard fingerprint template stored on the PIV card is to be used for authentication, then the reader must be a contact smart card reader and the PIV cardholder must insert the PIV card into the reader slot and enter their PIN before presenting a finger to the sensor for matching with the templates stored on the PIV card.

The use case scenario steps would be as follows:

1. The cardholder inserts the PIV card into the contact slot on the reader.
2. The CHUID is read from the PIV card contact interface.
3. CHUID identifiers are passed to the reader and control panel for the authorization check.
4. The cardholder enters a PIN to allow the reader to read the biometric templates stored on the card.
5. The user places a finger on the fingerprint sensor which is embedded in the reader.

6. The presented fingerprint is matched with the enrolled fingerprint template(s) read from the card.
7. If authenticated, access is granted based on access rights assigned to the cardholder.

While this option provides strong three-factor authentication, it may not meet throughput requirements for those facility entry points requiring high volume and rapid access. In addition, contact smart card readers may not be practical for an outdoor environment where the reader is exposed to the weather.

FIPS 201-1 allows other local agency approaches to the use of biometrics (SP 800-76-1 Section 1.2) that will enable the use of the contactless PIV card interface and would not require PIN entry. While these alternative options may be more appropriate for high-volume PACS environments, they may require a secondary biometric enrollment and may not be interoperable with other agencies. These are discussed in the other two options shown below.

Option 2 - Store Biometric Off-Card

In this scenario, agency-specific enrolled biometric data (e.g., face, fingerprint, iris, hand geometry) for each PIV cardholder is stored in an agency-controlled data repository (e.g., PACS server, control panel or reader) and the biometric is matched to the biometric data stored 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 and the user's agency-specific biometric data has been enrolled.

The use case scenario steps would be as follows:

1. The cardholder places the PIV card in close proximity to the contactless reader.
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.

The primary advantage of this option is that it avoids the reduced throughput associated with the use of contact readers and PIN entry which would otherwise be required to access the fingerprint data stored on the PIV card. In addition, this option allows the use of any type of biometric technology. The disadvantage of this option is that each user must have their biometric data enrolled in the local repository. This could be as simple as an automated process of copying the standard fingerprint templates from the PIV card and placing them in a local repository linked to the cardholder CHUID. However, if biometric technology other than fingerprints is used, then a separate enrollment for each cardholder is required.

Option 3 - 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 cardholder is stored on the PIV card in an agency-specific non-PIV 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 not interoperable with PIV 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. Further standards would need to be developed for technologies such as match-on-card to be interoperable between agencies.

The use case scenario steps would be as follows:

1. The cardholder places the PIV card in close proximity to the contactless reader.
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 which are also stored in the agency-specific container on the PIV card.
6. If authenticated, access is granted 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.

The primary advantage of this option is that it avoids the reduced throughput associated with the use of contact readers and PIN entry which would otherwise be required to access the fingerprint data stored on the PIV card. In addition, this option allows the use of any type of biometric technology. However, this option is ***not*** interoperable with PIV cards issued by another agency and requires the use of a visitor PIV card for access control.

8.2 PIV Card Revocation

PIV card revocation is a process that starts with the request for the revocation of the PIV Authentication Certificate and any other certificates associated with that PIV card. The revocation takes place at the certificate authority and results in a revocation list. The revocation list for each certificate authority is available as well as the associated certificate status for each of the cards via the online certificate status response (OCSP) responder infrastructure for an organization. This revocation is independent of the privilege that is associated with the card in the PACS database. The PACS privilege can be revoked, suspended or changed independently of the shared service or legacy PKI revocation process described above. The PACS linkage of the cardholder record with the PIV PKI certificate as discussed in section 6.2 completes the process of revocation or suspension.

When the PKI certificate is revoked, cardholder record privileges can be revoked or the record could be flagged for future investigation by security staff. A system that is fully connected with the IDMS or human resources (HR) directory system can also provide an automated card revocation based upon the revocation in the IT systems. At all times, the diverse PACS infrastructure must be in harmony with PKI certificate infrastructure and the master HR/directory system. If a system is not connected to a network, local CRLs or cached OCSP responses can continue to provide revocation status that can be acted on locally with respect to policy for aged responses.

8.3 The Card Holder Unique Identifier (CHUID) as the Card Credential Number

The migration path from systems today to PACS that can fully use the CHUID should be part of the agency strategic plan/budget request and should be built based on the lifecycle replacement of existing PACS.

The CHUID is a composite object on the PIV credential. The primary purpose of this object is to provide a unique ID number for the credential assigned to an individual. It contains the following major elements:

- FASC-N (Federal Agency Smart Credential Number)
- GUID (Global Unique Identifier)
- Authentication key-map
- Expiration date
- Issuer signature and certificate

Some deployed PACS systems already support the FASC-N. The FASC-N is almost identical to the SEIWG-012 string used in most proximity and magnetic stripe access control solutions today. Yet there are some strategic differences with a PIV credential. Primarily, the local site may not be the issuer of the credential. As such, the fields within the FASC-N may be coded differently than a local solution is expecting.

There are two critical differences between deployed systems and PIV compliant solutions:

- How many bits are in the data field for the credential number
- How unique credential numbers are established

Deployed PACS solutions started with credential numbers that are 26 bits long. These are found in the "credential number" field of the SEIWG-012 string and the FASC-N. (Note that the credential number is in the same location for both). This enabled an easy solution for small populations and was sufficient for the local facility to guarantee that no individual ever re-used a credential number.

PIV cards are issued on a government-wide scale. As such, they will be issued to millions of individuals. 26 bits can no longer guarantee that each individual has a unique credential number government wide. This poses a risk that can lead to more than one individual with the same credential number if the existing 26-bit number continues to be used. The PIV standards address this risk by increasing the size of the credential number in a managed growth strategy.

PIV-compliant cards provide two mechanisms for government wide credential numbering that avoid conflicts: using additional fields within the FASC-N; using the GUID. The FASC-N is today's solution for PIV. The GUID is a longer term solution that is easier to maintain.

Within the FASC-N, a fully qualified credential number is specified in three fields: Agency Code, System Code and Credential Number. The Agency Code determines who the issuer is. The concatenation of the System Code and Credential number provides 10 decimal digits to describe all credentials issued by that agency. All agencies tend to start issuing credentials starting at credential number one. To avoid conflicts, all PACS systems using the FASC-N as a credential number must use all three fields. This represents 48 bits of information, which is a significant increase over the deployed solutions using 26 bits.

The GUID is the next generation credential number. It is defined as a 128 bit (16 byte) object. 16 byte technology is used extensively throughout the Internet (IPv6 addresses are 16 bytes long) and with cellular technologies. It is easy to find hardware that can manipulate and manage these addresses. The GUID provides a very large address space for credentials across all government

agencies and enables reduced management overhead for credential number allocation associated with managing agency codes and credential number spaces.

Detailed information about credential numbers and their construction can be found in the TIG SCEPACS v2.3.

Migrating from the 26-bit infrastructure through 48 bits and finally up to 128 bits has a direct impact on the distributed processing of credentials throughout a PACS system. Panels designed for 26-bit credential numbers will not be able to cache as many entries and may not be able to handle all registered credentials for that site. Security directors must evaluate solutions that assist in managing this transition to large credential numbers.

Where possible, using the fully qualified 48 bit credential numbers from PIV cards is preferred. If readers, panels or head end systems can not handle this minimum, PIV card readers can offer firmware solutions to manage credential numbers including:

- Truncating the credential to fit the current infrastructure. This has a fairly high probability of conflicts with PIV credentials issued by other agencies, as everyone tends to start at credential number one. This is not a recommended solution.
- Extracting the Agency Code, System Code and Credential Number from the FASC-N and hashing them together to form a 32 or 64 bit string. This significantly reduces the risk of conflicts, but does not guarantee uniqueness. A process to handle conflicts is required. This may be effective if a small number of users from non-local agencies will be present at the local facility.
- Using the TIG SCEPACS Medium Assurance Profile. This combines the chip ID with the credential number and forwards both to the PACS. This takes a small credential number and combines it with the chip that carries it, reducing risk of conflicts and increasing security of the overall transaction.

An added data load to consider is when and where to check the expiration date of the PIV credential. GSA policy for testing transparent CHUID readers sets a protocol that demonstrates transmission of both the fully qualified FASC-N credential number (48 bits) concatenated with the expiration date to form a 75-bit string (155-bit string if using the GUID). The requirement in FIPS 201-1 is to ensure that expired credentials are denied access. To meet this requirement, the security director may elect to use the PACS head end database to register the expiration date of all PIV credentials. When that date is exceeded, the head end revokes privileges to these credentials. An alternative strategy is to read the data from the CHUID and check expiration at the reader. This model is not recommended, but is an option provided by many PIV reader manufacturers.

For integrity and verification of the PIV credential, the Issuer Signature and Certificate perform two functions: This signature ensures that the CHUID is unaltered *and* it provides the certificate information for the PIV Security Object. At a minimum, this signature (or the PIV Security Object signature) should be verified upon initial registration of the credential to the PACS system.

The CHUID, by itself, is not an authentication factor. It is public information that is available as a free-read object to anyone. An additional factor should be considered for physical access solutions. These can include:

- Using the TIG SCEPACS Medium Assurance Profile. This binds the chip ID to the FASC-N contained in the CHUID. This reduces the risk of copied data by requiring that the specific chip registered for that CHUID in the PACS be presented to the reader for verification.
- Using a PIN
- Using a biometric

9 Conclusions

With FIPS 201-1, security directors are empowered with a tool to check the identity and status of individuals needing access to their resources. This provides capabilities beyond those of most legacy physical access credentials in place today. It is important to understand the different authentication mechanisms and what levels of threat they mitigate. With this knowledge a security director is in the best position to decide how to employ the FIPS 201-1 credential within the context of their overall security plan, bearing in mind requirements for throughput, operational and interoperability considerations.

In transitioning to accepting PIV credentials, it is recommended that the security director first define the end state identification verification goals, then decide the equipment, if any, needed to help them accomplish this goal and finally, develop a transition and migration plan that meets the agency's needs and budget.

The PIV credential enables agencies to implement a range of identity authentication methods, allowing the appropriate method to be used based on an agency's risk assessment and security requirements.

10 Definition of Acronyms

AC	Agency Code
CCN	Card Credential Number
CHUID	Cardholder Unique Identifier
CMS	Card Management System
CRL	Certificate Revocation List
CAC	Common Access Card
CN	Credential Number
DOJ	Department of Justice
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
FRAC	First Responder Authentication Credential
GUID	Global Unique Identifier
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
HR	Human Resources
IBIA	International Biometric Industry Association
IDMS	Identity Management System
IEC	International Electrotechnical Commission
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISO/IEC 7810	ISO/IEC 7810 (2003) Identification cards -- Physical characteristics
ISO/IEC 7811	ISO/IEC 7811-7 (2004) Identification cards -- Recording technique -- Part 7: Magnetic stripe -- High coercivity, high density
ISO/IEC 7816	ISO/IEC 7816 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts
ISO/IEC 14443	ISO/IEC 14443 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards
IS	Information security
IT	Information technology
kHz	Kilohertz
MHz	Megahertz
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
OSE	Open Security Exchange
PACS	Physical Access Control System
PDF	Portable Data Format
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SC	System Code
SCA	Smart Card Alliance
SEIWG	Security Equipment Integration Working Group

SIA	Security Industry Association
SP	Special Publication (by the National Institute of Standards and Technology)
SP 800-73-1	Special Publication 800-73-1: Interfaces for Personal Identity Verification
SP 800-76-1	Special Publication 800-76-1. Biometric Data Specification for Personal Identity Verification
SSP	Shared Service Provider
TIG SCEPACS	Technical Implementation Guidance Smart Card Enabled Physical Access Control System
TWIC	Transportation Worker Identification Credential
URL	Uniform Resource Locator

11 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council, in collaboration with the Security Industry Association (SIA), Open Security Exchange (OSE) and International Biometric Industry Association (IBIA), to assist government agencies with developing migration plans for using FIPS 201-1 compliant credentials in physical access control systems. Publication of this document does not imply the endorsement of any of the member organizations of the Smart Card Alliance, SIA, OSE or IBIA.

The Smart Card Alliance wishes to thank the Physical Access Council, SIA, OSE and IBIA members for their contributions. Participants from the following organizations were involved in the development of this white paper: AMAG Technology, BearingPoint, CoreStreet, Diebold Actcom Security Systems, Inc., EDS, Fargo Electronics, Gemalto, GSA, HID Global, Hirsch Electronics, Identification Technology Partners (IDTP), Integrated Engineering, International Biometric Industry Association, LEGIC Identsystems, MDI Security Systems, NASA, Northrop Grumman, Open Security Exchange, Privo Systems, Quantum Secure, Sagem/Morpho, SCM Microsystems, Security Industry Association, Shane Gelling Company, SI International, Tennessee Valley Authority, Thales e-Security, Tyco, U.S. Department of Defense, U.S. Department of State.

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

- **Laurie Aaron**, Quantum Secure
- **Christina Bagby**, SIA
- **Tim Baldridge**, NASA
- **Consuelo Bangs**, Sagem/Morpho
- **Nathan Cummings**, HID Global
- **Sal D'Agostino**, CoreStreet
- **Tony Damalas**, Diebold Actcom
- **Sue Dernik**, SI International
- **Bob Fee**, LEGIC Identsystems
- **Bob Gilson**, U.S. Dept. of Defense/DMDC
- **Bill Gorski**, Siemens Building Technologies
- **Walter Hamilton**, IDTP
- **Daryl Hendricks**, GSA
- **Steve Howard**, Thales e-Security
- **Mike Kelley**, BearingPoint
- **Gary Klinefelter**, Fargo Electronics
- **Lolie Kull**, EDS
- **Gilles Lisimaque**, IDTP
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, SCM Microsystems
- **Neville Pattinson**, Gemalto
- **Dwayne Pfeiffer**, Northrop Grumman
- **Corey Ramey**, Tennessee Valley Authority
- **JC Raynon**, SCM Microsystems
- **Roger Roehr**, Tyco
- **Steve Rogers**, Integrated Engineering
- **Adam Shane**, AMAG Technology
- **Dale Shane**, Shane Gelling Company
- **Jim St. Pierre**, MDI Security Systems
- **Mike Sulak**, U.S. Dept. of State
- **Lars Suneborn**, Hirsch Electronics
- **Steve Van Till**, Brivo Systems
- **Mark Visbal**, SIA
- **Eric Widlitz**, HID Global
- **Rob Zivney**, Hirsch Electronics

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance 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 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.

About the Security Industry Association

The Security Industry Association (SIA) is a nonprofit international trade association representing electronic and physical security product manufacturers, integrators, specifiers, and service providers. SIA advocates for and supports the industry by providing education, research, technical standards and representation and defense of its members' interests. SIA is sole sponsor of the International Security Conference and Exhibitions (ISC EXPO). Learn more at www.siaonline.org.

About the Open Security Exchange

Open Security Exchange (OSE) is a not-for-profit, multi-industry association working to accelerate the widespread convergence of physical security with IT. It provides a forum for incisive discussions and solutions bearing on the Convergence issue; actively involves all stakeholders in enterprise IT and physical security management; serves as an information and educational resource to the international user community; and influences open and interoperable standards relevant to convergence. Members include leading security manufacturers, integrators, users, and consultants.

OSE is open to new members with dues ranging from $250 for individuals to $10,000 for billion dollar corporate sponsors. For additional membership information, please visit www.opensecurityexchange.org or e-mail info@opensecurityexchange.org.

About the International Biometric Industry Association

Founded in 1998 as a non-profit trade association in Washington, DC, the International Biometric Industry Association (IBIA) represents the manufacturers, developers, and solution providers of biometric technologies used in electronic human identity authentication – face, fingerprint, hand, iris, vascular, speech, as well as skin/dermis. IBIA impartially represents all biometric technologies in all applications.

IBIA advances the use of biometrics as the most effective and reliable means of ascertaining personal identity for the government, the commercial/private sector, and the consumer. The industry's leading voice on key policy issues affecting biometrics, IBIA fulfills its mission through education and advocacy.