Achieving a FIPS 201 PACS Solution

Abstract

This paper investigates the suitability of various options for PIV enabling a physical access control system. An augmentation approach that maximizes the reuse of existing system components and wiring is presented.

Contents

Executive Overview

HSPD-12 mandates that all government agencies use PIV identity cards for physical access control as a way to ensure a secure and interoperable approach. PIV enabling a PACS requires some changes but can be accomplished without the need for wholesale rip and replacement of existing equipment. This white paper will show that the required changes are limited to four areas: providing new card readers technically compatible with the physical characteristics of the PIV card, adding the ability to read and interpret the data on the PIV card, adoption of the FASC-N and GUID as unique user identifiers, and using strong PKI based validation at enrollment and time-of access. It concludes that choosing to augment the functionality of existing panels and door controllers yields the most secure and cost effective approach to providing strong PKI based validation at the time-of-access.

Introduction

Background

In August 2004, Homeland Security Presidential Directive 12 (HSPD-12) mandated the establishment of a government-wide standard for identity credentials to improve both logical and physical access control. In addition it required the use of this standard credential by all Federal employees and contractors when gaining physical access to federally controlled facilities as well as logical access to federally controlled information systems. In February, 2005 NIST released the required standard as Federal Information Processing Standards Publication 201 (FIPS 201). Issuance of these credentials is now in progress and agencies are turning their attention to identifying and implementing changes to their physical access control systems (PACS) to support the new Personal Identity Verification (PIV) card.

Purpose

There are several potential approaches to PIV enabling a physical access control system. Some of these are less costly and more secure than others. This paper addresses the strengths and weaknesses of each and identifies criteria for selecting the most suitable approach.

Achieving Trust Across Agencies

A major goal of HSPD-12 is to achieve trusted interoperability throughout the federal government. This trust is achieved by, among other things, having a highly secure identity card that supports strong authentication mechanisms. The PIV card has several built in security features, including:

- Cryptographic signing of integrity sensitive data elements such as certificates, fingerprints and facial images
- An on-card FIPS 140-2 certified cryptographic module
- FIPS 140-2 Security Level 3 protection of private keys stored on-card
- Keys are generated on-card and the private keys cannot be exported
- All cryptographic operations using the private keys are performed on-card
- Access to card commands involving the PIV private key require a PIN
- Cardholder PIN is matched on-card

These features can strongly enhance the overall security of a physical access control system if used properly. Ensuring the proper use and validation of the PIV credentials is at the heart of the process of upgrading an existing PACS to make it consistent with the intent of HSPD-12.

Typical Physical Access Architecture

A typical PACS architecture will look similar to that shown in Figure 1 below. While different PACS vendors may name their components differently, the essential functionality of all systems is the same[1]. Before launching into a discussion of changes required to enable a FIPS 201 PACS solution, it is important to understand the current state of the industry.

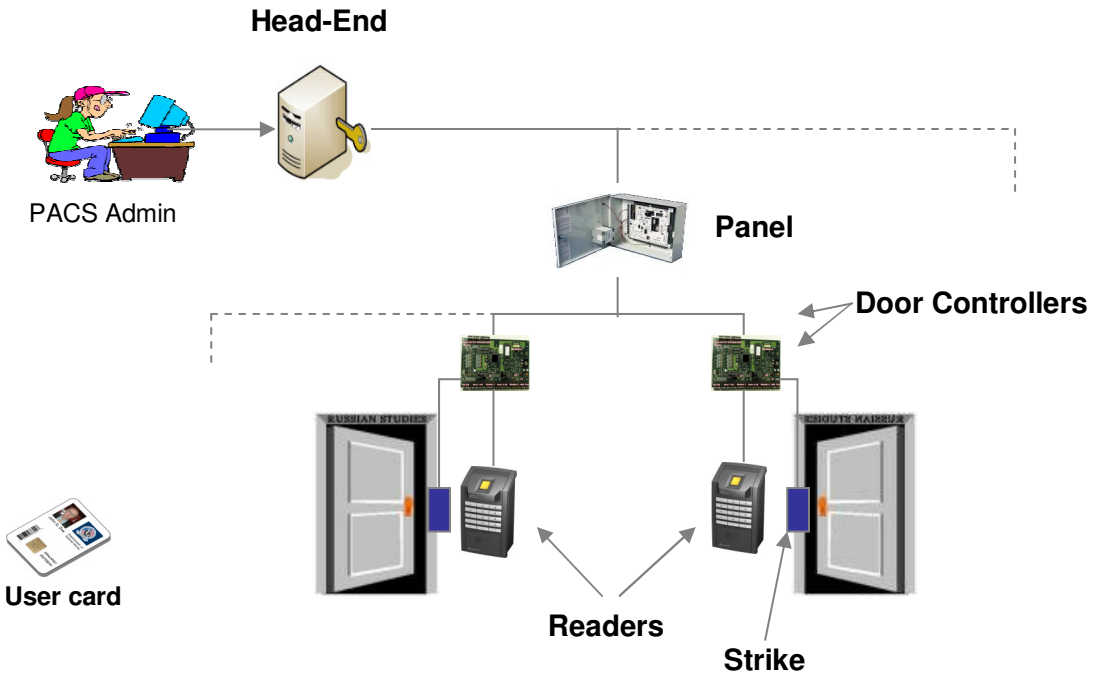

Figure 1: *Typical Physical Access Control System (PACS)*

The basic components of a PACS are the head-end server, panels, door controllers, readers, lock or strike mechanisms and the user identity cards. Each of these components is described below.

The **head-end** server is where the system is managed. This includes the following functionality:

- Enroll[2] users (name, …)
- Assignment of one or more unique badge IDs to the user
- Maintain status of enrolled users (active, inactive)
- Maintain user access privileges (often called access levels)
- Maintain door attributes (e.g., lock ID, type, software version, etc.)

[1] Panels are sometimes referred to as Intelligent System Controllers or PACS Field Controllers. Door controllers are sometimes referred to as Reader Interface Modules

[2] In this document we use the term "enroll" in the sense of provisioning users into a PACS head-end.

- Maintain door policies (level required for access, time based requirements)
- Collects, manages and reports access events (e.g., who entered, when, etc.)

The head-end server is the "brains" of the system and must therefore be located in a secure location.

The **control panel** is the access control "decision maker". Its role is to:

- Maintain and enforce door policy by matching user access level with door access level
- Stores access control data locally so that it can continue to operate when connectivity to head-end is lost
- Executes alarm and sensor logic
- Contains battery backup so that it can continue to operate during loss of power

A given PACS may have several panels depending upon the size of the system.

The **door controllers** provide the mechanical interface to execute the access control decisions. This involves:

- Driving the door strike
- Providing audio signals to indicate door latch is open
- Providing LED signals to indicate access control decisions (access granted or denied)
- Providing on/off signals for video recorders, door ajar alert, manual "buzz in", etc.

Depending upon the manufacturer, a door controller can control one, two or several doors.

The **readers** are familiar to all of us. Their primary purpose is to provide an electrical interface to the User ID card. Their functions include:

- Providing an access request presentation point to user
- Reading the claimed identity data from card
- Accepting authentication data (e.g., PIN, biometric)
- Communicating identity and authentication data to panel via the door controller
- Providing LED and audio on/off feedback to cardholder

Readers come in a variety of types: contactless, contact, with PIN pads, with biometric sensors and in various combinations.

Common **lock/latch mechanisms** in use are:

- Door strike – typically wired back to door controller where the latch is controlled by door controller (as shown in Figure 1)
- Lock – typically not wired back to door controller. In this case the reader is built into the lock which contains an access control list (ACL) and access policies specific to the lock.

Various **identity card** types are currently in use by physical access control systems. Examples include:

- Magnetic Stripe
- Proximity (e.g., HID PROX)

- Smart Card (e.g., PIV, iClass, DESFire, MIFARE) – smart cards are further characterized by type of interface (contact, contactless or dual) and size of processor, and memory.

Perhaps the most defining characteristic of existing systems is that user identity cards are issued locally by each PACS. This means that the choice of card type, format of the data on the card and assignment of badge IDs are all site dependent. In addition, there are very few standards associated with existing physical access control systems. Readers typically use the Wiegand protocol to talk to the door controllers but most other components and protocols are proprietary, including the identity cards. The result is that there is virtually no interoperability between separate PACS, even those from the same vendor.

Criteria for Choosing a PACS Upgrade Approach

The focus of this paper is on upgrading existing PACS deployments as opposed to deploying a new PACS. Regardless of the approach taken there are certain goals that apply. In general, a suitable approach to PIV enabling an existing PACS should meet the following criteria:

- **Maximize reuse** – the approach should not be based on a rip and replace strategy as this is not required. Maximizing reuse is key to minimizing cost.
- **Minimize custom modifications** – custom modifications are typically expensive and difficult to maintain or replace and should be avoided. A commercial off the shelf approach should be used wherever possible.
- **Support multiple PACS** – many organizations are not standardized on a single PACS make or model for their entire enterprise. A PIV enabling solution that is not tied to a specific make or model will make future upgrades of the PACS components much easier.
- **Support multiple authentication mechanisms** – NIST Special Publication 800-116 [SP 800-116] identifies four authentication mechanisms suitable for controlling access to "controlled", "limited" and "exclusion" areas[3]. The PIV enabling solution should support all of these mechanisms and provide the capability to dynamically switch between them in response to changes in threat level.
- **Support PIV-I** – PIV Interoperable[4] cards are used by federal contractors who are included in the HSPD-12 mandate and may need access to a controlled facility. This capability will enable PIV-I visitors as well as temporary PIV-I cardholding employees to use the access control system.
- **Improve security** – HSPD-12 is all about improving security in both physical and logical access control. To be effective the solution must securely execute the recommended authentication mechanisms.

[3] See also Appendix B for a description of these controlled areas.
[4] PIV-I cards are defined as "an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers , and is issued in a manner that allows Federal government relying parties to trust the card." See reference [PIV-I].

Changes Imposed by FIPS 201 Compliance

The introduction of the PIV card represents a major step forward in standardization of access control within the federal government. There is now one standard identity card that is centrally issued and is recognizable and trustable by all government agencies. While using the PIV card in existing PACS will require some changes it will not necessitate a complete replacement of the PACS components. Figure 2 below shows where these changes affect the system.

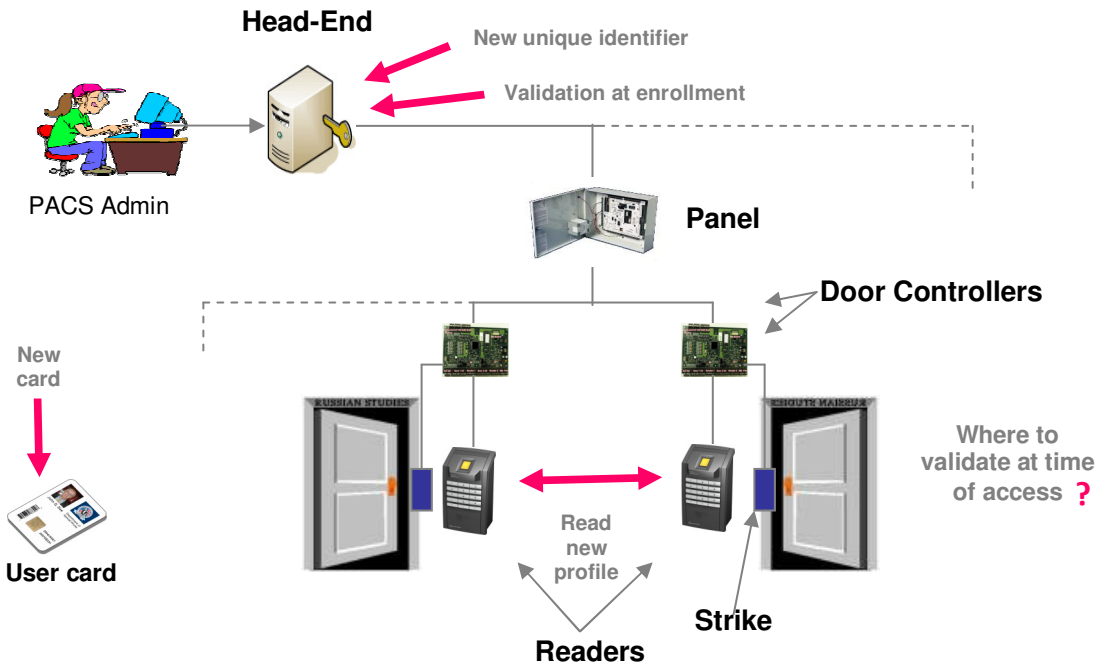

Figure 2: *Changes required to PIV enable a PACS*

Upgrading an existing PACs to enable it to properly use a PIV card as the user identity card requires a few small but significant changes:

1. The PIV card is as an ISO 14443 type smart card with a contactless interface that operates at 13.56 MHz. In addition some authentication mechanisms require using the contact interface. The most common identity cards in use today are contactless proximity cards which operate at 125 kHz. This incompatibility in communication protocol and the need in some cases to support the contact interface will require replacement of the readers.
2. The PIV card employs a new profile for representing the data on the card. The system must therefore add functionality to read and interpret this new profile.

3. Each PIV card contains a unique identifier called a FASC-N[5]. (The unique identifier on PIV-I cards is the GUID[6].) New functionality must be added to extract the unique identifiers from the card data and use them in the access control decision process.
4. To ensure secure use of the PIV card some level of authentication and validation must be performed as part of the enrollment process and at the time-of-access. This is new functionality that must be added to the system.

Validation

Of the four PACS changes identified above, adding PKI based validation for the PIV credential is the most complex. The term "validation", as used in this document, is defined to be the process of authentication (i.e., proving your claimed identity) and revocation checking of the presented credential.

Authentication

Authentication is the process of proving one's claimed identity. There are three basic threats associated with authenticating a user claiming to be the person identified on the PIV card:

1. Counterfeit identifiers – a genuine PIV credential is issued by a trusted authority. At the point and time of access it is imperative to know that the presented identifier is genuine and has not been forged by someone seeking unauthorized access. This threat is mitigated through the use of digital signatures on each of the credential's data objects (e.g., certificates, fingerprint template, facial image). Validation of these signatures ensures the data were signed by the trusted authority.
2. Cloned or copied identifiers – trusting a PIV credential certificate requires knowing that it is not a copy of a legitimate user's certificate. This threat is mitigated by executing a PKI private key challenge to ensure the certificate (through its public key) is bound to the private key embedded in the PIV card.
3. Lost or stolen identifiers – trusting the identifier requires knowing that it represents the person presenting it. This threat is mitigated by verifying the binding of the card holder to the card by requiring either a PIN, biometric or both as part of the validation process.

In general the decision to grant or deny access is not based on authentication alone. The person requesting access must also be authorized to do so and their identity credential must be checked to ensure it has not been revoked by the issuing authority.

Validation: What, When and Where

Validation of the PIV card would typically include some or all of the following:

1. Path discovery – the process of discovering a path from the PIV certificate to an embedded trust anchor.

[5] FASC-N stands for Federal Agency Smart Credential Number.
[6] GUID stands for Global Unique IDentifier. See reference [PIV-I] for additional information.

2. Path signature verification – establishing that every certificate in the path is genuine and not counterfeit.
3. Data object signature verification – establishing that every signed data object on the card was signed by a trusted issuer (e.g., certificates, fingerprint template, facial image template) to ensure they are genuine and not counterfeits.
4. Cross checking data object identifiers – all signed data objects on the PIV card have an identifying number (FASC-N) unique to that card. Checking that each data object contains the same FASC-N (or GUID) ensures they all belong to the same credential.
5. Various PKI conformity and freshness checking (key usage, expiration dates, etc.).
6. PIN check – to ensure the card holder is bound to the credential to mitigate the threat of lost or "shared" cards.
7. Private key challenge – to ensure the certificate is bound to the token to which it was issued and has not been copied or cloned.
8. Biometric check – to ensure the card holder is the same person that was issued the PIV card. This mitigates the threat of "shared" cards and disclosure of the card's PIN.
9. Periodic checking of the revocation status of the PIV Authentication Certificate
10. Periodic revalidating the full path – to ensure all of the certificates in the path remain valid and have not been revoked.

Validation during enrollment should include all of these checks to ensure at the highest level possible that all enrollees are in fact who they claim to be. This would typically be done as a function at or in conjunction with the PACS head-end.

Validation at the time-of-access will involve a subset of these checks depending upon the assurance level required and authentication mechanism chosen for the specific access point being addressed[7]. The question of where this validation should be done however is more challenging. Possible options include placing this functionality in:

- Head-end
- Readers
- Panel/Door Controllers
- Separate module

Performing time-of-access validation at the head-end would seem to be a logical choice since it could take advantage of the full PKI validation functionality used for enrollment. However this approach would require adding new wiring to support two way communications between the readers and the head-end to facilitate signature checking on the credential data elements (CHUID, certificates, biometric templates), execution of a private key challenge and execution of a biometric match. In most cases this would be prohibitively expensive. In addition, this approach would fail to operate properly during a loss of power or reader to head-end communication.

[7] See NIST references [SP 800-116] and [SP 800-73-2] for descriptions of the various authentication mechanisms and associated validation procedures.

Alternately the replacement readers, something that may need to be done regardless of the approach chosen, could include the validation functionality. The new readers would require more powerful (and costly) processors to perform the cryptographic processes associated with PKI validation. This approach also requires two way communications with external networks or the head-end in order to receive periodic downloads of certificate status data, trust anchors for signature verification and to service path discovery requests for any visitors with PIV or PIV-I cards. In addition there are two security issues associated with this approach:

- Security related processing on the unsecured side of the PACS boundary
- PACS network connection available on the unsecured side of the PACS boundary

Putting the time-of-access validation into the panel or door controller components is a more attractive approach in that it addresses most of the deficiencies and security issues associated with the approaches discussed above. Specifically,

- Security related processing is on the secured side of the PACS boundary
- PACS network connection is on the secured side of the PACS boundary
- There is potentially much less rewiring to be done
- The system would continue to operate properly as these components typically have battery backup for lost power and could store the required validation information locally.

The drawback with placing the PKI validation functionality into a panel or door controller is that these components would have to be replaced rather than upgraded. Replacement is necessary because upgrading existing boards would require some or all of the following changes:

- Addition of a more powerful processor to perform the cryptographic PKI operations in a timely manner
- Addition of external serial ports for two way communications with the readers
- Addition of Ethernet port for communication with head-end and/or external networks for periodic retrieval of status information

Note that any such upgrade would also have to be done separately for all makes and models of these components which would not be cost effective.

An alternative to upgrading or replacing all the panels and/or door controllers is to augment the existing system functionality with the addition of a new “plug-in” module. To be successful this new module must work with existing PACS panels and door controllers as they are, without requiring any changes. This approach would then be the most cost effective way to PIV enable an existing PACS.

The CoreStreet Approach

CoreStreet’s approach to PIV enabling an existing PACS is shown in Figure 4. In this approach the PIV enabling functionality is added by augmenting the existing door controller and panel functionality. It requires two changes: replacing existing card readers with PIV enabled readers

and inserting a CoreStreet FIPS-201 F5 module between the reader and the door controller. The F5 module contains all the PKI validation functions executed at the time-of-access.

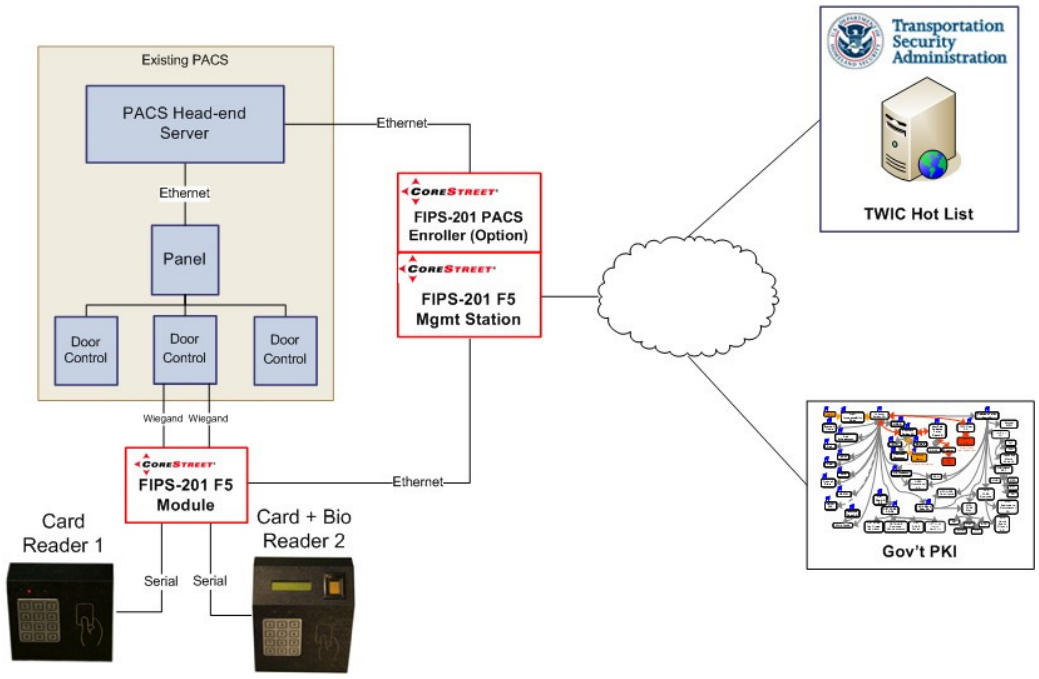

Figure 4: *PIV Enabled PACS using the F5 Panel Augmentation Approach*

Inserting the F5 module requires no modification or replacement of any non-reader component in an existing PACS. It provides all the validation functionality required by FIPS 201 in compliance with HSPD-12. F5 modules are installed between any existing PACS panel or door controller and a supported reader: contact card-only, contactless card-only, contact and contactless card-only, card + PIN, card + bio or card + PIN + bio. Readers are selected based on assurance level requirements. The F5 module-reader combination supports CHUID, CAK, PKI, and BIO authentication methods as described in SP 800-116. Each F5 module can support one or two readers.

F5 modules are managed by a CoreStreet FIPS-201 F5 Management Station (F5MS) that provides centralized control of assurance level settings and distribution of dynamic validation data such as credential revocations and trusted issuers. The F5MS also controls pushing firmware updates to all F5 modules.

The F5 module validates cards according to its assurance level setting, constructs the badge ID from data on the card and then passes the badge ID to the PACS panel for an access decision. The PACS Head-end maintains the user access authorizations as is currently done. For invalid cards, the F5 module can be configured to send a preset badge ID to the PACS panel and/or close

an output relay. Cardholder data is captured automatically the first time a card is presented for access and then stored at the F5MS. This feature allows traditional enrollment of cardholders using existing PACS enrollment functionality, integration with an identity management system (IDMS) or use of a third party enrollment package such as visitor software or the CoreStreet FIPS-201 PACS Enroller.

Features and Benefits of F5 Panel Augmentation Approach

CoreStreet's F5 panel augmentation approach enables an agency to PIV enable their existing PACS system in a cost effective and secure manner that meets all of the previously defined criteria:

- **Maximizes reuse** – the CoreStreet FIPS-201 F5 solution minimizes cost by augmenting the capability of existing panels and door controllers and requires no changes to the existing system other than adding PIV compatible readers.
- **Minimizes custom modifications** – the F5 solution does not require any custom modifications to existing PACS components. Future upgrades to the existing PACS can be done without requiring any custom modifications.
- **Supports multiple PACS** – the F5 solution is PACS make and model independent. The optional Enroller component can be integrated with various PACS head-ends.
- **Supports multiple authentication mechanisms** – the F5 solution provides dynamically configurable support for all authentication mechanisms defined in SP 800-116 (CHUID, CAK, PKI, BIO and combinations).
- **Supports PIV-I** – the F5 solution supports a variety of identity credentials in use today, including PIV, PIV-I, TWIC, FRAC and CAC (legacy, NG, EP). All four TWIC authentication modes as defined in the TWIC reader specification are supported.
- **Improves security** – the F5 solution provides a complete PKI validation approach to support strong authentication of the card holder. This includes configurable periodic status checking via OCSP, CRL or TWIC hot list and validation of contractor and visitor identities via certificate path discovery and validation through the Federal Bridge.

Summary

HSPD-12 mandates that all government agencies use PIV identity cards for physical access control as a way to ensure a secure and interoperable approach. PIV enabling a PACS requires some changes but can be accomplished without the need for wholesale rip and replacement of existing equipment. We have shown that the required changes are limited to four areas: providing new card readers technically compatible with the physical characteristics of the PIV card, adding the ability to read and interpret the data on the PIV card, adoption of the FASC-N and GUID as unique user identifiers, and using strong PKI based validation at enrollment and time-of access. We have further shown that choosing to augment the functionality of existing panels and door controllers yields the most secure and cost effective approach to providing strong PKI based validation at the time-of-access.

Appendix A: Questions for your PACS Solution Provider

In planning out your approach to PIV enabling an existing PACS you will want to ensure you have answers to the following questions. Will your proposed approach:

1. Work properly when network communications to the headend is lost?
2. Work properly during a power outage?
3. Support interagency validation? If yes, is the approach for this to:
    a. Use a "trust list"? (i.e., a list of trusted issuers. This approach will require manual maintenance.)
    b. Use path discovery and validation through the Federal Bridge?
4. Support revocation status refreshing on a configurable time schedule?
5. Support re-validation of the trust path on a configurable time schedule? Note the end entity certificate may be valid but the path may not.
6. Have any secure processing taking place on the unsecure side of the PACS boundary?
7. Have any security sensitive network connections on the unsecure side of the PACS boundary?
8. Require replacing the PACS headend, panels or door controllers?
9. Require replacing wiring to the readers?
10. Provide for different reader types that support the various assurance mechanisms identified in SP 800-116? (E.g., card-only contact and/or contactless, card + PIN, card + PIN + bio.)
11. Provide the means to change the required assurance level for individual readers? For example, as the threat level goes up you may want to raise the assurance level on all or some of your readers from CHUID to CAK or PKI.
12. Support the following types of cards:
    a. PIV
    b. PIV-I
    c. CAC (including legacy, Next Generation, End Point)
    d. TWIC
    e. FRAC
13. Provide a workable transition from your current access control token by simultaneously supporting legacy cards (e.g., prox cards) and PIV cards?
14. Retain all your existing PACS functionality at each access point such as video, 2 person rule, forced door, etc.?
15. Require re-enrolling your personnel with their new PIV card?

Appendix B: Implementation Guidance

A prerequisite for planning and implementing a solution to PIV enable a PACS is to determine just how much security is required and where. NIST's Special Publication 800-116 provides excellent guidance in answering this question. Figure 3 below is taken from this document and shows the recommended segmentation of access control points in terms of security based risks.

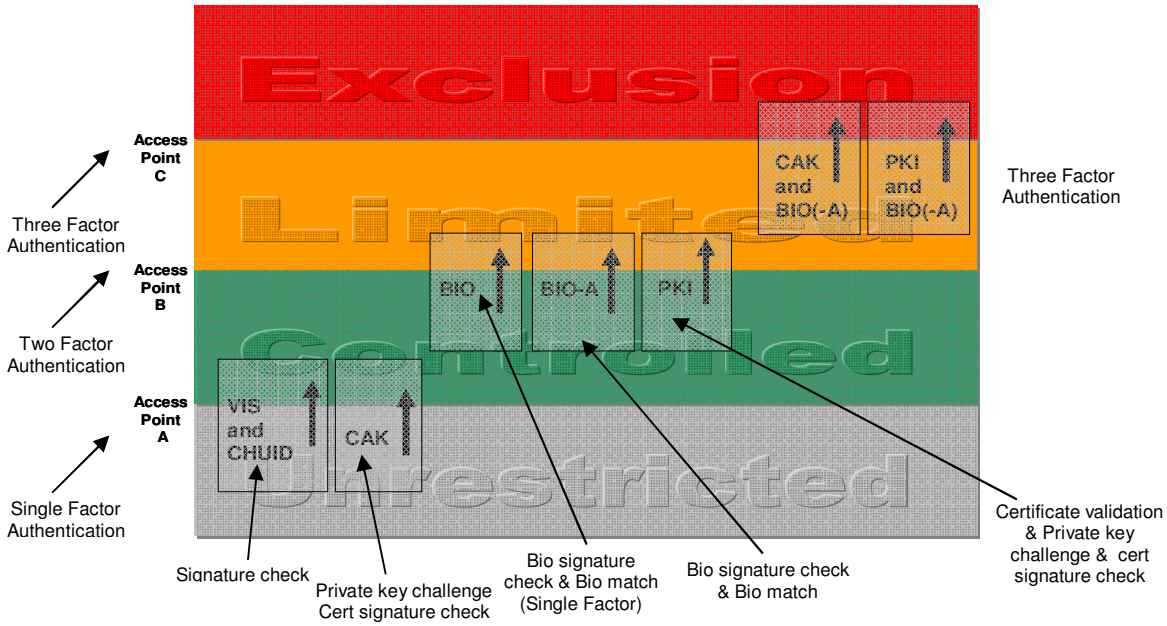

Figure 3: *NIST SP 800-116 PIV Authentication Mechanism Use Cases*

In this diagram the Unrestricted area is consider public with no restrictions as to who has access. Access to the Controlled area is restricted to those who can prove affiliation. For example, possession of an Agency's badge could be sufficient to gain access at an outer perimeter of a facility. Access to the Limited area is restricted to members of a group who are fulfilling a specific role. Finally, access to the Exclusion area is restricted by individual authorization, analogous to the "need-to-know" requirement in the classified world.

SP 800-116 defines and describes the authentication methods shown in Figure 3. The PIV card is designed to support each of these methods which are intended to provide different levels of assurance of the identity of the user. Which authentication method should be used depends upon the security requirements at the point of access.

Appendix C: Definitions

The following table defines how various terms are used in this document.

Access Level	A set of attributes or privileges defined in the PACS head-end. Each access level is a set of reader and time zone pairs. Each time zone is a set of time intervals within a day bound to week types and holiday types in which they are active. Each user credential is assigned any number of access levels each with a limiting date range.
Access Policy	Access policies consist of a group of access levels assigned to a given access point. They define the attributes users must have to gain access to a given set of access points at a given set of times. They are set and maintained in the PACS head-end.
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of proving your claimed identity; establishing confidence in user identities.
Authorization	The concept of allowing access to resources or physical areas only to those permitted to use or access them. Authorization (deciding whether to grant access) is a separate concept to authentication (verifying identity), and usually dependent on it.
Certification Authority	A trusted entity that issues and revokes public key certificates.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. A credential may be a physical artifact (e.g., a PIV Card) or a data object (e.g., a PKI certificate). In the PIV Card context the token is a private key locked on the card.
Data integrity	The property that data has not been altered by an unauthorized entity.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
FASC-N	Federal Agency Smart Credential Number. This number is unique across all agencies in the US Federal Government and is a mandatory component specified in FIPS 201 for the PIV card.
FIPS 201	Federal Information Processing Standards publication number 201. This standard defines the format and profile of the Federally mandated PIV Card.

Identity	The qualities of an individual that make them different. Example qualities include name, eye color, height, gender, etc.
Identity	A unique name of an individual person. Since legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Card	A credential in the form of a physical artifact. An identity card can be used as both a credential and token (i.e., when used as a "flash pass") in which case possession of the card provides single factor authentication of claimed identity.
Lock	A device to delay, complicate and/or discourage unauthorized entry.
On-Line Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
PACS	Physical Access Control System. A PACS includes multiple components, typically a Head-end, Intelligent System/Door Controller, Card Reader and electronic Locks.
PACS Head-end	The management software used to control lock access policies and user access levels.
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
PIV Card	Personal Identity Verification (PIV) card. A Federally mandated identity card ("smart" card) issued to an individual that contains 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).
Private key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Proof of Possession protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).
Public key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public key certificate	A digital document issued and digitally signed by the private

	key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.
Relying party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Shared secret	A secret used in authentication that is known to the claimant and the verifier.
Symmetric key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Trust list	A collection of trust anchors. The most common example is the collection of root certificates that are explicitly trusted by the user and stored locally in the user's Web browser or other client application.
Validation	The process of establishing the trust worthiness or legitimacy of a PKI credential or proof

Appendix D: Acronyms

The following table defines the acronyms used in this document.

Acronym	Definition
ACL	Access Control List
BIO	Biometric authentication
CA	Certificate Authority, also Certification Authority
CAC	Common Access Card
CAK	Card Authentication Key
CHUID	Card Holder Unique IDentifier
CRL	Certificate Revocation List
DoD	Department of Defense
EP	End Point – used in terms of version of CAC
F5MS	F5 Management Station
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
FRAC	First Responder Authentication Credential
GSA	Government Services Administration
GUID	Global Unique IDentifier
HSPD-12	Homeland Security Presidential Directive 12
IDMS	IDentity Management System
ISO	International Standards Organization
LED	Light Emitting Diode
NG	Next Generation – used in terms of version of CAC
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PACS	Physical Access Control System
PKI	• Public Key Infrastructure • Also used as "PIV Authentication Key" to identify an SP 800-116 defined authentication method
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV Interoperable
PROX	Proximity card
TWIC	Transportation Workers Identity Credential

Appendix E: References

[HSPD-12] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

[FIPS 201] Federal Information Processing Standard 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

[SP 800-63] NIST Special Publication 800-63, *Electronic Authentication Guideline,* Version 1.0.1, September, 2004

[SP 800-73-2] NIST Special Publication 800-73-2, *Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation,* September, 2008

[SP 800-116] NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS),* September, 2008

[PIV-I] CIO Council publication, *Personal Identity Verification Interoperability For Non-Federal Issuers,* May, 2009

About CoreStreet

Every day, the world's most demanding government and commercial enterprises rely on CoreStreet technology to authorize critical events, ranging from signed communications and transactions to physical access.

More information, including technical whitepapers, industry solution studies and a list of the patents awarded to the company is available at www.corestreet.com.

www.corestreet.com
+1 617 661 3554
info@corestreet.com