Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS)

DRAFT

Version 2.0.2

May 24, 2012

Table of Contents

Figures

Tables

1. INTRODUCTION

1.1 Background

A Physical Access Control System (PACS) allows federal entities to assign different access requirements based on the risk of the physical asset being accessed. In this way, a PACS is used to mitigates the risk of a physical security breach. One important facet of a PACS is the authentication mechanisms supported.

[HSPD-12] requires a common identification standard for federal employees and contractors (i.e., an identity credential that can be interoperable government-wide). This resulted in the Personal Identity Verification (PIV) Card, which [FIPS 201] and associated documents technically define. As of Q3 2011, the federal government has issued 4,270,560 PIV Cards to federal employees (91% of total federal employees) and 846,365 PIV Cards to federal contractors (81% of total federal contractors).

In addition, the federal government has implemented policy for non-federal issuers (NFIs) of identity cards to produce identity cards that can technically interoperate with federal government PIV systems and can be trusted by federal government relying parties. This resulted in the PIV Interoperable (PIV-I) Card. To-date, the Federal Public Key Infrastructure (FPKI) has approved five PIV-I Card Issuers and one PIV-I Bridge (who in turn has approved two PIV-I Card Issuers to-date). "Conservative estimates for the number of active PIV-I credentials to be issued exceeds 25 million, serving non-executive federal, state and local agencies, first-responder organizations and others."[1]

The emergence of PIV Cards and PIV-I Cards has created a new set of challenges for PACS implementations, including but not limited to new and stronger authentication technologies (mechanisms), non-local card issuance, and new federal policies. This is different from the traditional PACS-related tokens, technologies, and policy environment.

In February 2011, OMB issued [OMB M-11-11], which is applicable to end-users, integrators/solution providers, and manufacturers/developers, and mandates the following:

1. Effective immediately, all new systems under development must be enabled to use PIV credentials;
2. Effective the beginning of FY2012, existing physical and logical access control systems (LACS) must be upgraded to use PIV credentials;
3. Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation;
4. Agency processes must accept and electronically verify PIV credentials issued by other federal agencies; and
5. The government-wide architecture and completion of agency transition plans must align as described in the Federal Chief Information Officers (CIO) Council's FICAM Initiative.

In response to the large number of issued PIV and PIV-I Cards, their new authentication mechanisms, and the [OMB M-11-11] mandate, the Federal Identity, Credential and Access Management (FICAM) Initiative is publishing this document to provide guidance for leveraging PIV and PIV-I credentials in a federal agency PACS.

---

[1] CertiPath, http://www.certipath.com/certipath-bridge/piv-i-issuers

A variety of other federal documents[2] have been published that directly or indirectly affect a PACS implementation in this regard, including but not limited to:

- Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* [OMB M-04-04];
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* [OMB M-11-11];
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* [HSPD-12];
- Federal Information Processing Standards 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS 201];
- National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [NIST SP 800-53];
- NIST Special Publication 800-79, *Guidelines for Accreditation of Personal Identity Verification Card Issuers* [NIST SP 800-79];
- NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* [NIST SP 800-116]; and
- *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* [FICAM Roadmap].

1.2 Purpose and Audience

The sole purpose of this document is to provide detailed technical and security guidance for leveraging PIV and PIV-I authentication mechanisms in a federal agency PACS - to provide interoperability across the federal enterprise and thus comply with directives such as [OMB M-11-11].

The primary audience for this guidance is technical staff with responsibilities such as integrating PACS components, selecting PACs solutions, and determining the most appropriate local use of PIV and PIV-I in a local PACS.

A secondary audience is procurement officials that need technical guidance for citation in PACS procurements that intend to implement the mandates within OMB M-11-11].

1.3 Scope

The scope of this guidance document is limited to the following:

1. Leveraging PIV and PIV-I authentication mechanism in a PACS:
    a. to implement strong security controls; and
    b. to provide interoperability between different facilities.
2. Providing authentication patterns to illustrate proper and improper uses of PIV and PIV-I authentication;

[2] For NIST documents (Special Publications, Federal Information Processing Standards, Interagency or Internal Reports), see http://csrc.nist.gov/publications/. For OMB Memoranda, see http://www.whitehouse.gov/omb/memoranda_default.

3. Understanding the risks, pros, and cons of the various PIV and PIV-I authentication mechanisms; and
4. Reconciling PIV and PIV-I authentication mechanisms against levels of assurance specified in various documents such as [NIST SP 800-116], [NIST SP 800-53], [OMB M-04-04], [OMB M-11-11], [FIPS 201], [Facility Security Levels].

A discussion of and guidance for aspects of a PACS other than leveraging PIV and PIV-I Cards are out of scope for this document[3]. That is, all other aspects of a PACS (e.g., how to implement and manage core PACS components such as readers, controllers, head ends, servers, client work stations; defining and managing access control policies; integrating add-on functions such as CCTVs, intrusion detection systems, life safety systems, and IT support infrastructure) are out of scope for this document.

In addition, biometric match-on-card (MOC) and other technologies such as iris scanning are not currently addressed in authoritative documents. Accordingly, those technologies are out of scope for this document, which deals only with off-card fingerprint comparison.

There is intent for this guidance document to be consistent with authoritative documents. If there is an inconsistency, the applicable authoritative document takes precedent.

1.4 Document Organization

This document is divided into four parts. Section 1 provides a high-level introduction as well as purpose and scope. Sections 2-7 describe the current PACS landscape, as well as current standards and guidance that directly or indirectly affect PACS. Section 8, *Enterprise PACS Security Functions*, describes specific and measurable security controls that impact the successful operations of PACS as a security countermeasure. The remainder of the document analyzes common authentication patterns, providing insights, clarifications and guidance, especially in light of Section 8.

[3] Please see other sources for a broader, deeper treatment of these out-of-scope topics. See *Appendix D: Document References*, as a starting point for identifying sources.

2. PIV AND PIV-I CARDS

This document focuses on use of PIV and PIV-I Cards in a PACS. The Cards are defined as follows:

- **PIV Card -** an identity card that is fully conformant with federal PIV standards (i.e., FIPS 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV Cards are interoperable with and accepted by all Federal Government relying parties to authenticate identity.
- **PIV-I Card -** 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 and non-federal relying parties to accept the card to authenticate identity. PIV-I credentials provide identity proofing (or identity certainty). PIV-I Cards are issued by non-federal issuers whose proofing process must be commensurate with PIV that binds a card to a person. PIV-I does not assert that a background investigation was performed. Additional investigation requirements may be necessary based on actual assignment and asset risk. PIV-I credential requirements are defined in *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)* [FBCA CP].

Both PIV and PIV-I conform to the following NIST publications:

- **[NIST SP 800-73]** – provides PIV Card technical interoperability specifications. PIV-I Cards must adhere to the [NIST SP 800-73] data model and card edge requirements;
- **[NIST SP 800-76]** – provides PIV Card biometric technical guidance. PIV-I Cards must conform to [NIST SP 800-76]; and
- **[NIST SP 800-78]** – provides PIV Card technical guidance regarding digital credentials present on the PIV Card. This is where much of the trust in the identity credential will be established. PIV-I Cards must ensure their digital credentials meet [NIST SP 800-78] technical requirements.

Table 2-1 compares the requirements for each Card type.

Table 2-1, PIV-I Guidance Document Comparison of PIV and PIV-I Cards

	Policy Comparison	**PIV**	**PIV-I**
Identity Verification	NACI	●	
Trust model	FIPS 201 Conformant	●	
	PIV OID on PIV Authentication Certificate (trust model)[4]	●	
	FBCA PIV-I Hardware equivalent Authentication Certificate[5]		●
	FBCA PIV-I Content Signing equivalent object signing certificate		●
	Content Signing EKU for PIV card issuers	●	
	Content Signing EKU for PIV-I card issuers		●
	PIV Card Authentication Certificate	●	
	PIV-I Card Authentication Certificate		●
	Technical Comparison		
Authentication Assurance Level	NIST SP 800-63-1, Assurance Level 4[6]	●	●
Card Edge and data model	Card Stock on GSA APL[7]	●	●
	PIV Application Identifier (AID)	●	●
	Command edge and NIST SP 800-85 conformant[8]	●	●
	NIST SP 800-73 conformant GUID present in the CHUID	●	●
	RFC 4122 conformant UUID required in the GUID data element of the CHUID[9]		●
	RFC 4122 conformant UUID present in the Authentication Certificates[10]		●
	Visually distinguishable from PIV Card		●
	Asymmetric Card Authentication Key (CAK) presence	Optional	Required
	Symmetric CAK presence	Optional	

[4] http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf

[5] The FBCA establishes certificate equivalence for Non-Federal Issuers. This is achieved by a mapping of one organization's policy with other organization's policy, and the issuance of a cross-certificate to associate one policy OID with another.

[6] This Assurance Level is only ensured when using the PKI certificates in these credentials.

[7] Conformant form factor.

[8] Contact and contactless command edge conformant defined in [NIST SP 800-73-2] part 2 requires support for specific ISO/IEC 7816 commands. Card edge and data model verified through NIST SP 800-85 test tools (further efforts are expected to address exceptions for Non-Federal Issuers).

[9] [NIST SP 800-73] does not require use of RFC 4122 to generate a valid GUID for PIV cards; but it is required for PIV-I cards.

[10] UUID value will be in subjectAltName extension of the PIV Authentication Certificate and Card Authentication Certificate.

3. PACS OVERVIEW

Similar to LACS, a PACS follows a straightforward operational process to authenticate users using one or more of a predefined set of credentials and then makes authorization decisions based on a predefined set of rules governing access. Prior to [FIPS 201], the Federal Government commonly implemented PACS that authenticated users using a proprietary, single-use card that typically contained a locally unique identifier. When this card is presented at an electronic reader, the identifier is checked against a proprietary, internal "white list" to make authorization decisions to a facility at an intended point of entry (e.g., door, turnstile). While this mode of operation tends to be the most common and uncomplicated method of managing access to controlled areas, it has vulnerabilities as described in [NIST SP 800-116]:

> "The physical access control systems (PACS) deployed in most federal buildings are facility-centric rather than enterprise-centric and utilize proprietary PACS architectures. Therefore, many issued identification (ID) cards operate only with the PACS for which they were issued. In addition to the lack of interoperability, deployed PACS technology presents the following challenges:
>
> 1. **Scalability** – some deployed systems are limited in their capability to process the longer credential numbers necessary for Government-wide interoperability.
> 2. **Security** – deployed PACS readers can read an identifying number from a card, but in most cases they do not perform a cryptographic challenge/response exchange. Most bar code, magnetic stripe, and proximity cards can be copied easily. The technologies used in these systems may offer little or no authentication assurance.
> 3. **Validity** – deployed PACS control expiration of credentials through an expiration date stored in a site database. There is no simple way to synchronize the expiration or revocation of credentials for a federal employee or contractor across multiple sites.
> 4. **Efficiency** – use of PACS Personal Identification Numbers[11] (PINs), public key infrastructure, and biometrics with deployed PACS is managed on a site-specific basis. Individuals must enroll PACS PINs, keys, and biometrics at each site. Since PACS PINs, keys, and biometrics are often stored in a site database, they may not be technically interoperable with PACS at other sites."[12]

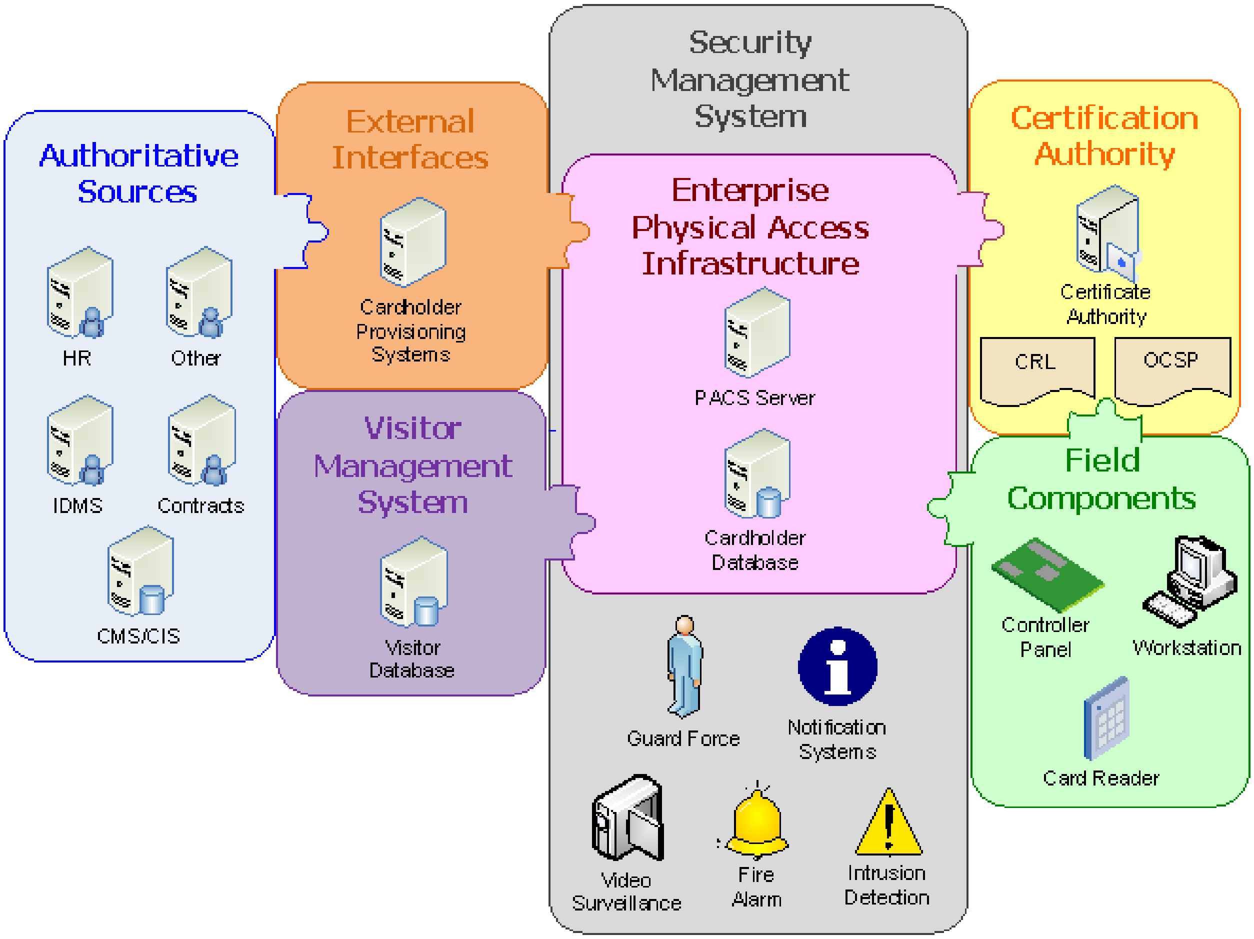
Figure 3-1[13] illustrates that a PACS is an essential part of a security management system, and requires interfaces with other parts of the overall identity management and security infrastructure. Supporting solution components, and key design characteristics can be found in [FICAM Roadmap] Section 10.2.

[11] "PACS PIN" refers to a PIN that is managed and authenticated by a particular PACS. PACS PIN is distinct from the PIV/PIV-I PIN authenticated by PIV or PIV-I Cards.

[12] http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[13] [FICAM Roadmap]

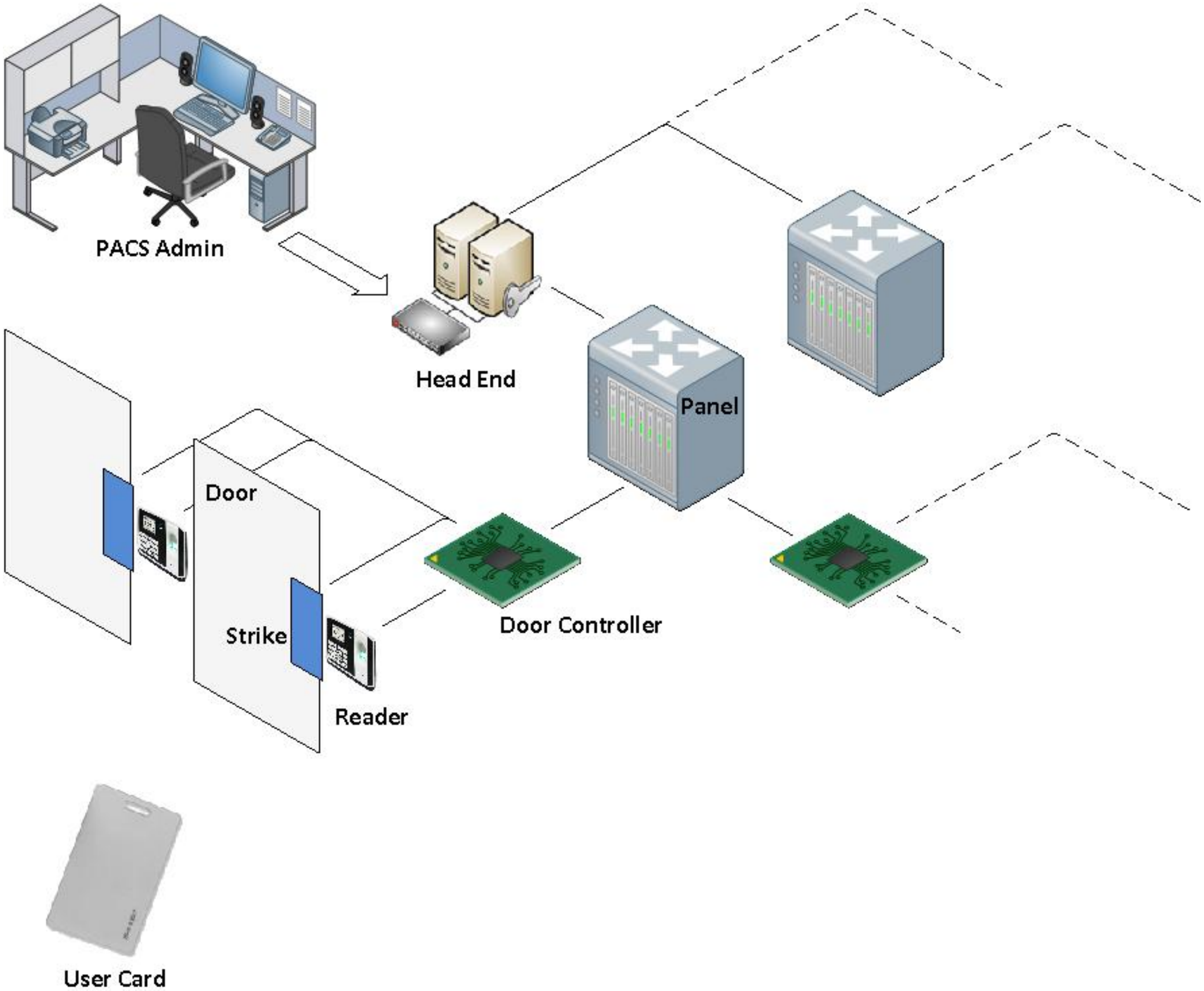
Figure 3-1, FICAM Roadmap Overview of PACS within the Overall Infrastructure



3.1 Current PACS Architecture

A typical current PACS architecture will look similar to that shown in Figure 3-2. While different PACS vendors may name their components differently, the essential functionality of all systems is the same.

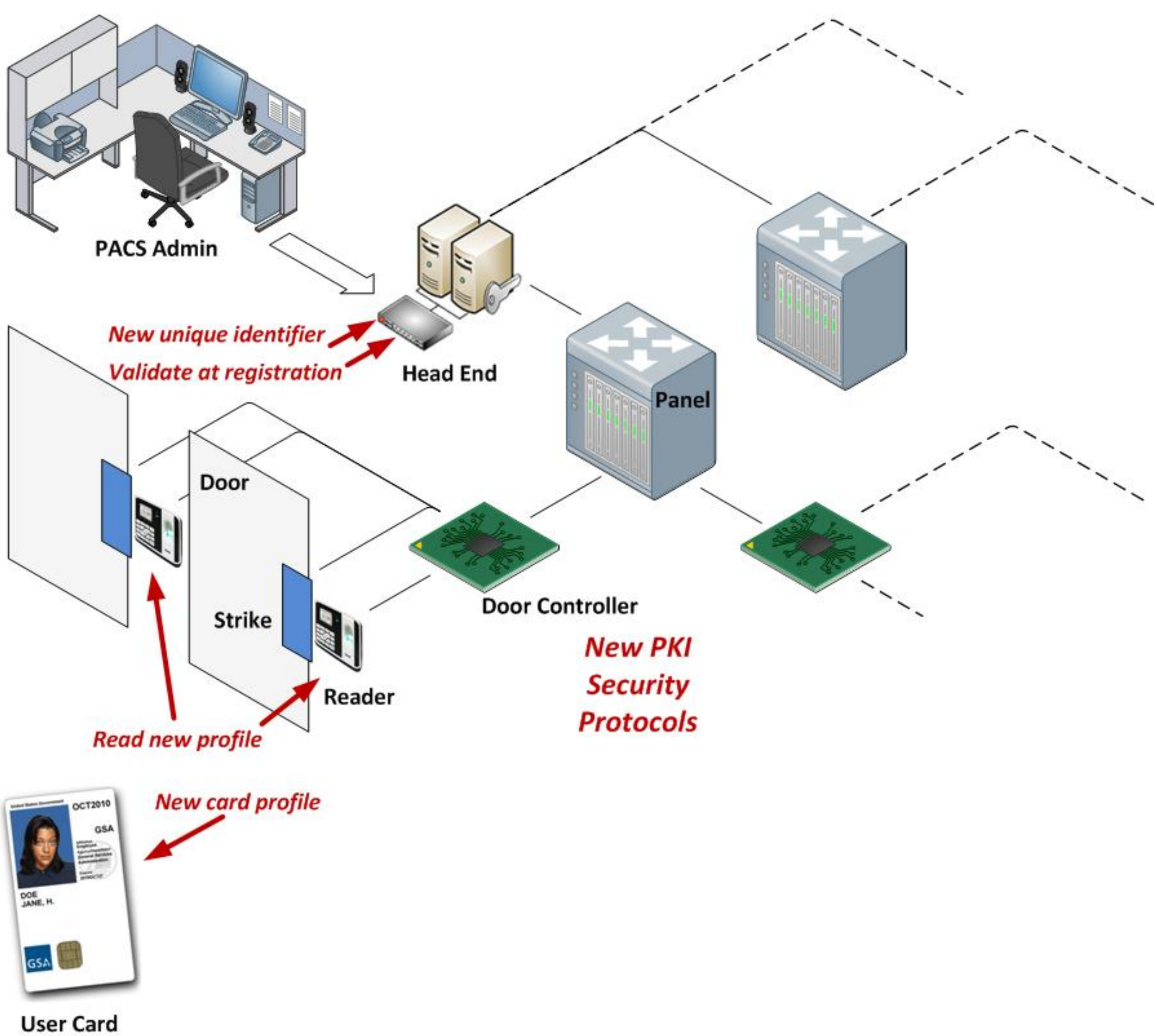
Figure 3-2, Typical Current PACS System



3.1.1 PACS and the introduction of PIV and PIV-I Cards

The introduction of PIV and PIV-I Cards represents major steps forward in standardization of access control within the Federal Government. There are now standard identity cards that are recognizable and trustable by all government agencies. While using a PIV or PIV-I Card in existing PACS will require some changes, it may not necessitate a complete replacement of the PACS components. Figure 3-3 shows where these changes may affect the system.

Figure 3-3, FIPS 201 Changes to PACS



Upgrading or replacing an existing PACS to enable it to properly use a PIV or PIV-I Card as the user identity card requires a few significant changes:

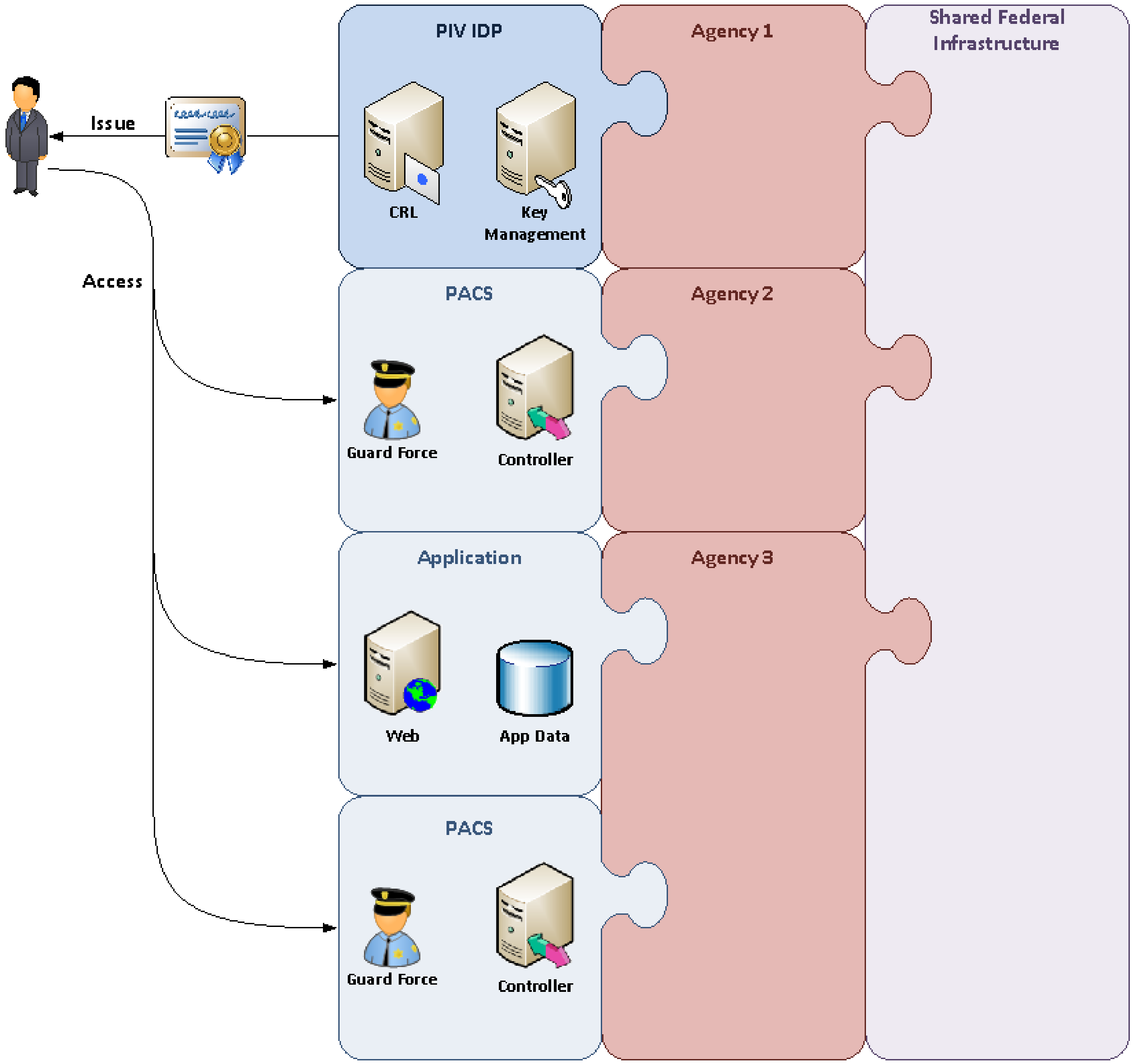
1. PIV and PIV-I Cards are an [ISO/IEC 14443] type smart card with a contactless interface that operates at 13.56 MHz. In addition, some authentication mechanisms require using the contact interface. The most common identity cards in use today are contactless proximity cards which operate at 125 kHz. 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 and PIV-I Cards employ a new profile for representing the data on the card. The system must therefore add functionality to read and interpret this new profile.
3. The PACS must be changed to use the Federal Agency Smart Credential - Number (FASC-N) Identifier as defined in [NIST SP 800-73-3] Part 1 Section 3.1.2.
4. Each PIV-I Card contains a unique identifier called a UUID. The UUID value is in accordance with [RFC 4122]. This functionality must be added to extract this unique identifier from the card data, and to use it in the access control decision process.
5. To ensure secure use of PIV and PIV-I Cards, some level of authentication and validation must be performed as part of the registration process and at the time-of-access. This is new functionality that should be added to the system.
6. The communication protocols between PACS components must be able to process much larger data elements (i.e., the signed CHUID).
7. The PACS depends on identity and credential information from the overall ICAM infrastructure.

3.2 Target PACS Architecture

Figure 3-4 depicts the target concept for cross-agency access. A PIV or PIV-I Card issued to a user by any agency can be used for access to various systems at other agencies that have integrated with the Shared Federal Infrastructure – this includes Enterprise PACS (E-PACS)[14]. Figure 3-4 is adapted from the technical layer of the FICAM segment architecture ([FICAM Roadmap] Section 3.2.5), which depicts the target concept for cross-agency access.

[14] http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

Figure 3-4, FICAM Roadmap Federal Enterprise Target Conceptual Diagram



The target state for E-PACS includes the following steps:

1. After a determination is made to authorize the cardholder to have access to a facility, the cardholder's credential is provisioned into the PACS.
2. A Cardholder desires access to a facility/area and presents his card to the card reader on the attack side (or non-secure side) of the access point.
3. The Cardholder presents his/her PIV or PIV-I Card (contact or contactless interface) to the card reader. The Cardholder performs authentication using one or some combination of authentication

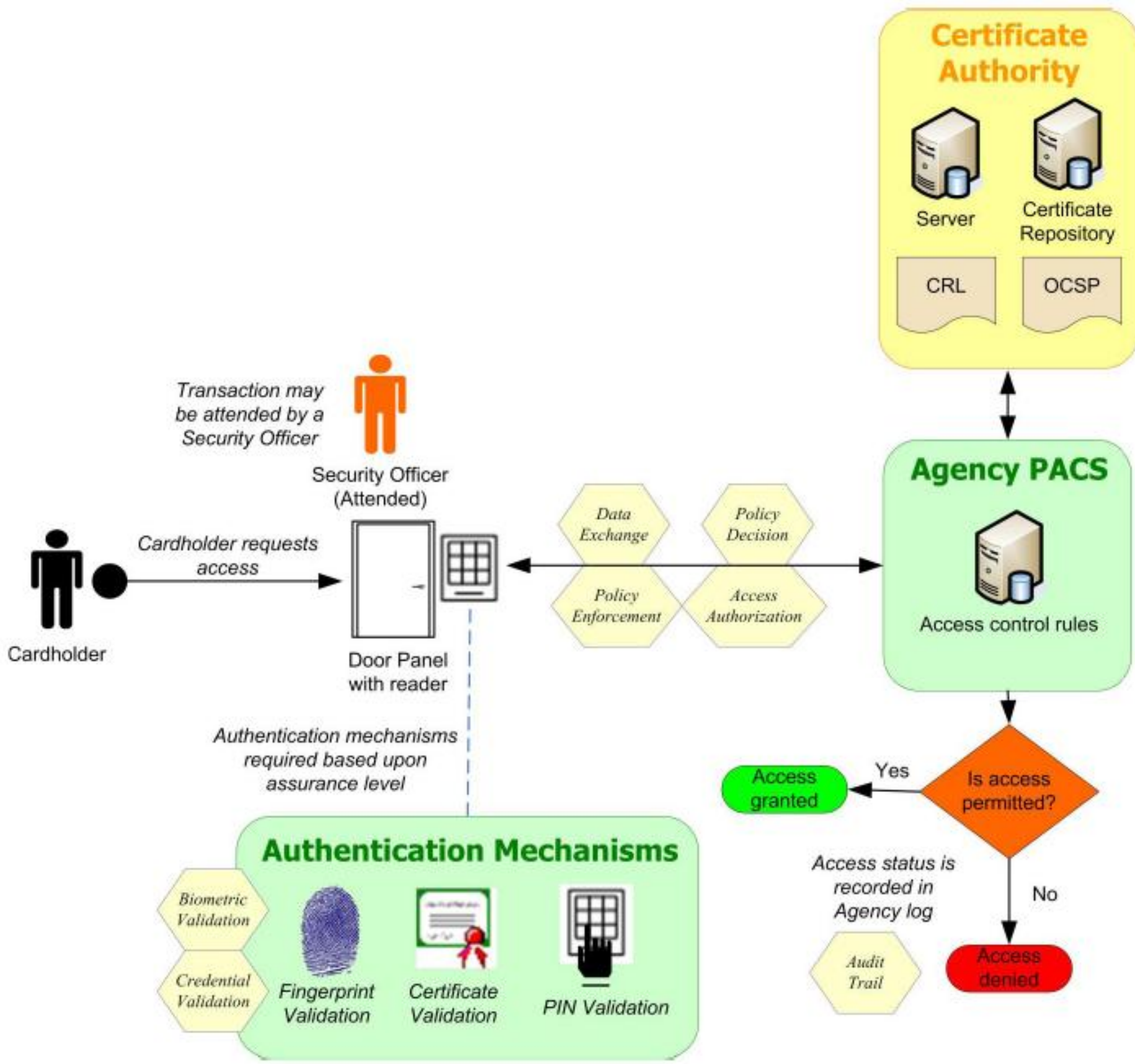
mechanisms discussed in Section 4 (see Section 8, and Table 8-3 in particular for more discussion).

4. Upon successful authentication of the card, the cardholder, and subsequent authorization by the PACS, the controller notifies the locking mechanism, the entry point opens, and the Cardholder is granted access to the facility/area. If authorization is unsuccessful, the access attempt is denied and the locking mechanism remains locked.
5. The PACS creates a record of the access event based on local audit policy.

Figure 3-5 shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.[15] Figure 3-5 is the desired target state process flow diagram drawn from [FICAM Roadmap] Use Case 8, *Grant Physical Access to Employee or Contractor*.

[15] http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

Figure 3-5, Generic FPACS Functions



4. SMARTCARD AUTHENTICATION MECHANISMS

PIV and PIV-I Cards themselves provide four electronic identification and authentication mechanisms, which alone or in conjunction with other authentication mechanisms can establish confidence (to varying levels of assurance) in the identity of the cardholder:

- **Authentication Certificate –** (PKI-Auth[16]) allows PKI-based authentication only accessible via the contact interface when the user PIN is provided;
- **Biometric[17]** – authentication of the cardholder's fingerprints using biometric templates on the card, including verification of the signature and signer;
- **Cardholder Unique Identifier (CHUID)** – contact or contactless read of the CHUID object, including verification of the signature and signer; and
- **Card Authentication Key (CAK)** – allows cryptographic authentication of the card via contact or contactless interface. This is currently an optional certificate on the PIV Card, and a required certificate on the PIV-I Card. CAK may also be a symmetric key on PIV Cards.

[FIPS 201] offers additional material on authentication mechanisms and levels of confidence. [NIST SP 800-116] has more recent and more detailed information in this regard. This document builds on [NIST SP 800-116] guidance for PACS.

[NIST SP 800-116] summarizes six possible authentication mechanisms using the PIV or PIV-I Card to establish confidence in the identity of the cardholder. Table 4-1 lists the authentication mechanisms, their authentication factors[18], and which interface(s) they can be used with. See Table 6-1 and Section 8 for further discussion. Note the following about Table 4-1:

1. The PIV/PIV-I PIN is required to be presented to the card when BIO, BIO (A) or PKI-Auth mechanisms are used. The PIN is considered as a factor (what you know) only when the PACS has an active cryptographic proof it can trust the card the PIN was presented to (CAK, PKI-Auth) and the BIO information comes from that same card.
2. Rows in gray do not appear in the original [NIST SP 800-116] Table 7-1.

[16] Referred to as "PKI" in [NIST SP 800-116].

[17] Biometric data is accessible only after providing the correct PIN and only via the contact interface. In addition, as biometric match-on-card and other technologies such as iris scanning are not currently addressed in authoritative documents, this document does not address them either.

[18] The level of assurance for one factor is not the same for the global levels of assurance defined by [OMB M-04-04]. See Table 8-3 for more details.

Table 4-1, PIV/PIV-I Authentication Mechanisms

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors[19]	Interface
PKI-Auth + BIO-A	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)	Observed Fingerprint (Medium Assurance Factor)	3	Contact
PKI-Auth + BIO	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)	Fingerprint (Low Assurance Factor)	3	Contact
CAK[20] + BIO-A	Smartcard with crypto key (High Assurance Factor)	PIN with indirect verification assumption (Low Assurance Factor)	Observed Fingerprint (Medium Assurance Factor)	3	Contact
CAK[20] + BIO	Smartcard with crypto key (High Assurance Factor)	PIN with indirect verification assumption (Low Assurance Factor)	Fingerprint (Low Assurance Factor)	3	Contact
BIO-A	Card (Low Assurance Factor)		Observed Fingerprint (Medium Assurance Factor)	2	Contact
PKI-Auth	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)		2	Contact
BIO			Fingerprint (Low Assurance Factor)	1	Contact
CAK[20]	Smartcard with crypto key (High Assurance Factor)			1	Contact/Contactless
CHUID + VIS	Printed Security feature on the Smartcard (Low Assurance Factor)			1	Contact/Contactless

[19] Low assurance factor indicates that there is no cryptographic verification that the information comes from (or is verified by) the card.

[20] The CAK may be a symmetric or an asymmetric key. Only Asymmetric keys provide interoperability between PACS and unrelated credential issuers.

For PIV and PIV cards, the authentication mechanisms are defined as follows (see Section 8 for more discussion):

A. **VIS**: Visual authentication entails inspection of the topographical features on the front and back of the PIV or PIV-I Card. The human guard checks to see that the PIV or PIV-I Card looks genuine, compares the cardholder's facial features with the picture on the card, checks the expiration date printed on the card, verifies the correctness of other data elements printed on the card, and visually verifies the security feature(s) on the card. The effectiveness of this mechanism depends on training, skill, and diligence of the guard (e.g., to match the face in spite of changes in beard, mustache, hair coloring, eye glasses).

B. **CHUID + VIS:** The controller controlling access to the door receives frequent updates from the PACS server and validates the CHUID on the PIV or PIV-I Card. In order to achieve single factor authentication, the asymmetric signature of the CHUID must also be validated[21].

C. **CAK:** Authentication of card is completed using the CAK, a unique cryptographic key that may be used on a contactless or contact card in a challenge/response protocol. The PACS obtains the CAK certificate from the PIV or PIV-I Card, validates the certificate (check the certificate‘s expiration date, signature validation, revocation status) and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate. The certificate and rights to access the facility are provisioned in the PACS. For example, when the symmetric CAK is present and used (non interoperable mechanism), the card reader obtains the diversification element from the card, calculates the card diversified key, and uses the key in a challenge/response to verify the card is authentic.

D. **BIO:** The PIN is presented to the card allowing the reader to read the reference biometric information and to attempt a match with the live sample. The cardholder provides a live fingerprint sample, which is validated against the biometric information embedded within the PIV or PIV-I Card. The PACS verifies the signature on the biometric data object. This authentication mechanism does not include authentication of the PIV or PIV-I Card.

E. **BIO-A:** Biometric authentication performed in the presence of a human guard is called BIO-A. The PIN is presented to the card allowing the reader to read the reference biometric information and to attempt a match with the live sample. In addition to the steps in process D, a Security Officer supervises the use of the PIV or PIV-I Card and the submission of the PIN and the biometric sample by the cardholder.

F. **PKI-Auth[22]:** The Cardholder provides PIN for validation by the PIV or PIV-I Card. The PIV or PIV-I Card validates the PIN allowing use of the PKI-Auth Key. The PACS validates the certificate (check the certificate‘s expiration date, signature validation, revocation status) and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate[23]. As a result of the successful cryptographic challenge/response, the successful PIN presentation is confirmed to the PACS.

---

[21] [NIST SP 800-116]

[22] Referred to as "PKI" in [NIST SP 800-116].

[23] See PIA-5. Certificate validation may be performed by integrated validation services.

G. **CAK + BIO:** This includes an integration of the steps from options C and D. The verification of the PIN can be trusted because the PIV or PIV-I Card is authenticated by the CAK.[24]
H. **CAK + BIO-A:** This includes an integration of the steps from options C and E. The verification of the PIN can be trusted because the PIV or PIV-I Card is authenticated by the CAK.[24]
I. **Card PIN**: The presentation of the PIN to the card is not considered a factor by the PACS unless the PACS can validate that the card is a valid PIV or PIV-I Card. As such, it does not appear in the table as an independent mechanism. There are only two mechanisms for determining that a card is a valid PIV or PIV-I Card, and both use cryptographic challenge/response:
   a. CAK, which does not require a PIN but indicates the card can be trusted; and
   b. PKI-Auth, which requires the correct PIN for the card to execute the authentication.

The following authentication-related differences between PIV and PIV-I Cards should be noted:

1. The PIV Card includes a FASC-N to uniquely identify it, and thus avoid identifier collisions. However, the FASC-N structure does not support its use beyond the U.S. Government. Therefore, PIV-I Cards include an RFC 4122 generated UUID in accordance with [NIST SP 800-73] Section 3.3 in the GUID field of the CHUID, as well as in the subject-alt-name extension of the authentication certificate in accordance with [PIV-I Profile]. RFC 4122 UUID construction and format rules ensure that the risk of PIV-I identifier collision is infinitesimal.
2. The PIV-I Certificate for Authentication is issued under the Common Policy's PIV Policy. All certificates issued under this policy conform to [PIV-I Profile].
3. The PIV Certificate for Authentication is issued under the PIV Policy defined in the Common Policy. All certificates issued under this policy conform to [PIV Profile].

[24] [NIST S P800-116] Appendix C uses the acronym CBP to define the combined authentication mechanisms of CAK + BIO or CAK + BIO-A. In addition, [NIST S P800-116] Appendix C specifies what authentication mechanism (or combination) can be used to move from one area (Uncontrolled, Controlled, Limited, Exclusion) to another.

5. GSA's Approved Products List (APL)

OMB designated GSA as the Executive Agent for government-wide acquisitions for the implementation of HSPD-12. OMB has directed federal agencies to purchase only products and services that are compliant with the federal policy, standards and numerous supporting technical specifications. In support of these mandates, GSA established the GSA FIPS 201 Evaluation Program Approved Products List (APL)[25]. More information about the GSA APL including its product categories and approval procedures can be found at http://fips201ep.cio.gov/.

The GSA APL identifies functional categories that may or may not be useful or relevant to PACS, as it supports the entire FIPS 201 spectrum, including enrollment, card production, issuance systems, and card readers for both logical and physical access applications. Specific categories have been identified that do support PACS. These categories include (not the exhaustive list):

- Biometric authentication system
  - 1:1 services for PACS
- Caching Status Proxy
  - Server-based Certificate Status Protocol (SCVP) and cached Online Certificate Status Protocol (OCSP) results
- CAK Authentication System
  - PKI challenge/response using CAK for PACS
- Card Printer Station
  - Prints a valid card per the standard, and security features as appropriate
- Certificate Validator
  - Standard Path Discovery and Validation (PDVal) tools
- PACS readers that transmit a 75-bit FASC-N
  - Card Reader – CHUID (Contact)
  - Card Reader – CHUID (Contactless)
  - Card Reader – CHUID Authentication Reader (Contact)
  - Card Reader – CHUID Authentication Reader (Contactless)
  - Card Reader – Transparent
  - CHUID Authentication System
- Facial Image Capturing (Middleware)
- Facial Image Capturing Camera
- Single Fingerprint Capture Device

It is important to note that GSA does functional testing. Simply selecting components on the APL when implementing a PACS (both as an Original Equipment Manufacturer and facility owner) does not assure that the system will perform in a way that results in a holistic, secure system as described in [NIST SP 800-116] and as required by [OMB M-11-11].

[25] More information about the GSA APL, including its product categories and approval procedures, can be found at http://fips201ep.cio.gov/index.php. The current APL can be found at http://fips201ep.cio.gov/apl.php.

6. PACS THREATS

As [NIST SP 800-116] notes, the PIV System protects the trustworthiness of PIV and PIV-I Cards, and data objects through PIV or PIV-I Card access rules and digital signatures. Overall trust in the execution of a PIV authentication mechanism is also dependent on correct operation of the PIV or PIV-I Card, the PACS, and the PIV or PIV-I Card validation infrastructure, and, to a degree, on protecting the confidentiality, integrity, and availability of the communication channels among them. Attacks may, therefore, be directed against any of these components, with varying difficulty and potential impact. There are many different attacks that can be perpetrated against a PACS. Table 6-1 summarizes the most common of these threats.

Table 6-1, Summary of Common PACS Threats

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
			Human-Exploitation Threats			
1	Social Engineering	Attacker persuades a cardholder to give them possession of the PIV or PIV-I Card.	See PAT-1.	See also [NIST SP 800-116].	Moderate	Low
2	Use of Unreported Lost or Stolen Card	Attacker steals or finds a card and uses it to gain access, before it is reported lost or stolen.	Use an authentication mechanism that requires PIN or biometric verification of user's identity. See PAT-1. In addition, establish a robust policy and process for reporting lost/stolen cards.	See also [NIST SP 800-116].	High	Low
			Card-based Threats			
3	Identifier Collision	An identifier collision occurs when the identifier used by the PACS is present in more than one Card. This can only happen as the result of a PACS design flaws, such as truncating identifiers.	PACS should not truncate identifier and should do a complete verification of Card identifiers enrolled in its database. Verification of the digital signatures of the card data objects prevents this from being possible. See PIA-3.3.	Using a strong hash is possible under some circumstances for the PACS but only when uniqueness of identifiers and signatures have been verified at least once. See also [NIST SP 800-116].	Moderate	Low
4	Use of Terminated Card	Attacker uses a card that has not been de-authorized from the PACS	PACS should verify cards which have been revoked by issuers using CRL, OSCP, or other available mechanism. See PIA-3.5.	Issuers must publish revoked cards but there is a windows of time between which the card may be revoked by the issuer and the PACS not aware of it. See also [NIST SP 800-116].	High	Low

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
5	Visual Counterfeiting	Attacker mimics the appearance, but not the electronic behavior, of an actual PIV or PIV-I Card. A replica may be created by color photocopying or graphic illustration methods and color printing to blank stock.	Use one or more printed security features such as (e.g., Holograms, ghost image, microtext, laser engraving, faded area). See PIA-3.3. In addition, use the electronic features on the card (see Section 10).	Increases the cost of card issuance and may require equipment for security officers to verify the card surface. See also [NIST SP 800-116]. In addition, VIS inspection of a card alone is not sufficient to grant access (see Section 10).	High	High to Moderate
6	Skimming	Attacker uses a concealed contactless PIV Card reader with a sensitive antenna to obtain the free-read data from the PIV or PIV-I Card, which includes the CHUID and the certificates.	Use active card authentication which is not subject to CHUID replay attacks even on un protected channels. See PIA-3.3. In addition, use of the RFID sleeve protects the card from skimming while in the sleeve.	May also happen with the contact interface as shown by many ATM attacks. See CHUID replay attack in this table. See also [NIST SP 800-116].	Low	Low
7	Sniffing	Attacker uses a long-distance receiver to capture the entire message transaction between the contactless reader and the PIV or PIV-I Card.	Use active card authentication which is not subject to CHUID replay attacks even on un protected channels. See PIA-3.3.	May also happen with the contact interface as shown by many ATM attacks. See CHUID replay attack in this table. See also [NIST SP 800-116].	Low	Low
8	Electronic Cloning	Attacker obtains a card and makes a copy of it, then uses it to gain access.	Use card active authentication (PKI-Auth or CAK). See PIA-3.3.	See also [NIST SP 800-116].	Moderate	Low

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
9	Electronic Counterfeiting	Injecting various FASC-N or UUID numbers to the PACS in attempts to discover a valid and authorized identifier. An alternate form of this attack is to guess multiple identifiers repeatedly. The alternate is mitigated by limiting the number of guesses (i.e., rate metering).	Verification of digital signatures (up to the trusted root) should be done on all data objects. This may require more verifications in a Federated Environment (e.g., name restrictions). See PIA-3.3.	Verification should be done (at a minimum) when the credential is first registered and the integrity of the data object should be verified at time of use (same data than when registered). See also [NIST SP 800-116].	Moderate	Low
10	Use of Expired Card	Attacker obtains an expired card (e.g., from a trashcan) and uses it to gain access.	Check expiration date of the credential. Physically destroy expired cards[26]. See PIA-4.	The CHUID as well as certificates contain expiration dates. Expiration dates for the specific mode of authentication must be checked (i.e. in CHUID mode, check CHUID expiration; in CAK mode, check CAK certificate).	High	Low

[26] See [GSA MSO] for steps for destroying a card.

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
11	Biometric Object Substitution	In the simplest form the attacker puts their own biometric object on a forged card. The attacker may also substitute a forged biometric on an otherwise valid card. In a more complex form the attacker may put their own valid biometric object on someone else's card in order to exploit someone else's privileges.	Verify the signature on the biometric object mitigates the simple forms of this attack by ensuring the biometric object is not forged. Countering the more complex form of this attack requires verification that the biometric object was issued with the other objects on the card (i.e., not substituted later). There are two potential countermeasures: -verify the security object on the card -authenticate another object on the card in addition to the biometric and verify that the identifiers for both objects are the same. See PIA-3.4.	Biometric objects are signed by the issuer, effectively binding the biometric object to the appropriate identifiers. This attack does not affect the trustworthiness of this binding or undermine biometric based authentication as long as the signature on the biometric object is verified. The more complex form is only useful to reduce the overall assurance when multiple authentication mechanisms are used together.	Low	Low
12	CHUID Replay Attack	Attacker installs listening device near PACS device (e.g., door) to capture access information, and the replays the captured information to the PACS device.	Use authentication mechanism not subject to replay, such as CAK or PKI. See PIA-3.3.	Use of the CHUID is subject to replay.	Moderate	Low
			Information-based Threats			
13	Trust Anchor Compromise	Attacker tells PACS that a bad CA should be trusted.	Trust anchors, like any software updates, should be protected against change by unauthorized users. See PSC-2.		Moderate	Low

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
14	Provisioning Attack	Attacker inserts bad accounts into the PACS to gain access.	Access to PACS data base needs to be controlled using tokens of equal or higher assurance than the access control tokens themselves. See PAU-4and PAU-5.	Conduct background investigations and require certifications on system by administrator.	Moderate	Low
15	Insider Attack with Electronic Counterfeiting	Attacker obtains identifiers from the Head End, which stores mappings of identifiers to access privileges. Attacker then uses the identifiers to obtain access privileges.	Identifiers should be as random as possible (e.g. UUID) and not structured (e.g. FASC-N). The data base in which they reside should be protected. Best practices encrypt this data. The best countermeasure is to make sure no identifier used alone (with no factor) allows access. See PIA-3.3.	Identifiers can also be obtained from the token themselves (identifier harvesting attacks). Identifiers are not authenticators, and by themselves represent zero factors of authentication.	Moderate	Low
			Man-in-the-Middle Threats			
16	Biometric Spoofing	Attacker obtains a copy of a cardholder's fingerprint from an object that the cardholder has previously touched, fabricates a replica finger using plastic or some other molded substance, and then places the "fake" finger on the biometric reader to gain access.	Use liveness detection or biometric technology more resistant to spoofing (e.g., vein patterns). Combine biometric with another factor.	It is relatively easy to collect someone's fingerprint pattern, even outside of the PACS environment. There is no standard to verify/qualify live detection.	Moderate	Low
17	Controller Impersonation	Attacker pretends to be the Controller and propagates decisions to other components (e.g., tells Head End to tell Controller to open door).	Protect communication between PACS components and require authentication between elements.	Best practice is to sign and encrypt communications between PACS components. Line supervision provides limited integrity.	Low	Low

#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
18	Head End Impersonation	Attacker pretends to be the Head End and directs Controller to take actions (e.g., open door).	Protects communication between PACS components. PACS components should not allow access (or make a decision) for an area of higher assurance than the one in which they are.	This may not prevent an insider to tamper with an element for others to have access to the area. Best practice is to sign and encrypt communications between PACS components. Line supervision provides limited integrity.	Low	Low
			System-based Threats			
19	Reader Compromise	Attacker inserts device at the PACS reader to affect desired behavior or capture information from the reader that can be used to gain access.	Reader components should be protected against tampering using hardware and software integrity and authenticity controls.	No sensitive information should be stored on the edge.	Moderate	Low
20	Controller Compromise	Attacker logs into to Controller as trusted role and changes the Controller to gain access.	Controllers or secure readers should not allow access in an area of higher protection than the area they are in.	Use of tamper detection is also required for all critical components in a PACS.	Moderate	Low
21	Physical PACS Manipulation	Attacker tampers with PACS components directly to gain access.	Protects all PACS components with tamper detection switches and protection mechanisms.	Telecom closets and wiring runs should also be protected. Line supervision provides limited integrity.	Moderate	Low
22	Exceptions Attack	Attacker causes a PACS exception to occur, in order to gain access (e.g., CHUID too big)	All software in all elements should be coded to prevent such exceptions. Software and hardware should never lower the security when an exception happens (e.g., Power Fail does not allow the door to open, buffer overflow does not allow access,)	Software should be written by programmers following the following security principles: Authentication, Authorization, Data validation, Session management, Logging, Error handling, Cryptography, Performance, Code quality.	Moderate	Low

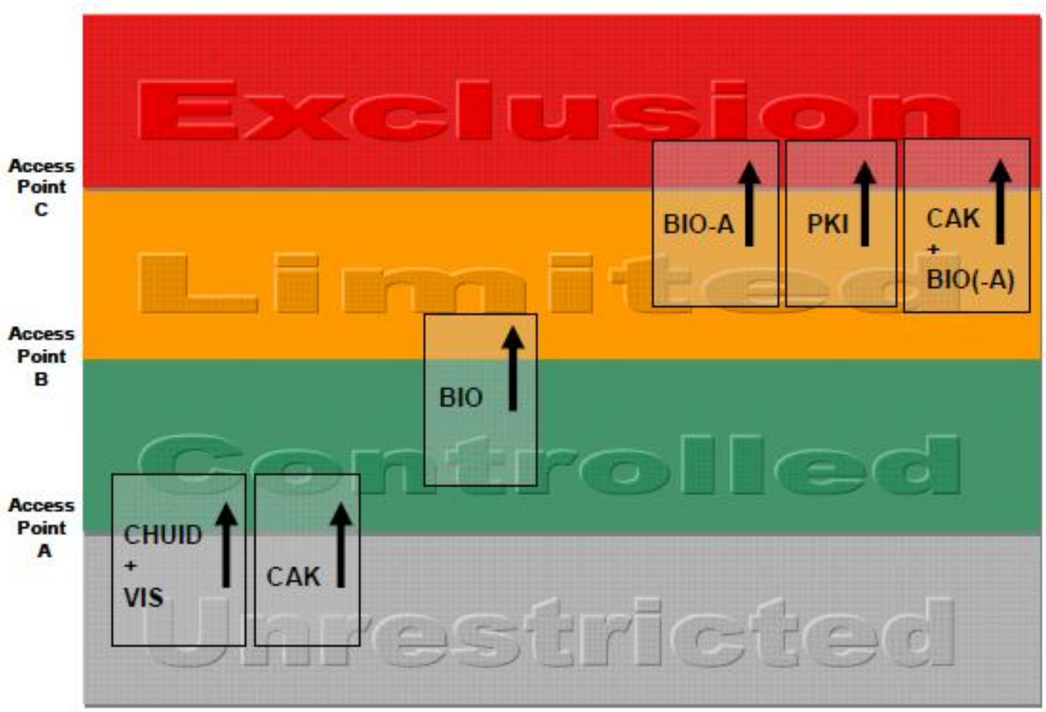
#	PACS Threat	Description	Countermeasure	Comment	Likelihood without Counter measure	Likelihood with Counter measure
23	Denial of Service Attack	Attacker attempts to make the network unavailable to the PACS so the PACS cannot receive fresh revocation data, for example. This attack could allow someone in with a recently-revoked credential.	Trigger an alarm indicating Denial of Service attack. In addition, use cached revocation data during the attack.	If you're not caching, you are subject to a Denial of Service attack.	Moderate	Moderate
24	Environmental Attack	Attacker does something to the environment (e.g., start a fire, turn power off) in order to initiate a PACS action (e.g., unlock doors to allow escape from fire).	PACS should be able to modify its access rules based on the security conditions. Exception conditions rules should be defined ahead of time.	Most facilities react to fail/safe by allowing doors to automatically open allowing people to get out.	High	High to Moderate

7. SUMMARY OF EXISTING PACS GUIDANCE

7.1 NIST SP 800-116 Risk Model

NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* [NIST SP 800-116], introduces the concept of Unrestricted, Controlled, Limited, and Exclusion security areas to facilitate risk-based PIV authentication as needed for different areas within a facility. In addition, [NIST SP 800-116] specifies the authentication mechanisms commensurate for each security area. Figure 7-1 illustrates the innermost use of each PIV authentication mechanism. A mechanism may be used at the interface it straddles (e.g., BIO on the interface between Controlled and Limited) and also at any interface below this one (e.g., BIO also on the interface between Unrestricted and Controlled). All permitted combinations of mechanisms and interfaces are shown in [NIST SP 800-116] Appendix C. The permitted combinations follow from general rules, such as "In a traversal from Unrestricted to Exclusion, one factor must be presented to cross the first interface, two to cross the second interface, and three to cross the third interface" where the presented factors are viewed cumulatively beginning with the Unrestricted-to-Controlled interface.

Figure 7-1, Innermost Use of PIV Authentication Mechanisms

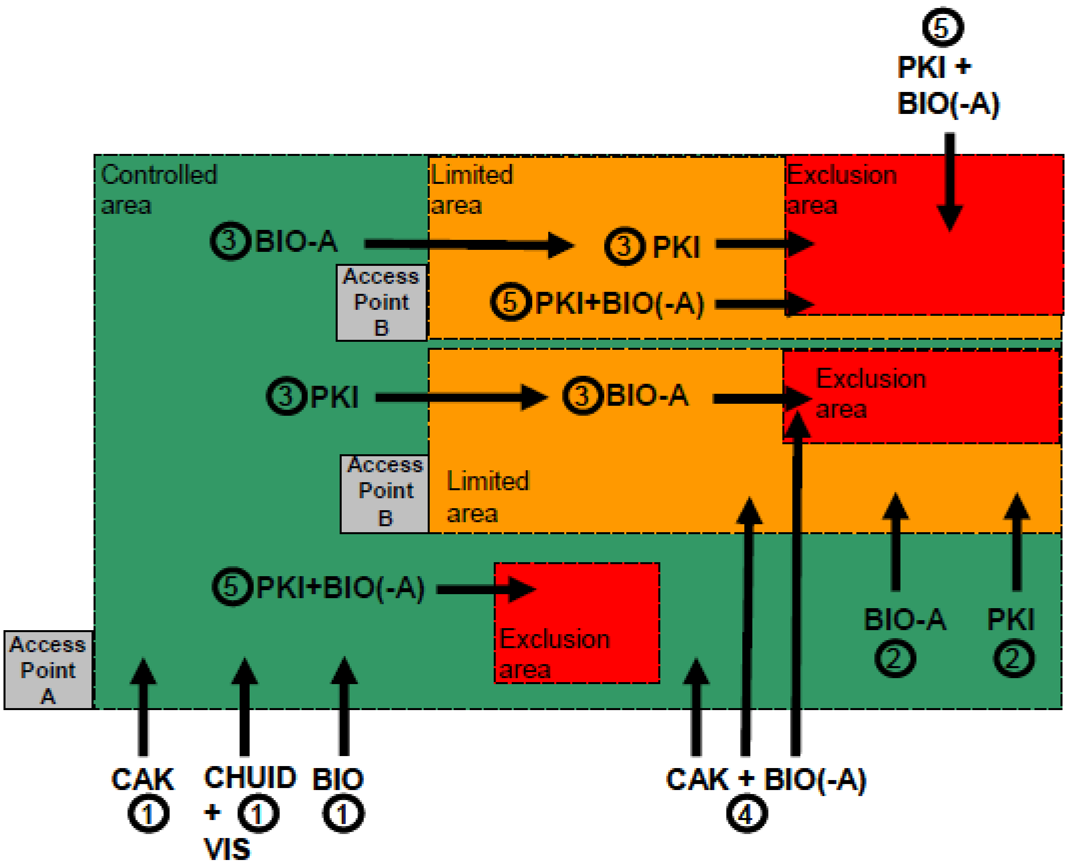


Since the areas accessible by different access points within a facility do not always have the same security requirement, the appropriate authentication mechanism should be selected to be consistent with the overall security requirements of the protected area. A given facility may need multiple authentication mechanisms.

Visual (VIS), Cardholder Unique Identifier (CHUID), Biometric (BIO), Attended Biometric (BIO-A), and PIV Authentication Key (PKI) are PIV authentication mechanisms defined in FIPS 201. Card Authentication Key (CAK) is an optional PIV authentication mechanism.

Figure 7-2[27] shows various authentication methods (and combinations) using PIV credentials to access the various type of areas defined in [NIST SP 800-116]. For example, accessing an Exclusion area requires three-factor authentication. One combination is to use PKI+BIO(A), as shown in option 5, to move from an Unrestricted area to an Exclusion area. Care should be taken when doing such combinations. For example, using a BIO to access the Controlled area (option 1) should not be followed by a BIO(A) when going into a Limited area. Using a PKI (option 2) provides more identity assurance for the subject.

Figure 7-2, Examples of Mapping PIV Authentication Mechanisms



27 [NIST SP 800-116]

The [NIST SP 800-116] risk-based model is defined in terms of maturity levels as follows[28]:

- **Maturity Level 1**—Ad hoc PIV verification.
- **Maturity Level 2**—Systematic PIV verification to Controlled areas. PIV Cards and currently deployed non-PIV PACS cards are accepted for access to the Controlled areas at this level.
- **Maturity Level 3**—Access to Exclusion areas by PIV or exception only. Non-PIV PACS Cards are not accepted for access to the Exclusion areas at this level.
- **Maturity Level 4**—Access to Limited areas by PIV or exception only. Non-PIV PACS Cards are not accepted for access to the Limited or Exclusion areas at this level.
- **Maturity Level 5**—Access to Controlled areas by PIV or exception only. Non-PIV PACS Cards are not accepted for access to any areas at this level.

[28] Currently, [NIST SP 800-116] addresses just PIV.

8. ENTERPRISE PACS SECURITY FUNCTIONS

[NIST SP 800-53] provides a general framework for applying security controls to any federal information system, regardless of its mission. As a federal information system, an E-PACS is subject to these controls and the Certification and Accreditation (C&A) process to ensure that it is correctly protected.[29]

However, in addition to the need to be secured, an E-PACS itself has an important security mission of its own: to protect federal facilities and its employees, contractors, and visitors. So, in addition to the [NIST SP 800-53] controls that specify how it should be protected, there is also a need for a set of security controls to specify what is needed to assure that the E-PACS provides adequate protection.

The controls listed in this Section follow the framework established in [NIST SP800-53]. These controls are specific to the system defined as an E-PACS. They are in addition to those in [NIST SP 800-53] that address the PACS as an IT system. These controls should inform your risk assessment.

The prefix 'P' has been added to [NIST SP 800-53] control families when control family discussion pertains to E-PACS. For example, the Identification and Authentication (IA) control family is specified as PIA when applicable to E-PACS.

[29] See [OMB M-10-15], which clarifies that 1) PACS are IT systems, even on a stand-alone network; and 2) you have to perform the activities of the NIST Risk Management Framework, including security authorization, on them.

Table 8-1, SP 800-53 Security Control Families

Class	ID	Control Family	NIST SP 800-53	E-PACS
Technical Controls	AC	Access Control	✓	✓ PAC
	AU	Audit and Accountability	✓	✓ PAU
	IA	Identification and Authentication	✓	✓ PIA
	SC	System and Communications Protection	✓	✓ PSC
Operational Controls	AT	Awareness & Training	✓	✓ PAT
	CM	Configuration Management	✓	✓ PCM
	CP	Contingency Planning	✓	✓ PCP
	IR	Incident Response	✓	
	MA	Maintenance	✓	
	MP	Media Protection	✓	
	PE	Physical and Environmental Protection	✓	✓ PPE
	PS	Personnel Security	✓	
	SI	System and Information Integrity	✓	
Management Controls	CA	Security Assessment and Authorization	✓	✓ PCA
	PL	Planning	✓	✓ PPL
	PM	Program Management	✓	
	RA	Risk Assessment	✓	✓ PRA
	SA	System and Services Acquisition	✓	

Note that the E-PACS security controls use a three letter designator, "P", followed by the two letter designator of the corresponding [NIST SP 800-53] Security Control Family.

Each facility has a Facility Security Level (FSL) that is determined based on six factors:

1. Mission Criticality (1 to 4 pts)
2. Symbolism (1 to 4 pts)
3. Facility Population (1 to 4 pts)
4. Facility Size (1 to 4 pts)
5. Threat to Tenant Agencies (1 to 4 pts)
6. Intangible Adjustment (+ /- adjustment)

FSL	Pt Range
I	5-7
II	8-12
III	13-17
IV	18-20

Security controls may be satisfied in multiple ways. Not each is appropriate for every FSL. The control listing shows the extent to which each security control is appropriate.

8.1 Technical Controls

Technical security controls (i.e., safeguards or countermeasures) for an E-PACS are primarily implemented and executed by PACS through mechanisms contained in the hardware, software, or firmware components of the system or interconnected systems.

8.1.1 Identification and Authentication

The security controls in the Identification and Authentication (I&A) family specify the full set of controls to completely authenticate the cardholder.

Table 8-2, Summary of Identification and Authentication Controls

Class	Family	ID	Control
T	PIA	PIA-1	Identification and Authentication Policy Implementation
T	PIA	PIA-2	Authentication Modes
T	PIA	PIA-3	Identity Factor Authentication
T	PIA	PIA-3.1	Accepting Device (AD)
T	PIA	PIA-3.2	Validation of Trusted Origin (VTO)
T	PIA	PIA-3.3	Active Authentication
T	PIA	PIA-3.4	Protection of Authenticator (POA)
T	PIA	PIA-3.5	Revocation Check (RC)
T	PIA	PIA-4	Signature Validation
T	PIA	PIA-5	Full Path Validation

Class	Family	ID	Control
T	PIA	PIA-6	Cross-Agency Interoperable Authentication
T	PIA	PIA-7	Card Revocation Check Mechanisms
T	PIA	PIA-8	Provisioning via Import
T	PIA	PIA-9	Provisioning via Registration
T	PIA	PIA-10	I&A for Administration

8.1.1.1 PIA-1: Identification and Authentication Policy Implementation.

Control: The E-PACS should implement the identification and authentication measures specified in the Facility Access Control Policy, including: authentication modes, accessing populations, time of day restrictions, and threat level restrictions and exceptions.

Detailed Guidance: The Facility Access Control Policy (PPL-1) documents the policy that the E-PACS should enforce during identification and authentication (PPL-3, PPL-4, PPL-5, and PPL-6). This control specifies that E-PACS should implement the documented policy.

8.1.1.2 PIA-2: PACS Authentication Modes.

Control: The E-PACS should support one or more PIV-enabled authentication modes.

Detailed Guidance: There are three types of authentication factors – a) “something you have”, for example, possession of the PIV Card; b) “something you know”, for example, knowledge of the PIN; and c) “something you are”, for example, presentation of live fingerprints by a cardholder. There are many ways these factors can be used in combination to authenticate a cardholder. Broadly, these are categorized as 1-factor, 2-factor and 3-factor. Each specific combination is an authentication mode.

Table 8-3 enumerates the FPACS-enabled authentication mechanisms.

“CL?” indicates that the Authentication Mode is available on the contactless interface. All Authentication modes are available on the contact interface. “Int?” indicates that the Authentication Mode is interoperable across cards from other PIV issuers.

Any reference data used by the PACS as an authenticator (the PIN and/or BIO and/or symmetric key) must be protected by the PACS in accord with PIA-3.4. Without this protection, it is not a valid authentication factor.

Table 8-3, PACS-enabled Authentication Mechanisms

Factors	PACS-enabled Authentication Mechanism	Max Confidence	CL?	Int?	Factors
No Factor	PIN to PIV/PIV-I[30] (without cryptography)	No Confidence	CL	✓	
	CHUID (FASC-N, UUID)	No Confidence	CL	✓	
One Factor	CHUID+VIS	Little or No Confidence	CL	✓	Have
	BIO	Some Confidence	-	✓	Are
	CAK	Some Confidence	CL		Have
	CHUID[31] + PIN to PACS	Some Confidence	CL	✓	Know
	CHUID + BIO to PACS	Some Confidence	CL	✓	Are
Two Factor	CHUID + PIN to PACS + BIO to PACS	High Confidence	CL	✓	Know + Are
	CAK + PIN to PACS	High Confidence	CL		Have + Know
	CAK + BIO to PACS	High Confidence	CL		Are + Have
	BIO-A	High Confidence	-	✓	Have + Are
	PKI-Auth	High Confidence	-	✓	Know + Have
Three Factor	PKI-Auth + BIO	Very High Confidence	-	✓	Know + Are + Have
	PKI-Auth + BIO to PACS	Very High Confidence	-	✓	Know + Are + Have
	CAK + BIO	Very High Confidence	-		Know + Are + Have
	CAK + BIO to PACS + PIN to PACS	Very High Confidence	CL		Know + Are + Have

[30] Note that PIN to PIV/PIV-I is not an authentication mechanism. Rather, PIN to PIV/PIV-I is only a component of PKI-Auth, BIO, or BIO-A.

[31] CHUID is not a factor without VIS. CHUID provides a possible index (e.g., FASC-N, UUID, GUID, human - entered). Here, for example, the CHUID is used as an index for PIN to PACS.

8.1.1.3 PIA-3: Identity Factor Authentication

Control: When authenticating an identity factor, the E-PACS should perform a complete factor authentication that includes the following five authentication elements:

1. **Accepting Device** – device that interacts with card or cardholder for authentication purposes.
2. **Verification of Trusted Origin** – ensuring that the authenticators come from a trusted source.
3. **Active Authentication** – authentication that requires activity by the card or cardholder such as a challenge/response, submitting a biometric sample, or a PIN challenge.
4. **Protection of Authenticator** – ensuring that the integrity and confidentiality of authenticators are not compromised.
5. **Revocation Check** – ensuring that authenticators have not been revoked.

Detailed Guidance: Though there are clear differences between the various types of have, know, and are identity factors, they each require the same five elements for a full and complete authentication. Omitting any of the authentication elements introduces a vulnerability that would permit a counterfeit or cloned card to be incorrectly authenticated (i.e., falsely accepted).

Each of the five authentication elements is given a control. These are enumerated in PIA-3.1 to PIA-3.5. Table 8-4 highlights the authentication elements applied to have, know, and are factors.

Table 8-4, Authentication Elements

	Have Factors	Know Factors	Are Factors
Authentication Mode:	• CHUID + VIS • PKI • CAK	• PIN to PIV/PIV-I[32] • PIN to PACS	• BIO-A • BIO • BIO to PACS
PIA-3.1 **Accepting Device**	• Smart Card Reader	• PIN PAD	• Biometric Reader
PIA-3.2 **Verification of Trusted Origin**	• Verify signature on the CHUID and validate associated Content Signer Certificate • PKI - Signature Check on PKI Certificate • CAK (Asymmetric) - Signature Check on CAK Certificate • CAK (Symmetric) – knowledge of shared secret • See PIA-5	• PIN to PIV/PIV-I – trust transferred by PIV Authentication Private Key • PIN to PACS – Secure connection to authoritative reference	• Verify signature on the biometric and validate associated Content Signer Certificate • BIO to PACS – Protected storage for Biometric Reference Template • See PIA-5

[32] PIN to PIV/PIV-I is a knowledge factor only if the identity card is verified as a PIV or PIV-I Card through another authentication mechanism such as CAK or PKI-Auth.

	Have Factors	Know Factors	Are Factors
PIA-3.3 **Active Authentication**	• Challenge Response	• PIN to PIV/PIV-I – Verified on Card, crypto channel transfers trust to PACS • PIN to PACS – Verify in PACS	• Biometric Match
PIA-3.4 **Protection of Authenticator**	• Protection from Modification by non-vetted entities • Protection from duplication is desired, and is typically achieved by active authentication (see PIA-3.3)	• PIN to PIV/PIV-I – provided by FIPS 140-2 Level 2 Module • Encrypted (or controlled access) at rest, • Secure delivery to comparison element	• Encrypted (or controlled access) at rest, • Secure delivery to comparison element
PIA-3.5 **Revocation Check** (within 18 hours)	For all PIV factors, revocation checking is always accomplished by performing PDVal and revocation checking on CAK or PIV Authentication certificates.		

8.1.1.4 PIA-3.1: Accepting Device (AD).
Control: The E-PACS should have Accepting Devices that support I&A requirements documented in the Facility Access Control Policy.

Detailed Guidance: The accepting device, commonly called a "reader," should accept the factor presented by the cardholder. Examples of ADs are card readers (contact and/or contactless), PIN pads, fingerprint readers, iris scanners, and other biometric devices. As with any PACS, the accepting devices should be equipped with internal tamper switches, mount tamper switches, line voltage monitoring, and other protections preventing attacks attempting to manipulate or copy the data collected or physical location of the device.

8.1.1.5 PIA-3.2: Validation of Trusted Origin (VTO).
Control: The E-PACS should verify (1) the issuer, (2) that the reference authenticator was created by the issuer and (3) that the reference authenticator has not been altered.
Detailed Guidance: This control establishes trust in both the issuer and the reference authenticator created by the issuer. See also PIA-5.

Where a digital certificate is provided for the reference authenticator (e.g. for a PIV Authentication Key, a Card Authentication Key, or a Biometric Object), signature validation and PDVal should be performed on the digital certificate to establish VTO.

Where secret key cryptography is used, establishing that the PIV or PIV-I Card contains the shared secret (the secret or symmetric key) establishes VTO. This is accomplished by establishing a mutually authenticated session based on the secret or symmetric key.

To mitigate substitution attacks, an E-PACS should always ensure the public key presented for authentication is the same one registered in the PACS database record for that credential. One way this can be achieved is using a secure hash. Without this check, an attacker can easily copy a known good CHUID and put his own PKI credentials on the card, defeating the access control decision process.

8.1.1.6 PIA-3.3: Active Authentication (AA).

Control: The E-PACS should verify that the factor presented (1) matches the reference authenticator and (2) is genuine and is not altered, cloned, forged, replayed or spoofed.

Detailed Guidance: Every authentication compares or "matches" a factor presented to the AD with a reference authenticator. This operation may be implemented or protected by one or more cryptographic mechanisms. The techniques for active authentication vary by factor. Examples of Active Authentication include:

1. Have: Challenge/Response (applies to both public and secret keys).
2. Have: Visual Inspection (VIS). In general VIS is a very weak form of AA, and is much weaker than any of the other environments. VIS is appropriate for facilities that require little or no confidence in the asserted identity.
3. Know: PIN to PIV/PIV-I (the PIV or PIV-I Card matches the presented PIN with the reference PIN stored on the card). PIN to PIV/PIV-I is a knowledge factor only if the identity card is verified as a PIV or PIV-I Card through another authentication mechanism such as CAK or PKI.
4. Knowledge: PIN to PACS (the PACS "matches" the presented with the registered PIN value securely stored in the PACS). See PIA-3.4.
5. Biometric: BIO and BIO-A (the PACS matches the biometric template provided by the PIV card with the live scan biometric presented by the cardholder).
6. Biometric: BIO to PACS (the PACS matches the biometric template securely stored in the PACS with the live scan biometric presented by the cardholder). See PIA-3.4.

8.1.1.7 PIA-3.4: Protection of Authenticator (POA).

Control: The E-PACS should protect the integrity and confidentiality of the reference authenticator used by PIA 3.3.

Detailed Guidance: The POA authentication element assures that the reference authenticator used in PIA-3.3 is adequately protected. The E-PACS should protect the authenticator where it is stored (at rest) and where it is transmitted (in motion.) There are four cases:

Case 1: The reference authenticator is carried by the PIV or PIV-I Card and provided by it to the PACS to perform the authentication. The PACS trusts that the PIV or PIV-I Card has correctly protected the Authenticator. Examples include:

1. Digitally-signed and PIN-protected biometric reference templates

Case 2: The reference authenticator is carried by the PIV or PIV-I Card and used by it to perform the authentication. The PACS trusts that the PIV or PIV-I Card has correctly protected the Authenticator, and that it has correctly performed the authentication. Examples include:

1. PIV Authentication Key

   a. PIN to PIV/PIV-I (trust that the PIV or PIV-I Card has authenticated the PIN is transferred to the PACS as a result of the PIV authentication Key challenge).
2. Card Authentication Key

Case 3: The referenced authenticator is registered in the PACS system. The PACS trusts itself to correctly protect the authenticator. Examples include:

1. PIN to PACS
2. BIO to PACS

Trust and integrity in these modes require the PACS to provide the following capabilities:

1. Digital signatures binding the credential number to the BIO and/or PIN (or an equivalent secure process);
2. Protection of the PIN and BIO with encryption at rest;
3. Secure communications from the PIN or BIO capture device to the system element that performs the comparison; and
4. Use of FIPS 140-2 validated cryptographic services.

Case 4: The PACS uses symmetric CAK between the card and the system. Symmetric CAK supports single or mutual authentication. This mode is an option offered by PIV, but is not interoperable across the federal enterprise (see Appendix A). Special handling of keys is needed to ensure integrity of this mechanism:

1. There is a secure key distribution mechanism to ensure all parts of the PACS receive and protect the symmetric keys appropriately.
2. All symmetric keys managed by the PACS are stored in and processed using FIPS 140-2 validated modules.
3. It is recommended that these keys be stored in a FIPS 140-2 Level 2 hardware device.
4. Diversification of card keys as well as rollover of the master keys should be used.

8.1.1.8 PIA-3.5: Revocation Check (RC).

Control: The E-PACS should verify that the credential presented has not been revoked.

Detailed Guidance: The RC authentication element verifies the credential created by the issuer should be accepted. RC is important because the issuer may have revoked the credential. There are two cases:

General Case: The organization that issued the PIV or PIV-I Card is different than the organization that operates the E-PACS. (This is the general case.) The E-PACS should perform an RC on the PIV Authentication Certificate (or the equivalent PIV-I Authentication Certificate or CAK Signature Certificate.) Further, if the reference authenticator has its own certificate (e.g. a certificate for the fingerprint biometric). The E-PACS should also perform a RC on the reference authenticator’s certificate, if applicable.

The E-PACS may perform the RC check at the time of access. As a performance optimization, the E-PACS may instead choose to perform RC checks in advance on “anticipation of access.” Whatever strategy is used, the E-PACS should positively determine that at the time of authentication, the RC status information is not older than 18 hours, the mandated maximum allowed by the FPKI Common Policy.

Special Case: Special Case: An organization may have an Enterprise IdM in place. In this environment, it is possible to have direct provisioning and de-provisioning of access records that are tightly bound to Human Resources processes. This provides a faster (and potentially more secure) way of managing revocation, as the organization does not have to wait on PKI to propagate CRL status information that may be over 18 hours stale. This method must be in addition to PKI status checking per PIA-3.2 and PIA-5.

Whenever a RC check is performed an Expiration Check should also be performed (see PIA-3.6).

8.1.1.9 PIA-3.6: Expiration Check (EC).

Control: The E-PACS should verify that the credential has not expired.

Detailed Guidance: The EC authentication element verifies the credential created by the issuer should be accepted. EC is important because the credential may no longer be valid, and issuers will not revoke expired credentials if they are compromised after expiration. The E-PACS should either check the expiration data in the CHUID, the CAK Certificate, or the Authentication Certificate according to the mode of authentication in use. In any of these cases, the signature of these objects should also be verified (see PIA-4).

8.1.1.10 PIA-4: Signature Validation

Control: The E-PACS should verify the signatures of any signed objects involved in authentication (e.g., authenticating acceptance devices, the card or the card holder).

Detailed Guidance: Signature validation of a data object provides validation of origin (trust in the creator of the data object) as well as a proof of data integrity (the data object has not been invented or modified since its creation). Signature validation may be achieved for static data objects by a verification of the hash value of the data objects against the hash value of the same data object stored after a full signature validation.

This control substantially overlaps control 3.2, Validation of Trusted Origin (VTO). However, signature validation is so central to all PKI-based authentications; this duplication allows signature validation to be explicitly recognized as a control in its own right.

8.1.1.11 PIA-5: Full Path Validation

Control: The E-PACS should use PDVal for signed objects involved in authentication (e.g., authenticating acceptance devices, the card or the card holder).

Detailed Guidance: Full path validation is central to all PKI-based authentications; this allows path validation to be explicitly recognized as a control in its own right, taking into account all possible revocations of intermediate CAs. PDVal should be performed at time of use or with a frequency in accordance with local policy. Best practice is to perform full path validation periodically, at least once per week. The PDVal status can then be cached to improve performance at time of access.

PDVal should be performed at time of use or with a frequency in accordance with local policy using cached status values. Depending on the local policy, PDVal may additionally require:

1. Policy Mapping
2. Basic Constraint Checking
3. Name Constraint Checking

The E-PACS should include an enterprise Certificate Path Validation (CPV) component that conforms with *NIST Recommendation for X.509 Path Validation*, May 3, 2004 that processes X.509 certification paths composed of X.509 v3 certificates and X.509 v2 CRLs.

The CPV component should support the following features:

1. Name constraints;
2. Policy Mapping;
3. Basic Constraint Checking;
4. Name Chaining;
5. Signature Chaining;
6. Certificate Validity;
7. Key usage, basic constraints, and certificate policies certificate extensions;
8. Full CRLs; and
9. CRLs segmented on names.

Defined in [RFC 5280].

The CPV component should verify that digital signatures and public keys in the certification path chain in accordance with [RFC 5280], using the appropriate algorithm as detailed in the certificate. That is, the CPV component should verify that the signature on each certificate in the path verifies using the public key in the preceding certificate, and the signature on the first certificate in the path verifies using a trust anchor's public key.

The CPV component should verify that issuer and subject names in certification paths chain in accordance with [RFC 5280]. That is, the CPV component should verify that the issuer of each certificate in the path was the subject of the preceding certificate, and the issuer of the first certificate in the path is the name associated with the trust anchor public key.

Note that full path validation includes checks of the expiration, revocation, and signature for each certificate in the path, implementing PIA 3.4, PIA-3.5, PIA-3.6, and PIA-4.

8.1.1.12 PIA-6: Cross-Agency Interoperable Authentication

Control: The E-PACS should support authentication of PIV and PIV-I cards from other issuers via:

1. PKI, or
2. Asymmetric CAK

The E-PACS may support the authentication of PIV and PIV-I cards from other issuers via:

1. Symmetric CAK
2. CHUID + BIO
3. CAK + BIO
4. PKI + BIO

5. PIN to PACS[33]
6. BIO to PACS

The relative assurance levels of these mechanisms are specified in Table 8-3.

Detailed Guidance: The E-PACS should support Asymmetric Card Authentication Key to maximize interoperability with PIV-I cards.

8.1.1.13 PIA-7: Card Revocation Check Mechanisms

Control: The E-PACS should support verifying that the PIV card has not been revoked using the PIV Authentication Key's digital certificate or the Card Authentication Key's digital certificate.

Detailed Guidance: OCSP, SCVP, and CRL checks are all mechanisms to verify that a digital certificate used for cryptographic authentication has not been revoked. FIPS 201 requires that all PIV Card issuers support OCSP, so that is the default interoperable standard.

An organization may have an Enterprise IdM in place. In this environment, it is possible to have direct provisioning and de-provisioning of access records that are tightly bound to Human Resources processes. This provides a faster (and potentially more secure) way of managing revocation, as the organization does not have to wait on PKI to propagate CRL status information that may be over 18 hours stale. This method must be in addition to PKI status checking.

8.1.1.14 PIA-8: Provisioning via Import

Control: The E-PACS should support batch import of identity records from a trusted source.

Detailed Guidance: The E-PACS should accept import of records from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-9.

8.1.1.15 PIA-9: Provisioning via Registration

Control: The E-PACS should support registration of a PIV or PIV-I Card from an internal or external source.

Detailed Guidance: In-person registration should include a biometric verification of the cardholder. The Facility Access Control Policy may require gathering attributes beyond those available from the card (e.g. JPAS clearance information). It is recommended that the PACS always record the following from a PIV or PIV-I Card:

1. CHUID;
2. PIV Authentication Certificate; and
3. Card Authentication Certificate (if available).

Provisioning via Registration should satisfy controls PIA-3.1, PIA 3.2, PIA 3.3, PIA 3.4, PIA 3.5, and PIA-3.6 specifically for the PIV Authentication Key and for the biometric object (the fingerprint template).

[33] PIN values are not automatically interoperable.

Special Case: The E-PACS should support off-site, remote visitor request workflow process. This function should provide a web-based workflow tool to enable visitors to remotely submit the following information to the security office:

1. CHUID;
2. PIV Authentication Certificate;
3. Card Authentication Key Certificate;
4. Sponsor information; and
5. Date and time of visit.

An effective visitor request workflow should, prior to provisioning the PIV Card to the E-PACS, ensure that:

1. PIA-3.2 and PIA-5have been satisfied;
2. The visit request is approved by the sponsor and the security administrator; and
3. Access control privileges within the E-PACS are assigned by the security administrator.

8.1.2 Access Control

The Access Control family of security controls addresses the controls for how facility access control decisions are made, given that the card holder has successfully been identified and authenticated.

Table 8-5, Summary of Access Control Controls

Class	Family	ID	Control
T	PAC	PAC-1	Enforcement of Rules of Access
T	PAC	PAC-2	Access Control Exception Procedures
T	PAC	PAC-3	Exclusion List Check

8.1.2.1 PAC-1: Enforcement of Rules of Access

Control: The E-PACS should enforce the access rules specified in the Facility Access Control Policy.

Detailed Guidance: The Facility Access Control Policy documents the rules of access (PPL-5). This control specifies that the documented rules of access should be enforced. This policy defines the relationship between the credential, the individual it represents, and the mechanisms used to enforce associated access rights. Examples for access rules include:

1. Time and schedule;
2. Role/group access;
3. FPCON management; and
4. Escalation of authentication factors based on time/schedule.

8.1.2.2 PAC-2: Access Control Exception Procedures

Control: The E-PACS should have procedures and practices that address possible causes of access denial.

Detailed Guidance: The use of PIV technology, together with one or more authentication factors, introduces complexity which may ultimately lead to incorrect access denied decisions (false rejects). The E-PACS Facility should have mechanisms that enable legitimate cardholders to improve their performance (e.g. reduce false rejects). However, the mechanisms should not be so powerful that attackers are able to exploit them to obtain incorrect access control decisions (false accepts).

The E-PACS should have procedures and practices that manage this risk by preventing fraudulent users from gaining access (e.g. for gaining access based on visual verification after a proper access denied decision based on card revocation.) In contrast, legitimate users should be encouraged to cooperate with the system to improve the false rejection rates of any factor (e.g. biometric, contactless, length of authentication).

8.1.2.3 PAC-3: Exclusion List Check

Control: The E-PACS should support verifying that the PIV or PIV-I Card has not excluded by a PACS system administrator.

Detailed Guidance: A site or PACS system can maintain a list of cards/cardholders that should not be granted access, regardless of whether the card is still valid or has been revoked. Such a list is called an "exclusion list" and can originate from multiple sources.

8.1.3 Audit and Accountability

Table 8-6, Summary of Audit and Accountability Controls

Class	Family	ID	Control
T	PAU	PAU-1	Audit and Accountability Policy and Procedures
T	PAU	PAU-2	Audit Log Record Contents
T	PAU	PAU-3	Card Usage Logging
T	PAU	PAU-4	Card Registration Logging
T	PAU	PAU-5	System Operation Logging
T	PAU	PAU-6	System Configuration Logging
T	PAU	PAU-7	Audit Analysis Capability

8.1.3.1 PAU-1: Audit and Accountability Policy and Procedures

Control: The E-PACS should log auditable events as documented in the Facility Access Control Policy.

Detailed Guidance: PPL-8 specifies that the Facility Access Control Policy should document what should be audited. This control specifies that the E-PACS should implement the documented policy.

8.1.3.2 PAU-2: Audit Log Record Contents

Control: The E-PACS should collect and record the following information for auditable events:

1. Date and time;
2. Element on which the event occurred;
3. Triggering event;
4. Credential Identifier;
5. Action Taken; and
6. Additional Information.

Detailed Guidance: Some types of information may not apply for certain events. For instance, there may not be data in the event record for (4) Credential Identifier or (5) Action Taken for a power failure event. The recorded information:

1. *Date and time*: a system sequence may be used if a clock is not available. This is required so that the order of events within the E-PACS can be sorted or sequenced.
2. *Element on which the event occurred*: For a reader, enough information to identify the specific reader. For a controller, enough information to identify the specific controller.
3. *Triggering event*: card presented, power failure, tamper detected, reader software update, reader mode changed, etc.

4. *Credential Identifier*: One of: (1) Credential identifier, (2) Credential not recognized, or (3) Not a credential event (e.g. power failure). The credential identifier should exactly match or correlate to a credential identifier under which that Card was registered.
5. *Action Taken*: (e.g. access granted or denied, identity authenticated or denied, PDVal required)
6. *Additional Information*: (e.g. reader mode, credential type, number of retries)

8.1.3.3 PAU-3: Card Usage Logging

Control: The E-PACS should have the capability to log the following events:

1. PIA-3.2, Verification of Trusted Origin
2. PIA-3.5, Path Validation
3. PAC-1, Enforcement of Rules of Access (e.g. Authorization decisions)
4. Mappings, transforms, or translation of numbers or identifiers used by different parts of the system. (This is often called credential number processing and transmission)

Detailed Guidance: Any record generated by a credential-related event should be traceable to the credential that was registered by the system. Examples: single #, multiple indexes and #s for same credential, transformation of #, ….

Records should be sufficient to support reporting such as:

1. Card activity (e.g., 3 days of card activity);and
2. Last known location card was used.

8.1.3.4 PAU-4: Card Registration Logging

Control: The E-PACS should log collect and record events at the time the card is registered to the system

Detailed Guidance: The following events should be recorded at card registration.

1. PIA-3.2, Verification of Trusted Origin
2. PIA-3.5, Path Validation as appropriate
3. Authentication Factor(s) verified (e.g. PIV Authentication Key, PIN, and/or biometric)
4. Status of background investigation
5. Status of suitability

8.1.3.5 PAU-5: System Operation Logging

Control: The E-PACS should log security-relevant events initiated by the Head End System.

Detailed Guidance: Security-relevant events initiated by the Head End System include, but are not limited to:

1. Periodic certificate PDVal and revocation status checking as defined in PIA-3.2, Verification of Trusted Origin, PIA-5, Path Validation;
2. Any modification to the status of a credential in the PACS IDMS;
3. Push of credential status throughout the PACS;
4. Individual and group reporting of alarms (e.g., door force, door prop);
5. Badge holder tracking by group or individual;
6. What date individuals were provisioned or de-provisioned and by whom;

7. Verification of software driven configuration changes; and
8. All readers and their modes.

8.1.3.6 PAU-6: System Configuration Logging

Control: The E-PACS should log configuration changes to all system hardware, software and firmware components.

Detailed Guidance: Configuration changes to all system hardware, software, and firmware components include:

1. Verification of software driven configuration changes;
2. Any modification of the status of the PACS;
3. System time;
4. Software updates; and
5. Admin actions.

8.1.3.7 PAU-7: Audit Analysis Capability

Control: The E-PACS should provide a capability to analyze and correlate audit logs.

Detailed Guidance: Audit logs may be collected and recorded on different devices (PACS Head End, Controllers,). The E-PACS should have the ability to aggregate, sort, and correlate thee multiple logs. The goal is to be able to trace all activity of a given card in chronological order. One aspect of this is the ability to determine the most recent known location for the card.

8.1.4 System and Communications Protection

Table 8-7, Summary of System and Communications Protection Controls

Class	Family	ID	Control
T	PSC	PSC-1	Communication Between System Elements
T	PSC	PSC-2	Trust Anchor Protection

8.1.4.1 PSC-1: Communication between System Elements

Control: The E-PACS should Protect Communication between system elements and prevent introduction of untrusted elements.

Detailed Guidance: The E-PACS should protect the integrity and authenticity of all identifiers and reference authenticators in transmission. Cryptographic mechanisms are the most common way of protecting integrity and authenticity. Other methods to detect tampering include balanced impedance wiring or similar hardware mechanisms.

8.1.4.2 PSC-2: Trust Anchor Protection

Control: The E-PACS should provide a trust store for Root and Issuing Certification Authorities as authorized for the PACS per local policy.

Detailed Guidance: The E-PACS should allow for Create, Read, Update and Delete (CRUD) management of trust store. This mechanism is used to provide management of the minimum set of trust anchors necessary to operate the E-PACS. This trust store should be managed based on local security policy. It is strongly recommended the trust store not to be the standard vendor trust store, and that vendor automatic updates to this trust store be turned off.

The E-PACS should support X.500, HTTP and LDAP URIs for CRL location.

The E-PACS should support OCSP.

The E-PACS should provide the ability to specify multiple SCVP servers that are utilized in priority order.

The E-PACS should support cryptographic algorithms required by [NIST SP 800-78].

8.2 Operational Controls

Operational security controls (i.e., safeguards or countermeasures) for an E-PACS are primarily implemented and executed by people rather than the PACS.

8.2.1 Configuration Management

Table 8-8, Summary of Configuration Management Controls

Class	Family	ID	Control
O	PCM	PCM-1	Configuration Administration
O	PCM	PCM-2	Component Installation and Configuration
O	PCM	PCM-3	Configuring Reader Authentication Modes

8.2.1.1 PCM-1: Configuration Administration

Control: The E-PACS should have the ability to enforce administrative privilege for configuration management operations.

Detailed Guidance: The E-PACS should authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system.

8.2.1.2 PCM-2: Component Installation and Configuration

Control: The E-PACS should have the ability to manage the system through configuration management methods.

Detailed Guidance: Initial configuration of hardware settings (e.g., DIP switches) should be done at installation and not for management of the hardware tree.

Each PACS physical component (e.g. system and door controller, readers) should be separately defined and addressable within the server user interface.

The E-PACS should support configuration downloads to each component. The system should provide sufficient logging for verification of download's status.

8.2.1.3 PCM-3: Configuring Reader Authentication Modes

Control: The E-PACS should support bi-directional communications to all readers that support dynamically configurable authentication modes.

Detailed Guidance: All E-PACS using dynamically configurable readers should support bidirectional communications with the system.

Where multiple authentication modes are supported, the following should be met:

(1) Bidirectional communication with the reader should be supported.

(2) For multi-factor readers, applicant's system allows modification of an individual reader or group's of readers' authentication mode from the server or a client/workstation to the server.

(3a) This support is present in the following administrative scenarios: The site administrator arbitrarily decides that all readers or a subset of readers must require either more or fewer authentication factors for which than the readers are presently configured.

(3b) Based on temporal access rules the administrator set. The system should support dynamic assignment of individuals (or groups of individuals) and resources (doors) on a time based schedule.

(3c) Based on Force Protection Condition (FPCON)[34], Maritime Security (MARSEC)[35] or other similar structured emergency response protocol for which the vendor claims support. There shouldn't be a requirement for an administrator's physical presence at a reader to be considered compliant.

(3d) if a time delay of longer than 120 seconds is required for a reader to change modes; this too should be considered non-compliant.

8.2.2 Contingency Planning

Table 8-9, Summary of Contingent Planning Controls

Class	Family	ID	Control
O	PCP	PCP-1	Continuity of Operations

8.2.2.1 PCP-1: Continuity of Operations

***Control*:** The E-PACS should provide testable methodologies for backup and restoration of databases.

Detailed Guidance: Testable methodologies include, but are not limited to:

1. Onsite and remote backup support;
2. Automatic v. manual backup options;
3. Destination media supported;
4. Perform backups/restores for supported options;
5. Kill power and test resiliency;
6. Kill network; and
7. Trust store and authenticator recovery.

[34] See http://www.fas.org/irp/doddir/dod/i2000_16.pdf for FPCON details.

[35] See http://www.uscg.mil/safetylevels/whatismarsec.asp for MARSEC details.

8.2.3 Physical and Environmental Protection

Table 8-10, Summary of Physical and Environmental Controls

Class	Family	ID	Control
O	PPE	PPE-1	Secure Processing Protection

8.2.3.1 PPE-1: Secure Processing Protection

Control: The E-PACS should perform all security relevant processing on the secure side of the physical security boundary.

Detailed Guidance: No security relevant decisions should be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door. This specifically applies to the door reader. Security relevant processing includes:

1. PKI PDVal (PIA-3.2);
2. Nonce generation (PIA-3.3);
3. Challenge/response (PIA-3.3);
4. Biometric matching for 1:1 verification (PIA-3.3);
5. Certificate revocation and status checking (PIA-3.5);
6. Credential identifier processing; and
7. Authorization decisions.

Certain compensating controls may be applied such as tamper switches and [FIPS 140-2]-certified cryptographic processing within the reader itself.

8.2.4 System and Information Integrity

No additional controls in this system family are identified for PACS at this time. However, the controls in [NIST SP 800-53] do apply to PACS. In addition, IP-based systems may have additional concerns such as geo-location, authentication and integrity of devices.

8.2.5 Awareness & Training

Table 8-11, Summary of Awareness and Training Controls

Class	Family	ID	Control
O	PAT	PAT-1	Security Awareness and Training Policy and Procedures
O	PAT	PAT-2	Security Training Records
O	PAT	PAT-3	Contacts with Security Groups and Associations

Training for users and guards on using biometrics in the system or card tearing may need to be described.

8.2.5.1 PAT-1: Security Awareness and Training Policy and Procedures

Control: An organization should establish, conduct, and comply with PACS-related training policies and procedures.

Detailed Guidance: There is no detailed guidance at this time.

8.2.5.2 PAT-2: Security Training Records

Control: An organization should maintain training records.

Detailed Guidance: There is no detailed guidance at this time.

8.2.5.3 PAT-3: Contacts with Security Groups and Associations

Control: An organization should establish and maintain contacts with Security Groups and Associations.

Detailed Guidance: There is no detailed guidance at this time.

8.3 Management Controls

Management security controls (i.e., safeguards or countermeasures) for an E-PACS focus on the management of risk and the management of information system security. These controls require ongoing management over time.

8.3.1 Security Assessment and Authorization

Table 8-12, Summary of Security Assessment and Authorization Controls

Class	Family	ID	Control
M	PCA	PCA-1	Fire, Life and Safety Certifications
M	PCA	PCA-2	UL 294 Assessment
M	PCA	PCA-3	FIPS 201 APL
M	PCA	PCA-4	FIPS 140 Validation
M	PCA	PCA-5	Facility Assessment
M	PCA	PCA-6	Security Authorization

8.3.1.1 PCA-1: Fire, Life and Safety Certifications

Control: The E-PACS should obtain appropriate certifications required to comply with federal and local fire, life and safety requirements.

Detailed Guidance: System owner should determine appropriate life safety requirements for their facility and obtain all applicable certifications. Building codes from the National Fire Prevention Association (NFPA) such as NFPA 72 and NFPA 101 Life Safety Code should be consulted during the planning stages of an access control project. These codes require that an access control system be connected to the Fire Alarm Control Panel. In addition, for government owned and leased facilities which are under GSA, the GSA fire and safety office of the particular region the facility should also be consulted as well as the Federal Protective Service (FPS) since fire alarm monitoring is usually done by the FPS Mega Centers.

8.3.1.2 PCA-2: UL 294 Assessment

Control: The E-PACS should obtain external certification such as those provided by Underwriters Laboratory Inc., standard UL-294.

Detailed Guidance: The E-PACS should have the following core certifications as appropriate to components within the system. These certifications should be achieved prior to listing on the APL. (1) UL assessment (UL 294 at a minimum).

8.3.1.3 PCA-3: FIPS 201 APL

Control: The E-PACS should incorporate components listed on the GSA FIPS 201 APL at all points in the system where products from an APL category are appropriate.

Detailed Guidance: It is important to note products FIPS 140 Validation status when choosing products from the APL (see PCA-4, PIA-3.4). When implementing system components, an E-PACS should only implement tested version numbers. When the APL updates approved versions, the E-PACS should be updated as well to support the latest tested bug fixes.

Special Case: if a serious security exploit has been identified that requires an update to E-PACS systems, it may be necessary to update system components beyond the latest approved version listed on the APL.

8.3.1.4 PCA-4: FIPS 140 Validation

Control: The E-PACS should incorporate FIPS 140 Validated components at all points in the system where cryptographic processing occurs.

Detailed Guidance: See [FIPS 140] for detailed guidance.

8.3.1.5 PCA-5: Facility Assessment

Control: The E-PACS should be subject to a facility assessment to ensure the configuration, architecture, and validation components follow E-PACS guidance. In general facility assessments should be treated like a pre-operational audit and done by a third party to the facility owner and integrator.

Detailed Guidance: An E-PACS facility assessments should cover:

Facility Architecture

1. Ensure proper authentication is used based on a facilities security level
2. System complies with mandatory requirements and guidance
3. Supports current APL products

System Configuration

1. Fitness for use
2. Proper controls and policies are in place to detect errors, monitor access and prevent intrusion
3. Products and specific version

Validation Components

1. Proper PKI configuration settings
2. Cached responses are being refreshed periodically

8.3.1.6 PCA-6: Security Authorization

Control: The E-PACS should obtain a security authorization.

Detailed Guidance: The E-PACS should meet security authorization requirements of Federal Information Security Management Act (FISMA) and [NIST SP 800-37] as applicable.

8.3.2 Planning

Table 8-13, Summary of Planning Controls

Class	Family	ID	Control
M	PPL	PPL-1	Facility Access Control Policy
M	PPL	PPL-2	Policy Specifies Assurance Level
M	PPL	PPL-3	Policy Specifies Authentication Modes
M	PPL	PPL-4	Policy Specifies Accessing Populations
M	PPL	PPL-5	Policy Specifies Rules of Access
M	PPL	PPL-6	Policy Specifies Time of Day Restrictions for Access
M	PPL	PPL-7	Policy Specifies Threat Level Restrictions and Exceptions
M	PPL	PPL-8	Policy Specifies Auditable Events

8.3.2.1 PPL-1: Facility Access Control Policy

Control: The E-PACS should have a documented Facility Access Control Policy.

Detailed Guidance: It is difficult to measure the effectiveness of an E-PACS if the policy fit is expected to enforce is not clearly documented. This and the following controls explicitly specify what the policy should document.

8.3.2.2 PPL-2: Policy Specifies Assurance Level

Control: The E-PACS Facility Access Control Policy should specify the PACS Assurance Level required for protecting this facility

Detailed Guidance: Facilities have varying requirements for facility protection, and therefore for the assurance of the implemented security controls. The required PACS Assurance Level should be specified as one of:

1. LITTLE OR NO confidence
2. SOME confidence
3. HIGH confidence
4. VERY HIGH confidence

8.3.2.3 PPL-3: Policy Specifies Authentication Modes

Control: The E-PACS Facility Access Control Policy should specify what Authentications Modes are required and permitted for each different security area (re: [NIST SP 800-116], unrestricted, controlled, limited, exclusion).

Detailed Guidance: See [NIST SP 800-116] for detailed guidance.

8.3.2.4 PPL-4: Policy Specifies Accessing Populations

Control: The E-PACS Facility Access Control Policy should specify the various populations of individuals for whom access to the facility is controlled.

Detailed Guidance: The policy should define the populations that are relevant for its operation. These populations will often be drawn from the following list: Employee, Contractor, Temp Worker, Visitor, Security Guard, Local Security Administrator, System Administrator, and Security Administrator.

For example, the E-PACS may include three specific populations: regular, visitor, and guest:

- **Regular**: individuals with a card that may be issued by the local authority or another source that is trusted by the E-PACS, and who regularly access the facility.
- **Visitor**: an external user[36] that is requesting short term access to an agency facility.
- **Guest**: individuals who do not bring a card from a source that is trusted by the E-PACS.

8.3.2.5 PPL-5: Policy Specifies Rules of Access

Control: The E-PACS Facility Access Control Policy should specify the rules of access for each population of individuals for whom access to the facility is controlled.

Detailed Guidance: There is no detailed guidance at this time.

8.3.2.6 PPL-6: Policy Specifies Time of Day Restrictions for Access

Control: The E-PACS Facility Access Control Policy should specify time of day restrictions for access.

Detailed Guidance: There is no detailed guidance at this time.

8.3.2.7 PPL-7: Policy Specifies Threat Level Restrictions and Exceptions

Control: The E-PACS Facility Access Control Policy should specify restrictions and exceptions for access that are based on the threat level.

Detailed Guidance: There is no detailed guidance at this time.

8.3.2.8 PPL-8: Policy Specifies Auditable Events

Control: The E-PACS Facility Access Control Policy should specify the events that should be recorded in the audit log.

Detailed Guidance: There is no detailed guidance at this time.

[36] An external user is any individual attempting or requesting access to agency facilities or systems that is not an employee, contractor, or primary affiliate of the agency. External users may be PIV holders from another agency, business partners, or private citizens.

8.3.3 Risk Assessment

Table 8-14, Summary of Risk Assessment Controls

Class	Family	ID	Control
M	PRA	PRA-1	Assess risk in accordance with ISC Guidance on PACS
M	PRA	PRA-2	Use a risk-based methodology to Determine security area designation for physical spaces in each facility.

As indicated in [HSPD-12], agencies were to begin using the common identification standard in November 2006 to gain physical access to federally-controlled facilities and logical access to federally-controlled information systems. [OMB M-11-11] states that DHS and GSA will work together to provide agencies with guidance for implementing the government-wide architecture defined in [FICAM Roadmap]. This includes a DHS partnership with the GSA Public Building Service (PBS) to ensure that implementation of physical access requirements for federal buildings, under PBS' purview, are implemented in accordance with [Facility Security Levels] and NIST guidelines.

Table 8-15, Matrix of mappings

Authentication Factors	NIST SP 800-116	Example Areas
0	Unrestricted	Badging Lobby, Visitors Center, Roadways, Cafeterias, Gift Shop, Recreation Facilities, Employee General Access to Buildings.
1	Controlled	Building, Program or Code Has Requested Accountability Controls, Access to Program Area Not Storing CNSI, No MEI Facility, LAN Closet, Electrical Closet, Hazmat Supplies, Admin Building, Facility Services, HQ.
2	Limited	Special Program Area Storing CNSI, MEI Facility, Other Very Sensitive Documents or Equipment, SEB, Mishap Investigation Facility, Lab Space.
3	Exclusion	Most-sensitive areas such as those containing trade secrets.

9. PACS Components

Table 9-1summarizes the basic, core components of current PACS implementations. The terms listed below are used throughout the remainder of this document for consistency.

Table 9-1, Core PACS Components

Component Name	Description
Contact Reader:	A smart card reader that communicates with the Integrated Circuit chip in a smart card using electrical signals on wires touching the smart card's contact pad. The PIV contact interface is standardized by International Organization of Standards / International Electrotechnical Commission (ISO/IEC) 7816-3. [ISO/IEC 7816]. The reader may also include a keypad for PIN entry and/or a biometric sensor as integral components.
Contactless Reader:	A smart card reader that communicates with the Integrated Circuit chip in a smart card using radio frequency (RF) signaling. The PIV contactless interface is standardized by ISO/IEC 14443 [ISO/IEC 14443]. Use of 125khz card is not part of the PIV standard[37]. The reader may also include a keypad for PIN entry and/or a biometric sensor as integral components.
Door Reader Interface	This functional interface, which can be in the Door Reader or the Controller, comes in different configurations. FIPS 201 does not specify which protocols can be used for this interface, provided the necessary data can be communicated to the Controller. Typical deployed implementations support transmitting a small amount of data (on the order of 10 to 15 bytes), but FIPS 201 defines data elements which are much larger. Therefore, depending on the agency's implementation strategy, an upgrade to the Door Reader to Controller interface may also be required. At a minimum, a 14 decimal digit FASC-N Identifier will be supported in most cases. Note that any change to this interface may also necessitate changes to the physical wiring and cabling infrastructures.
Controller (Sometimes referred to as **Control Panel,** or **Panel**):	A device located within the secure area that, among other functions, communicates with multiple PIV Card readers and door actuators, and with the Head End System. The PIV Card readers provide cardholder information to the Controller, which it uses to make access control decisions and release door locking mechanisms. The Controller communicates with the Head End System to receive changes in access permissions, report unauthorized access attempts and send audit records and other log information. Most modern controllers can continue to operate properly during periods of time in which communication with the Head End is disrupted and can journal transactions so that they can be reported to the Head End when communication is restored.
Head End System (Sometimes referred to as **Access Control Server**):	A system including application software, database, a Head End server, and one or more networked personal computers. The Head End server is typically used to enroll an individual's name, create a unique ID number, and assign access privileges and an expiration date. The server is also used to maintain this information and refresh the Controller(s) with the latest changes. In addition to taking care of PIV card registrations, the server may also support alarm monitoring, operator control, system configuration, transaction logging, report generation, graphic assessment, and back up of the controller database. Caching status proxy may also reside in the head end.
Door	A door is a managed breach in a secure perimeter that is controlled by the PACS. For the purposes of this document, it has an Attack Side and a Secure Side.

[37] See [OMB M-10-15].

Component Name	Description
Servers/External Interfaces	Because PACS are now using credentials issued by external providers, they have to interface with external systems such as: a. PIV issuance provider; b. Interfaces to the equivalent of a no-fly-list; c. PKI services; and d. Other Head Ends.
Infrastructure	Distributed substructure of a large-scale organization that facilitates related functions or operations, e.g., telecommunications infrastructure. With regard to PACS, components include conduit, cabling, power supplies, battery backup, electrified door hardware, door position switches, and remote exit devices, as well as connectivity with other life safety systems that will ensure egress in the event of an emergency.
Certificate Path Validation	Performs certificate path validation Functionality. This validates that the trust chain for the credential is not revoked, expired, or otherwise compromised. See PIA-5

10. AUTHENTICATION PATTERNS

The following subsections highlight common authentication patterns (also called use cases), and provide insights and considerations. The patterns are aligned with [NIST SP 800-116] authentication mechanisms as they pertain to gaining access to security areas (see Figure 7-1). Table 10-1, summarizes what authentication patterns in the subsections that follow are sufficient to move through the various security areas[38]. Each pattern lists unmitigated threats specific to it. Note that there are some threats that apply to all patterns.

Table 10-1, Summary of Patterns to Moving Between NIST SP 800-116 Security Areas

			Contact Interface	Contactless Interface	Authentication factor(s)	1. Electronic Cloning	2. Electronic Counterfeiting	3. Visual Counterfeiting	4. Use of Expired Card	5. Use of Terminated Card	6. Use of Lost or Stolen Card	7. Skimming	8. Sniffing	9. Social Engineering	10. Biometric Object Substitution	11. Identifier Collision	12. Biometric Spoofing		
#		**Pattern Name**	**Interface**		**Authenticators**	**Vulnerabilities**												**Considered PIV-enabled?**	**Example NIST SP 800-116 Area Movement**
Patterns with No Factors						**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**		
1		VIS						✓		✓	✓							No	None
2		Partial CHUID	C	CL		✓	✓		✓	✓	✓					✓		No	None
3		Primitive CHUID	C	CL		✓	✓			✓	✓	✓	✓					No	None
4		CHUID	C	CL		✓				✓	✓	✓	✓					No	None
5		Enhanced CHUID	C	CL		✓					✓	✓	✓					No	None
6		Primitive BIO	C				✓			✓	✓				✓		✓	No	None
Patterns with One Factor																			
7		Enhanced CHUID + VIS	C	CL	Have	✓					✓	✓	✓					Yes	Unrestricted to Controlled
8		Asymmetric CAK	C	CL	Have						✓			✓				Yes	Unrestricted to Controlled
9		Symmetric CAK	C	CL	Have						✓			✓				Yes	Unrestricted to Controlled
10		BIO	C		Are												✓	Yes	Unrestricted to Controlled
11		PIN to PACS	C	CL	Know									✓				No	Unrestricted to Controlled
12		BIO to PACS	C	CL	Are												✓	No	Unrestricted to Controlled
13		BIO-A to PACS	C	CL	Are													No	Unrestricted to Controlled
Patterns with Two Factors																			
14		BIO-A	C		Have + Are													Yes	Unrestricted to Limited
15		PKI-Auth	C		Have + Know									✓				Yes	Unrestricted to Limited
16		Asymmetric CAK + PIN to PACS	C	CL	Have + Know									✓				Yes	Unrestricted to Limited
17		Symmetric CAK + PIN to PACS	C	CL	Have + Know									✓				Yes	Unrestricted to Limited
Patterns with Three Factors																			
18		Asymmetric CAK + BIO-A	C		Have + Know + Are													Yes	Unrestricted to Exclusion
19		Symmetric CAK + BIO-A	C		Have + Know + Are													Yes	Unrestricted to Exclusion
20		PKI-Auth + BIO-A	C		Have + Know + Are													Yes	Unrestricted to Exclusion

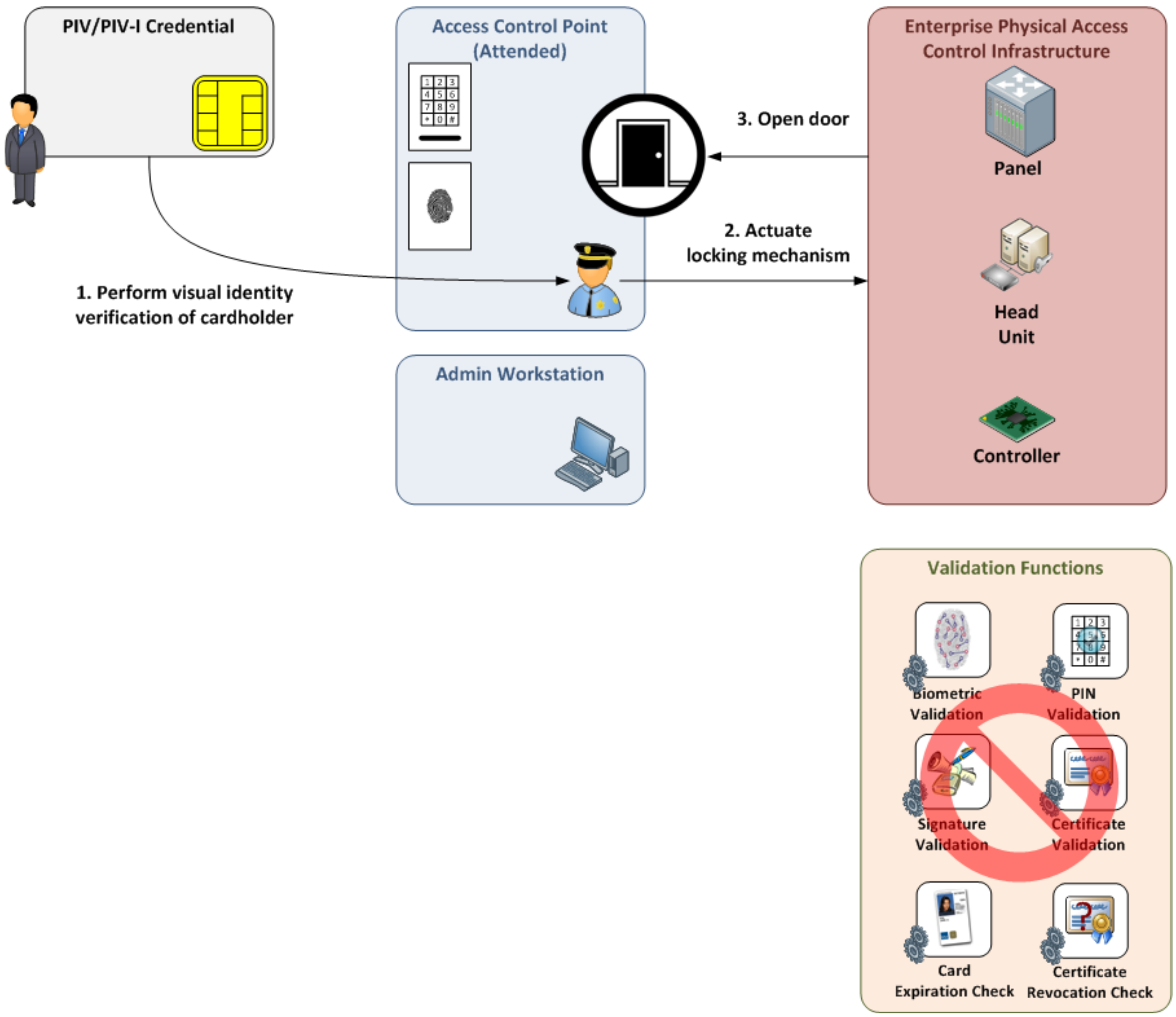
[38] This table shows an example area movement per authentication pattern. For a complete listing and discussion of all area movement permutations, see [NIST SP 800-116] Table 7-2.

10.1 Pattern #1: VIS

A PIV or PIV-I Card is used solely as a flash pass for guard inspection. None of the on-card authentication mechanisms (e.g., CHUID, PKI-Auth) are utilized, and no PACS validation functions are performed. The guard authenticates the cardholder by means such as comparing the picture on the card to the face of the cardholder, and/or determining that the card is genuine. Upon satisfactory verification, the guard initiates unlocking/opening of the door (e.g., presses a button), or allows the cardholder to pass.

0 Factor

10.1.1 Use Case Diagram



10.1.2 Description

This pattern does not use the contact or contactless interface. The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication as follows:

1. Photograph;
2. Name;
3. Employee affiliation employment identifier;
4. Expiration date;
5. Agency card serial number (back of card); and
6. Issuer identification (back of card).

The PIV Card may also bear the following optional components:

1. Agency name and/or department;
2. Department or agency seal;
3. PIV Cardholder's physical characteristics; or
4. Applicant's signature.

When a cardholder attempts to pass through an access control point for a federally-controlled facility, a human guard performs visual identity verification of the cardholder to determine whether the identified individual should be allowed to through the control point. The series of steps that is applied in the visual authentication process are as follows:

1. The human guard at the access control entry point determines whether the PIV or PIV-I Card appears to be genuine and has not been altered in any way.

    a. The guard compares the cardholder's facial features with the picture on the card to ensure that they match. It is strongly recommended that the guard physically hold the card during inspection.

    b. The guard checks the expiration date on the card to ensure that the card has not expired.

    c. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)

    d. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)

    e. 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.

2. The human guard opens the door, which may or may not involve the PACS.

3. Door is unlocked, and cardholder can enter.

Some of the characteristics of the visual authentication mechanism are as follows:

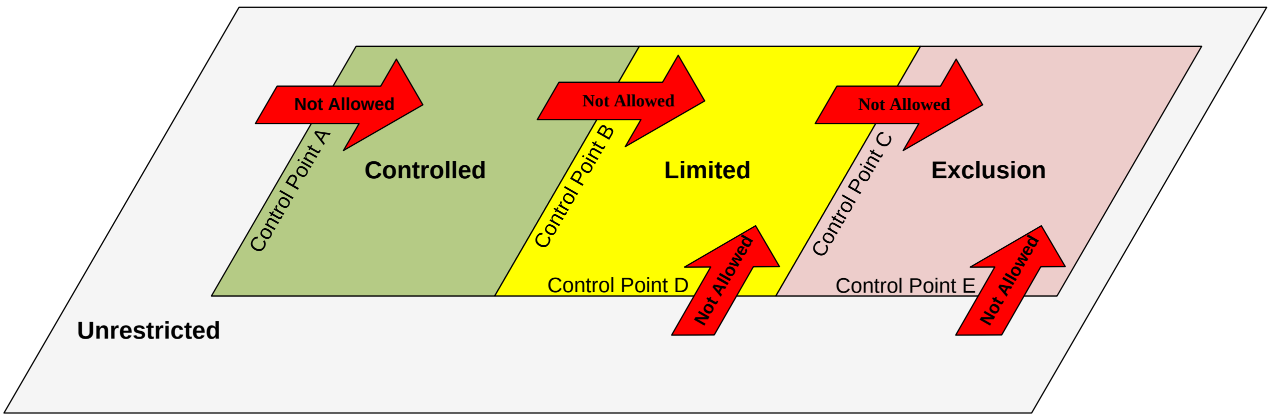
1. Human inspection of the card, which is not amenable for rapid or high volume access control.
2. Resistant to use of unaltered card by non-owner of card.
3. Low resistance to visual counterfeiting and forgery.
4. Applicable in environments with and without card readers.

10.1.3 Unmitigated Threats

Unmitigated PACS Threats
Use of Terminated Card
Use of Unreported Lost or Stolen Card
Visual Counterfeiting

10.1.4 Pros, Cons, Issues

This pattern is zero-factor authentication. Therefore, this pattern is not sufficient for any use. At a minimum, VIS must be combined with Enhanced CHUID authentication (see Pattern #7, Enhanced CHUID +VIS) to move from the Unrestricted area to the Controlled area .

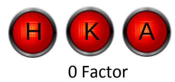


10.1.5 Considerations

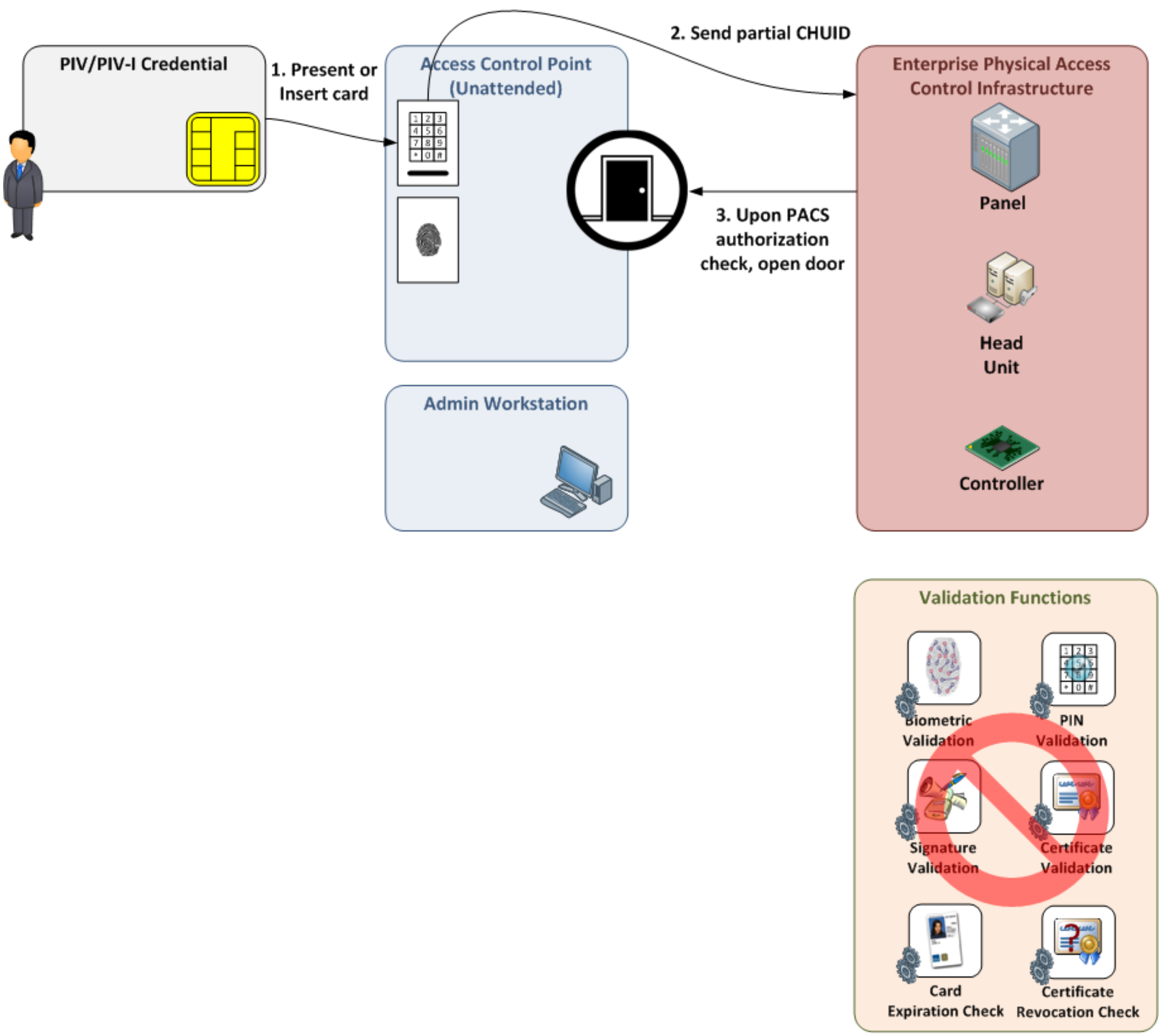
VIS should only be combined with electronic authentication mechanisms such as CHUID, BIO, CAK, or PKI.

10.2 Pattern #2: Partial CHUID

The PACS that is not capable of transmitting the full CHUID from the reader to the panel. Therefore, the CHUID is truncated before it is sent to the panel. For example, the weigand line is limited to 48 bits so it will not take a full CHUID because there isn't enough room to transmit certain information/fields. In addition, the PACS does not perform validation functions. The PACS does not validate the signature on the CHUID, does not validate the CHUID signing certificate (which should use PDVal), does not check the revocation status of the associated Authentication certificate, and does not check the card's expiration date (because the date may not have been included in the Partial CHUID).



10.2.1 Use Case Diagram



10.2.2 Description

This pattern can use the contact or contactless interface. In this use case, only a subset of the CHUID is used.

The CHUID is used for PIV or PIV-I Cardholder authentication using the following sequence:

1. Present or insert PIV or PIV-I Card to the card reader.
    a. The CHUID is read electronically from the PIV or PIV-I Card.
2. The Partial CHUID is sent to the E-PACS Infrastructure.
3. The PACS checks whether the card identifier is authorized to enter.
    a. Partial CHUID string is used to input to the authorization check to determine whether the cardholder should be granted access.
    b. Upon authorization, the door is unlocked.

Some of the characteristics of the Partial CHUID-based authentication mechanism are as follows:

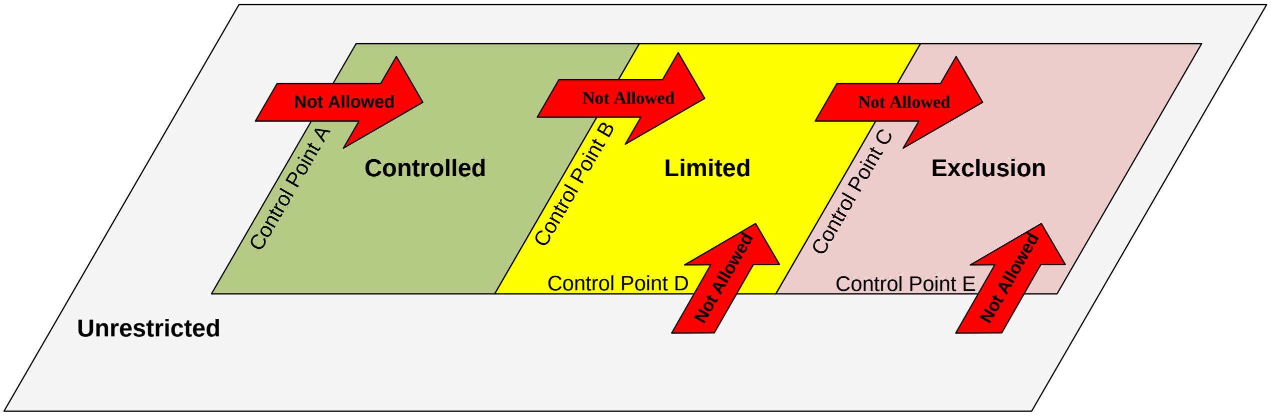
1. Can be used for rapid authentication for high volume access control.
2. It is possible for more than one user to have the same partial CHUID string and gain access to unauthorized buildings and areas.
3. Low resistance to use of unaltered card by non-owner of card.
4. Applicable with contact-based and contactless readers.

10.2.3 Unmitigated Threats

Unmitigated PACS Threats
Electronic Cloning
Electronic Counterfeiting
Use of Expired Card
Use of Terminated Card
Use of Unreported Lost or Stolen Card
Identifier Collision

10.2.4 Pros, Cons, Issues

This pattern is zero-factor authentication and not recommended for use. Therefore, this pattern is not sufficient for any use. At a minimum, Enhanced CHUID must be combined with VIS (see Pattern #7, Enhanced CHUID +VIS) to move from the Unrestricted area to the Controlled area.

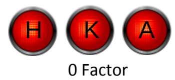


10.2.5 Considerations

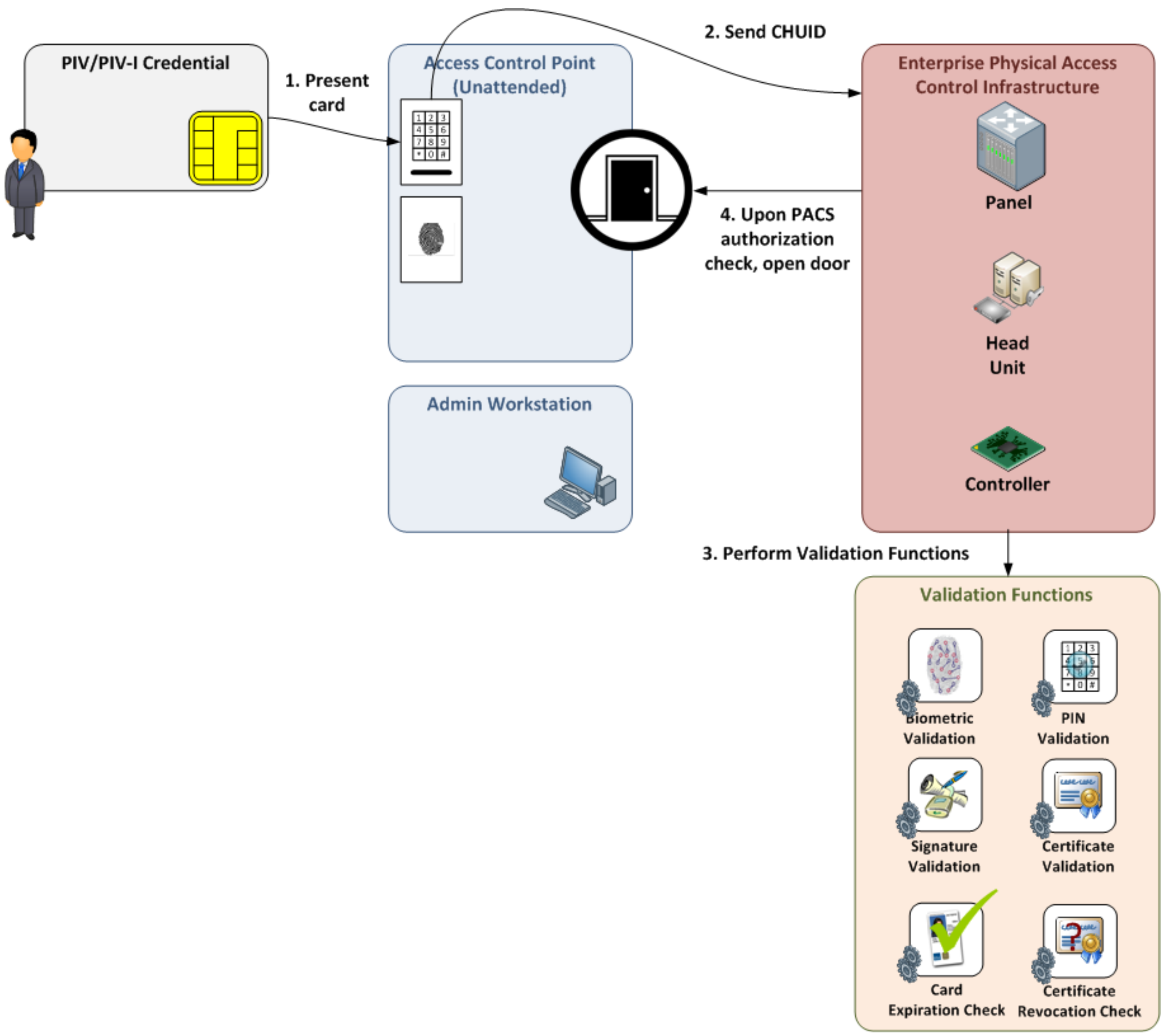
See Pattern #7, Enhanced CHUID +VIS, for use of the CHUID authentication mechanism.

10.3 Pattern #3: Primitive CHUID

The PACS uses a CHUID without validating the signature on the CHUID, without validating the CHUID signing certificate (which should use PDVal), and without checking the revocation status of the associated Authentication certificate. The PACS does check the card's expiration date.



10.3.1 Use Case Diagram



10.3.2 Description

This pattern uses just the contactless interface.

The CHUID is used for PIV or PIV-I Cardholder authentication using the following sequence:

1. Present the PIV or PIV-I Card to the card reader.
    a. The CHUID is read electronically from the PIV or PIV-I Card.
2. The CHUID is sent to the E-PACS Infrastructure.
3. The PACS performs validation functions.
    a. The CHUID expiration date is checked to ensure that the card has not expired (see PIA-3.6).
4. The PACS checks whether the card identifier is authorized to enter.
    a. One or more of the CHUID data elements (e.g. FASC-N, GUID) are used to input to the authorization check to determine whether the cardholder should be granted access.
    b. Upon authorization, the door is unlocked.

Some of the characteristics of the CHUID-based authentication mechanism are as follows:

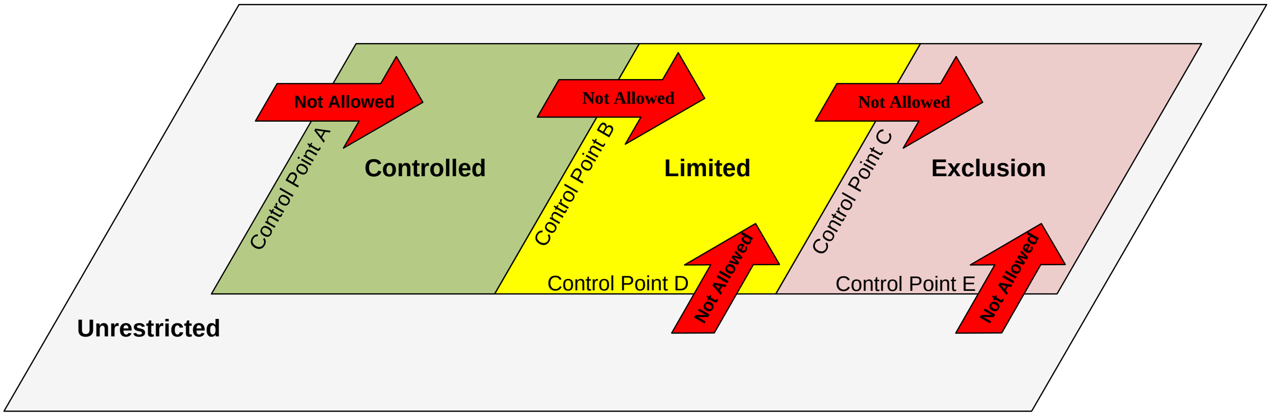
1. Can be used for rapid authentication for high volume access control.
2. Low resistance to use of unaltered card by non-owner of card.
3. Applicable with contact-based and contactless readers.

10.3.3 Unmitigated Threats

Unmitigated PACS Threats
Electronic Cloning
Electronic Counterfeiting
Skimming
Sniffing
Use of Terminated Card
Use of Unreported Lost or Stolen Card

10.3.4 Pros, Cons, Issues

This pattern is zero-factor authentication. Therefore, this pattern is not sufficient for any use. At a minimum, Enhanced CHUID must be combined with VIS (see Pattern #7, Enhanced CHUID +VIS) to move from the Unrestricted area to the Controlled area.

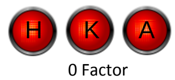


10.3.5 Considerations

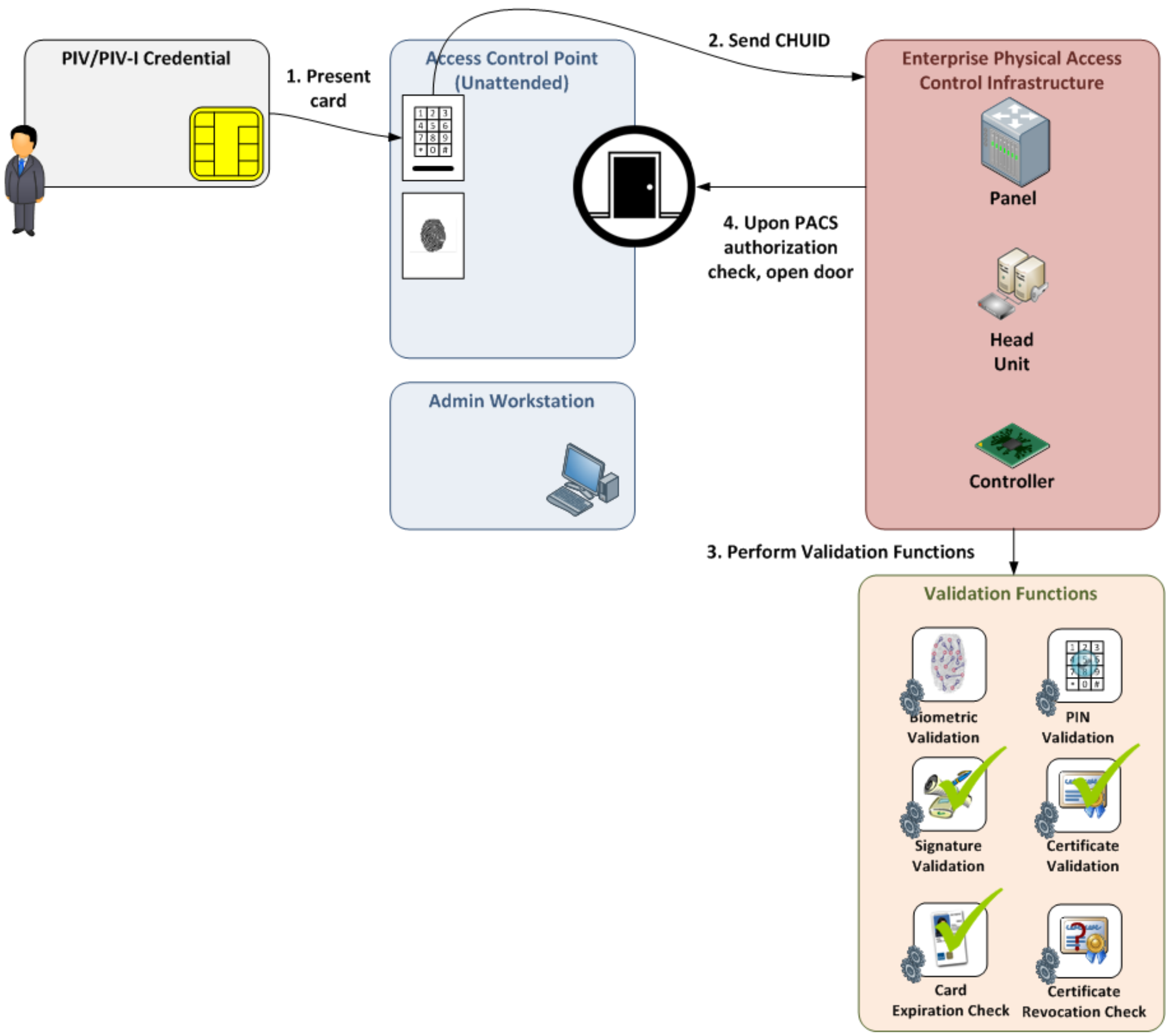
See Pattern #7, Enhanced CHUID +VIS, for use of the CHUID authentication mechanism.

10.4 Pattern #4: CHUID

The PACS uses a CHUID without checking the revocation status of the associated Authentication certificate. The PACS does validate the signature on the CHUID, does validate the CHUID signing certificate (which should use PDVal), and does check the card's expiration date.



10.4.1 Use Case Diagram



10.4.2 Description

This pattern uses just the contactless interface.

The CHUID is used for PIV or PIV-I Cardholder authentication using the following sequence:

1. Present the PIV or PIV-I Card to the card reader.
    a. The CHUID is read electronically from the PIV or PIV-I Card.
2. The CHUID is sent to the E-PACS Infrastructure.
3. The PACS performs validation functions.
    a. Validate the CHUID (see PIA-4).
        i. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered (see PCA-4).
        ii. Validate the certificate used to sign the CHUID. That is, use PDVal to ensure trusted issuer and certificate is not revoked (see PIA-5).
    b. The CHUID expiration date is checked to ensure that the card has not expired (see PIA-3.6).
4. The PACS checks whether the card identifier is authorized to enter.
    a. One or more of the CHUID data elements (e.g. FASC-N, GUID) are used to input to the authorization check to determine whether the cardholder should be granted access.
    b. Upon authorization, the door is unlocked.

Some of the characteristics of the CHUID-based authentication mechanism are as follows:

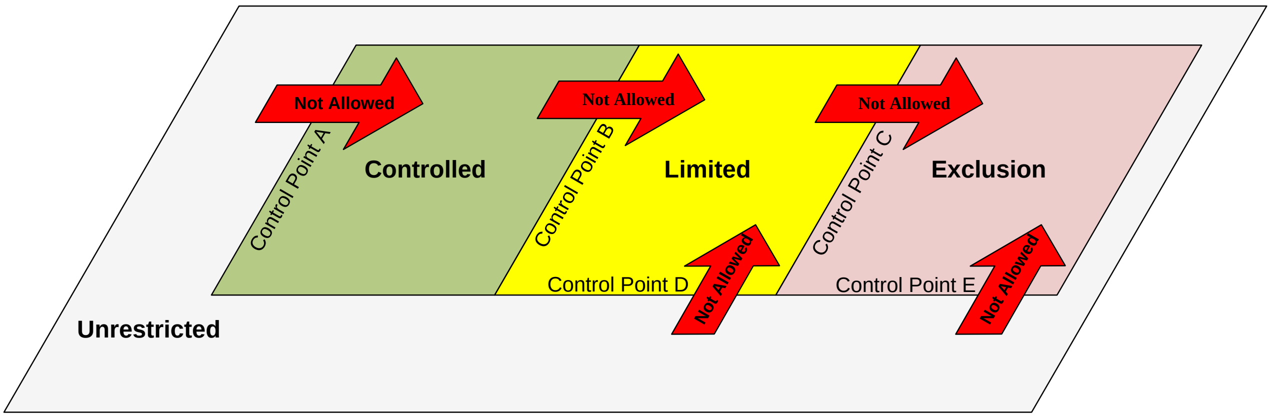
1. Can be used for rapid authentication for high volume access control.
2. Low resistance to use of unaltered card by non-owner of card.
3. Applicable with contact-based and contactless readers.

10.4.3 Unmitigated Threats

Unmitigated PACS Threats
Electronic Cloning
Skimming
Sniffing
Use of Unreported Lost or Stolen Card
Use of Terminated Card

10.4.4 Pros, Cons, Issues

This pattern is zero-factor authentication. Therefore, this pattern is not sufficient any use. At a minimum, Enhanced CHUID must be combined with VIS (see Pattern #7, Enhanced CHUID +VIS) to move from the Unrestricted area to the Controlled area.

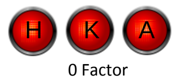


10.4.5 Considerations

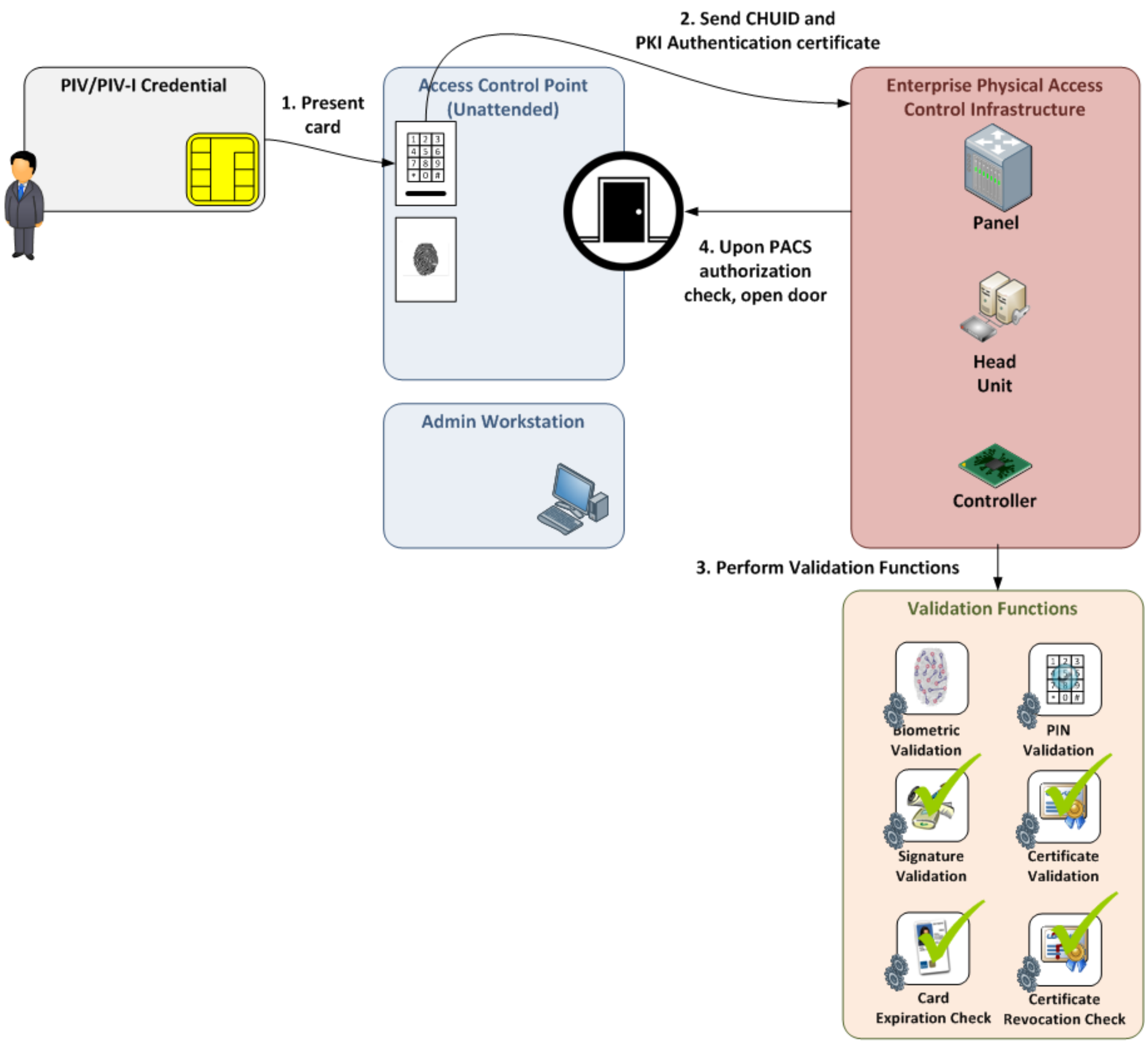
See Pattern #7, Enhanced CHUID +VIS, for use of the CHUID authentication mechanism.

10.5 Pattern #5: Enhanced CHUID

The PACS uses a CHUID and performs all validation functions. The PACS validates the signature on the CHUID, validates the CHUID signing certificate (which should use PDVal), checks the revocation status of the associated Authentication certificate, and checks the card's expiration date.



10.5.1 Use Case Diagram



10.5.2 Description

This pattern uses just the contactless interface.

The CHUID is used for PIV or PIV-I Cardholder authentication using the following sequence:

1. Present the PIV or PIV-I Card to the card reader.
    a. The CHUID and PKI Authentication certificate are read electronically from the PIV or PIV-I Card.
2. The CHUID and PKI Authentication certificate are sent to the E-PACS Infrastructure.
3. The PACS performs validation functions.
    a. Validate the CHUID (see PIA-4).
        i. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered (see PCA-4).
        ii. Validate the certificate used to sign the CHUID. That is, use PDVal to ensure trusted issuer and certificate is not revoked (see PIA-5).
    b. Perform PDVal and revocation check of associated PKI Authentication certificate. PDVal of the Authentication certificate should be done to perform revocation check, and FASC-N in CHUID and Authentication certificate should be compared and matched[39] (see PIA-5).
    c. The CHUID date is checked to ensure that the card has not expired (see PIA-3.6).
4. The PACS checks whether the card identifier is authorized to enter.
    a. One or more of the CHUID data elements (e.g. FASC-N, GUID) are used to input to the authorization check to determine whether the cardholder should be granted access.
    b. Upon authorization, the door is unlocked.

Some of the characteristics of the CHUID-based authentication mechanism are as follows:

1. Can be used for rapid authentication for high volume access control.
2. Low resistance to use of unaltered card by non-owner of card.
3. Applicable with contact-based and contactless readers.

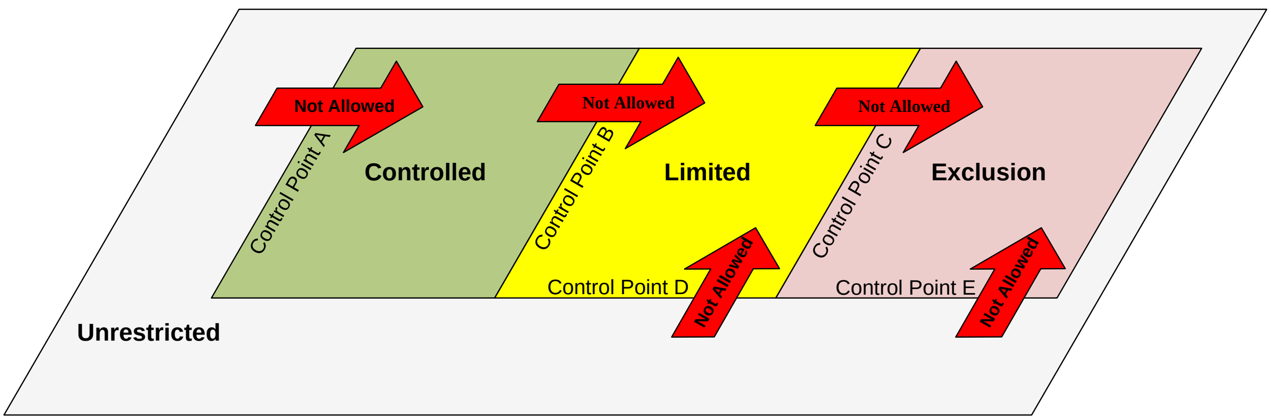
[39] Certificate being read from card can be done in advance (i.e., not at time of authentication).

10.5.3 Unmitigated Threats

Unmitigated PACS Threats
Electronic Cloning
Skimming
Sniffing
Use of Unreported Lost or Stolen Card (until card is revoked)

10.5.4 Pros, Cons, Issues

This pattern is zero-factor authentication. Therefore, this pattern is not sufficient for moving from the Unrestricted area into the Controlled area. At a minimum, Enhanced CHUID must be combined with VIS (see Pattern #7, Enhanced CHUID +VIS) to move from the Unrestricted area to the Controlled area.



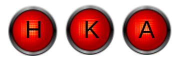
10.5.5 Considerations

With respect to CHUID, the only acceptable one-factor authentication is CHUID + VIS.

PDVal and revocation checking should occur before card use, and periodically thereafter.

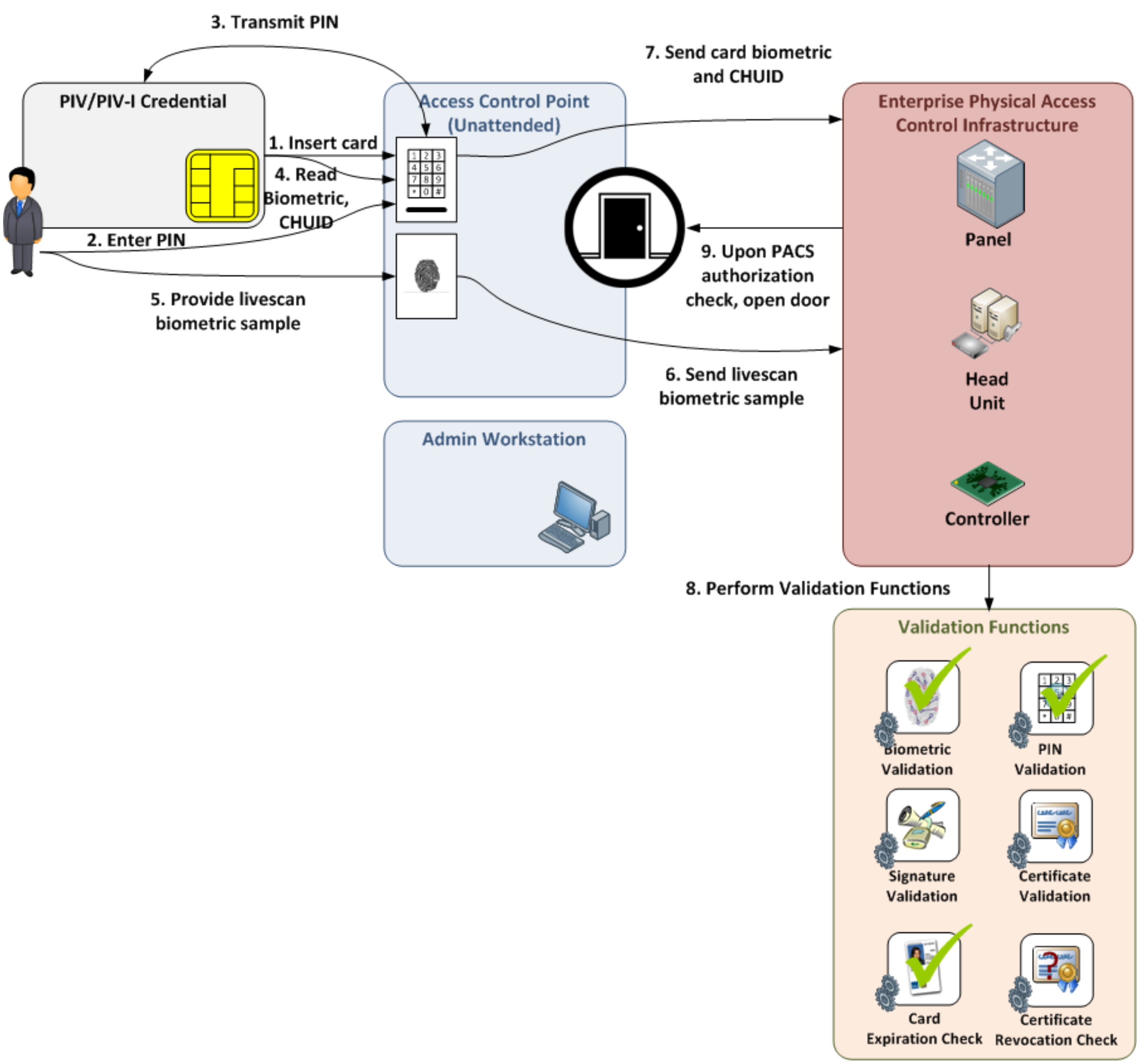
10.6 Pattern #6: Primitive BIO

The PACS uses a biometric without validating the signature on the biometric object, without validating the content signer certificate (which should use PDVal), and without checking the revocation status of the associated Authentication certificate. The PACS does check the card's expiration date. The PACS does validate the livescan biometric against the biometric retrieved from the card.



0 Factor

10.6.1 Use Case Diagram



10.6.2 Description

This pattern uses just the contact interface.

The following sequence is followed for unattended authentication of the PIV biometric. The ordering is flexible.

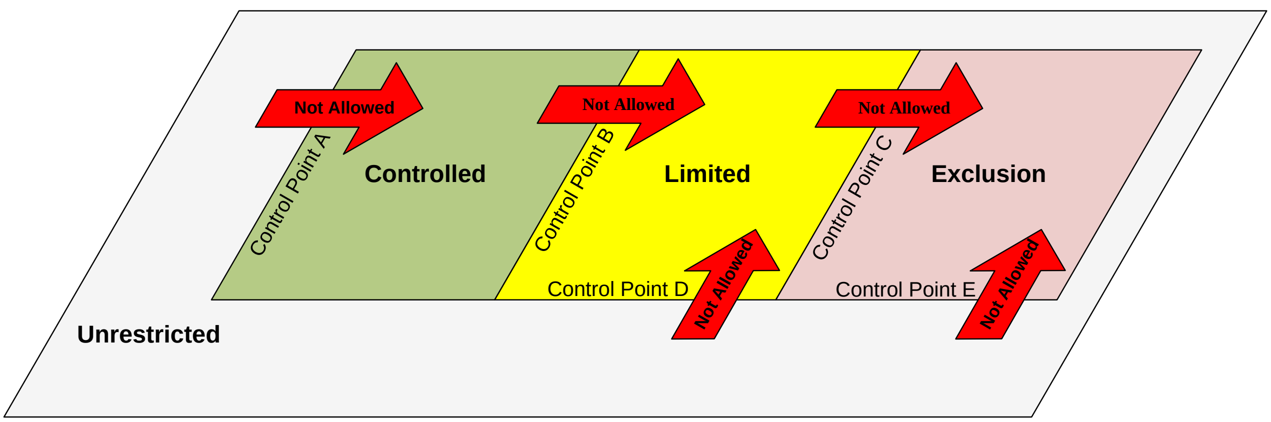
1. Insert PIV or PIV-I Card into reader.
2. Enter PIN.
3. PIN Transmitted to Card; Verify PIN; (if possible) notify remaining attempts after/if failed PIN.
4. Read data from card:
    a. Biometric
    b. CHUID
5. Obtain livescan biometric sample.
6. The Livescan biometric is sent to the E-PACS Infrastructure.
7. The CHUID and Card biometric are sent to the E-PACS Infrastructure.
8. The PACS performs validation functions.
    a. Validate livescan biometric against the card biometric.
    b. The CHUID expiration date is checked to ensure that the card has not expired (see PIA-3.6).
9. Upon biometric match, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

10.6.3 Unmitigated Threats

Unmitigated PACS Threats
Biometric Spoofing
Biometric Object Substitution
Use of Terminated Card
Use of Unreported Lost or Stolen Card
Electronic Counterfeiting

10.6.4 Pros, Cons, Issues

This pattern is zero-factor authentication. Therefore, this pattern is not sufficient for moving from the Unrestricted area into the Controlled area. At a minimum, this must be BIO (see Pattern #10: BIO) to move from the Unrestricted area to the Controlled area.

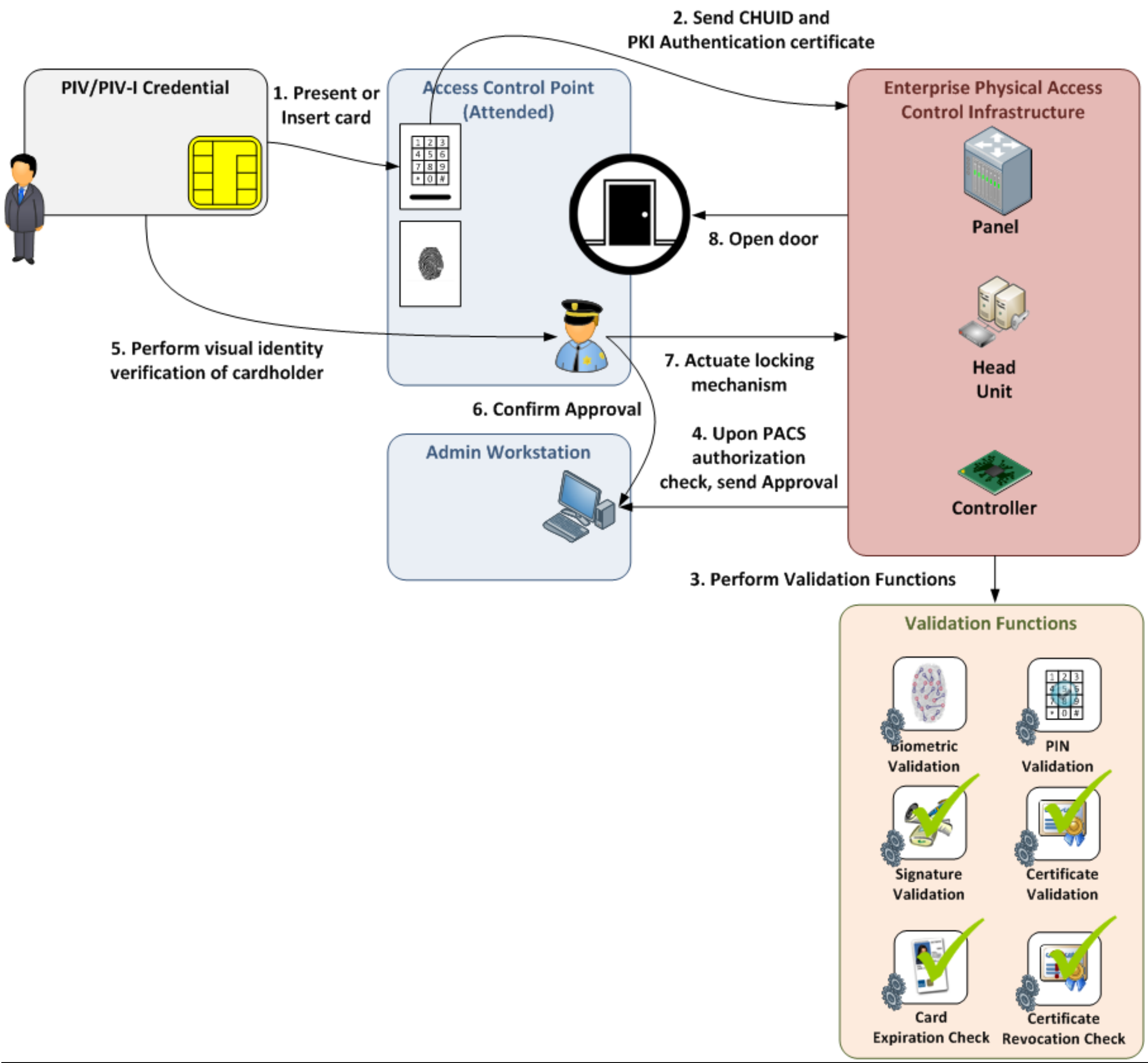


10.7 Pattern #7: Enhanced CHUID + VIS

This pattern can be achieved by combining Pattern #1: VIS and Pattern #5: Enhanced CHUID. In addition to using CHUID-based authentication with the PACS performing all necessary validation steps, the guard performs a visual identity verification of the cardholder. Though each pattern on its own is zero-factor authentication, combining these two patterns results in one-factor authentication.

1 Factor

10.7.1 Use Case Diagram



10.7.2 Description

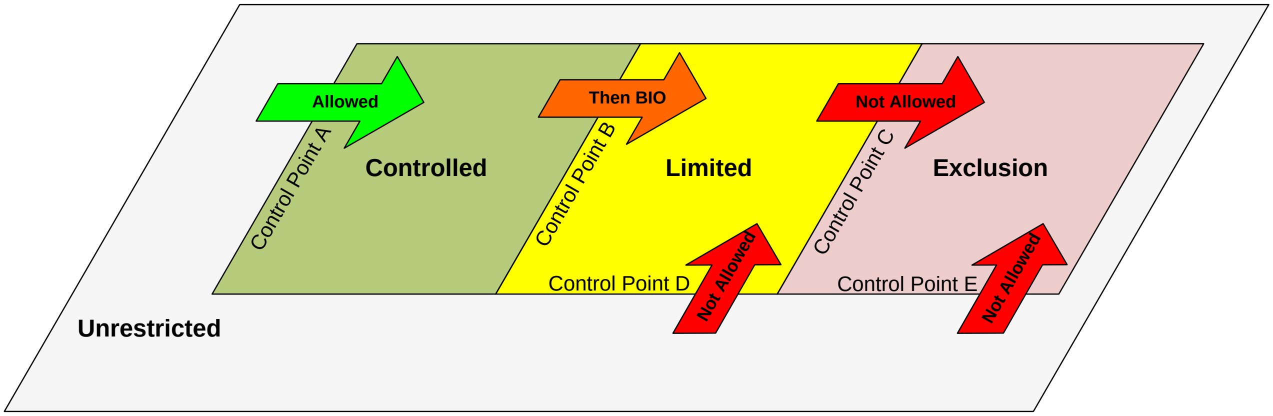
CHUID-based PIV or PIV-I Cardholder authentication is augmented by visual identity verification of cardholder to mitigate some risk factors of either design pattern alone. It should be noted that the two authentication steps are not two factors of authentication, as CHUID and VIS similarly fulfill the "something you have" factor of authentication. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

10.7.3 Unmitigated Threats

Unmitigated PACS Threats
Electronic Cloning
Skimming
Sniffing
Use of Unreported Lost or Stolen Card (until card is revoked)

10.7.4 Pros, Cons, Issues

This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area.



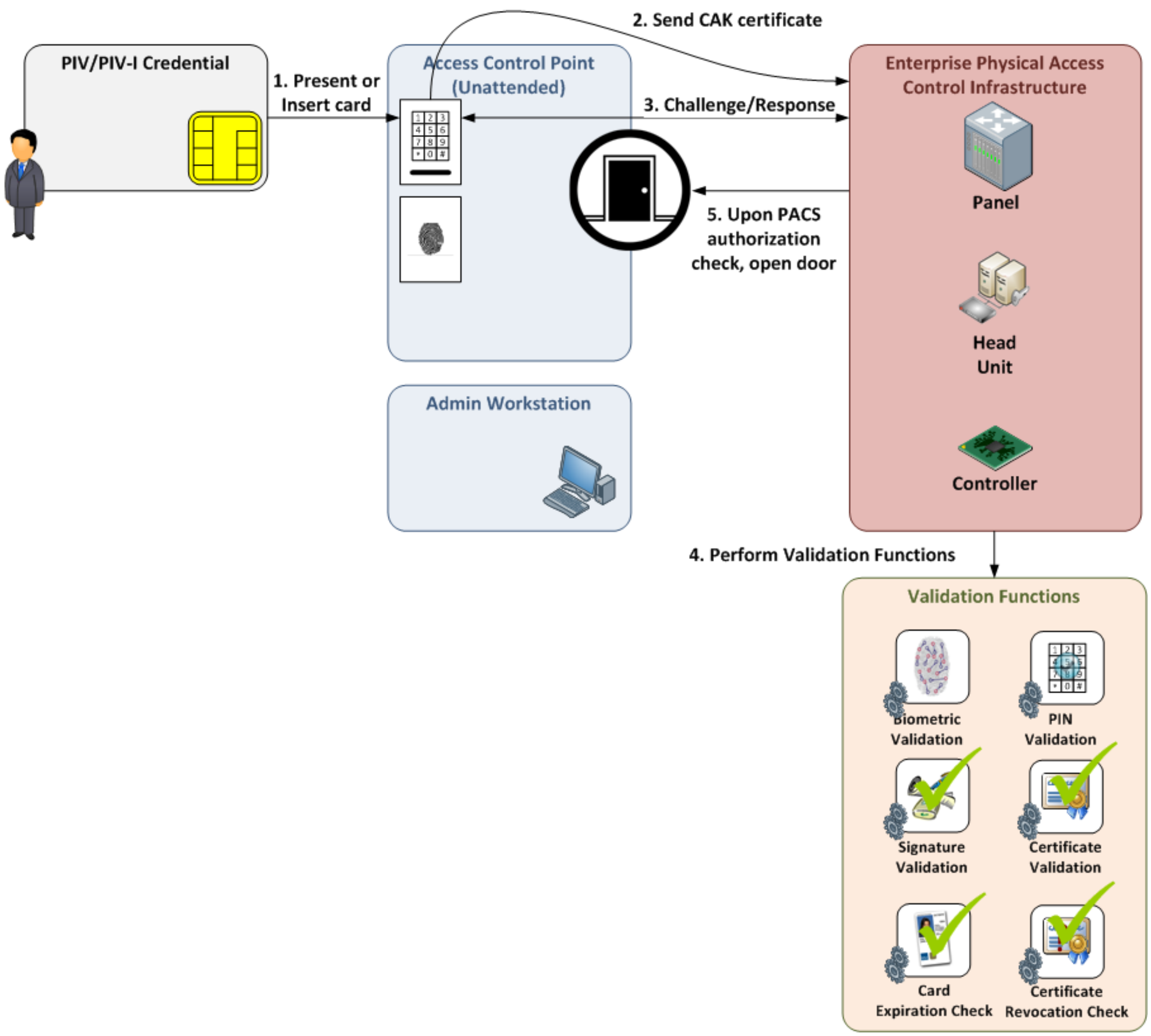
10.7.5 Considerations

Implement patterns #1 and #5 in combination (VIS and Enhanced CHUID). Note that implementing pattern #1 with pattern #2 (Partial CHUID), pattern #3 (Primitive CHUID), or pattern #4 (CHUID) will not achieve one-factor authentication, and is not consistent with [NIST SP 800-116].

10.8 Pattern #8: Asymmetric CAK

The PACS uses the asymmetric CAK (from the CAK certificate) in a challenge/response protocol. The PACS validates the CAK certificate (which should use PDVal), checks the CAK certificate's revocation status, and checks the CAK certificate's expiration date.

10.8.1 Use Case Diagram



10.8.2 Description

This pattern can use the contact or contactless interface.

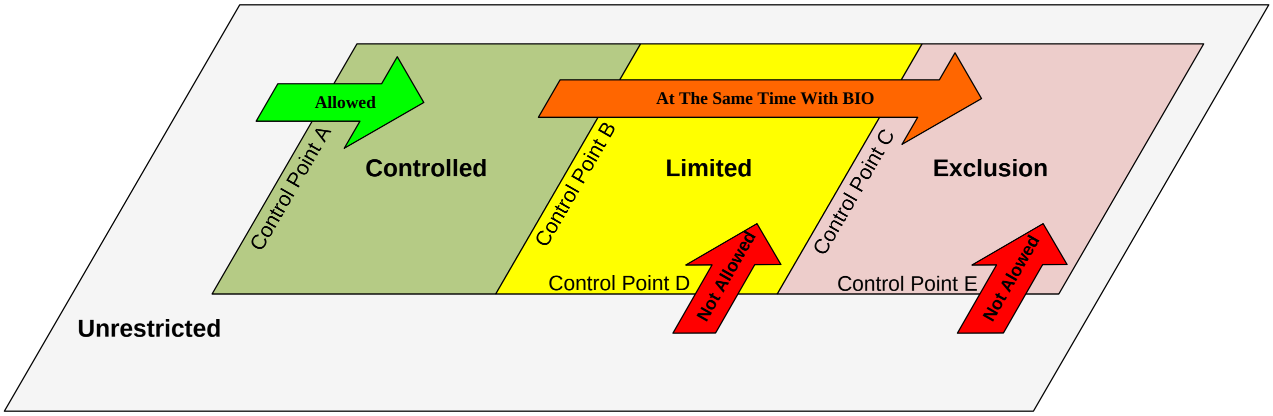
1. Present or insert PIV or PIV-I Card to card reader.
    a. CAK certificate is read from the PIV or PIV-I Card.
2. The CAK certificate is sent to the E-PACS Infrastructure.
3. Perform Challenge / Response:
    a. CAK certificate is sent to the PACS cryptographic validation function.
    b. PACS sends challenge to card (based on the public key in the CAK certificate).
    c. Card sends a response using private key on the chip.
    d. The PACS signature validation function validates the card response.
4. The PACS performs validation functions.
    a. CAK certificate PDVal and revocation check (see PIA-5).
    b. The CAK certificate expiration date is checked to ensure that the card has not expired (see PIA-3.6).
5. Upon successful challenge/response and PDVal/revocation check, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

10.8.3 Unmitigated Threats

Unmitigated PACS Threats
Social Engineering
Use of Unreported Lost or Unreported Stolen Card (until card is revoked)

10.8.4 Pros, Cons, Issues

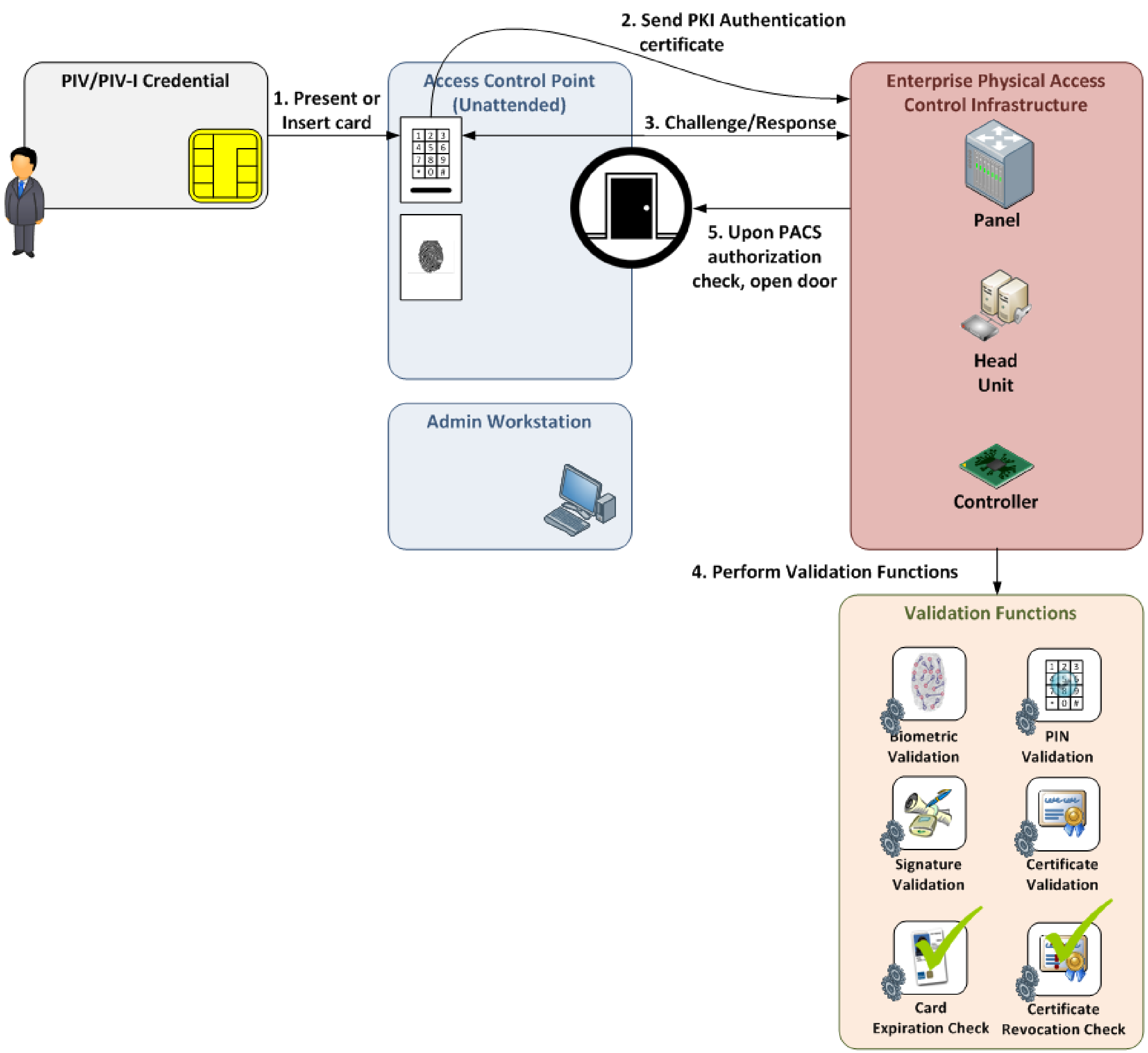
This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area.



10.9 Pattern #9: Symmetric CAK

The PACS uses the symmetric CAK in a challenge/response protocol. The PACS uses the PKI Authentication certificate to check revocation status. The PACS also checks the PKI Authentication certificate's expiration date.

10.9.1 Use Case Diagram



10.9.2 Description

This pattern can use the contact or contactless interface.

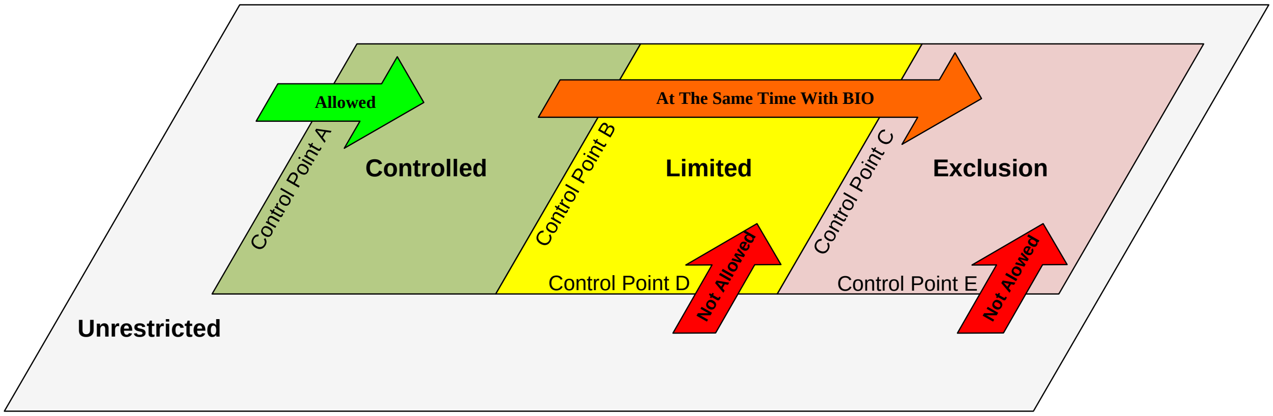
1. Present or insert PIV or PIV-I Care to card reader.
    a. The PKI Authentication certificate is read from the PIV or PIV-I Card.
2. The PKI Authentication certificate is sent to the E-PACS Infrastructure.
3. Challenge / Response:
    a. PACS reads the card identifier (diversification element) to be used to diversify the PACS key.
    b. PACS uses the diversification element to calculate the specific key of the card using the system master key.
    c. PACS sends random data to the card to be challenge.
    d. Card responds to the random challenge.
    e. PACS performs same encryption and compares.
4. The PACS performs validation functions.
    a. Check to see if card has been revoked using the PKI Authentication certificate.
    b. The PKI Authentication certificate expiration date is checked to ensure that the card has not expired (see PIA-3.6).
5. Upon successful challenge/response and revocation check, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

10.9.3 Unmitigated Threats

Unmitigated PACS Threats
Social Engineering
Use of Unreported Lost or Unreported Stolen Card (until card is revoked)

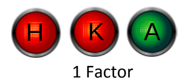
10.9.4 Pros, Cons, Issues

This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area.

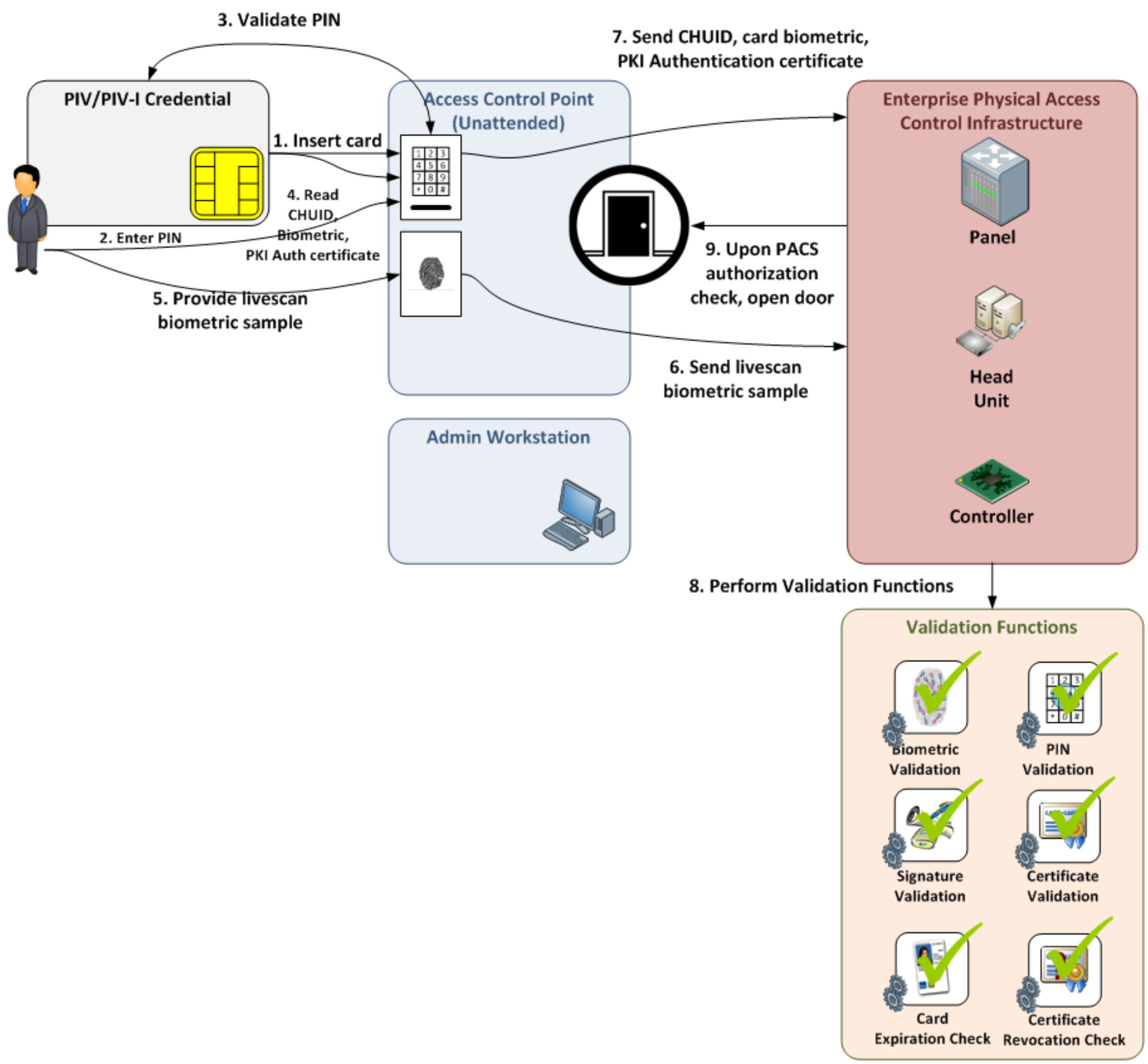


10.10 Pattern #10: BIO

The PACS validates a livescan biometric submitted by the cardholder against the biometric on the card, and performs all necessary validation functions. The PACS validates the signature on the biometric object, validates the content signer certificate (which should use PDVal), and checks the revocation status of the associated PKI Authentication certificate. The PACS also checks the PKI Authentication certificate's expiration date.



10.10.1 Use Case Diagram



10.10.2 Description

This pattern uses just the contact interface. The following sequence is followed for unattended authentication of the PIV biometric. The ordering is flexible.

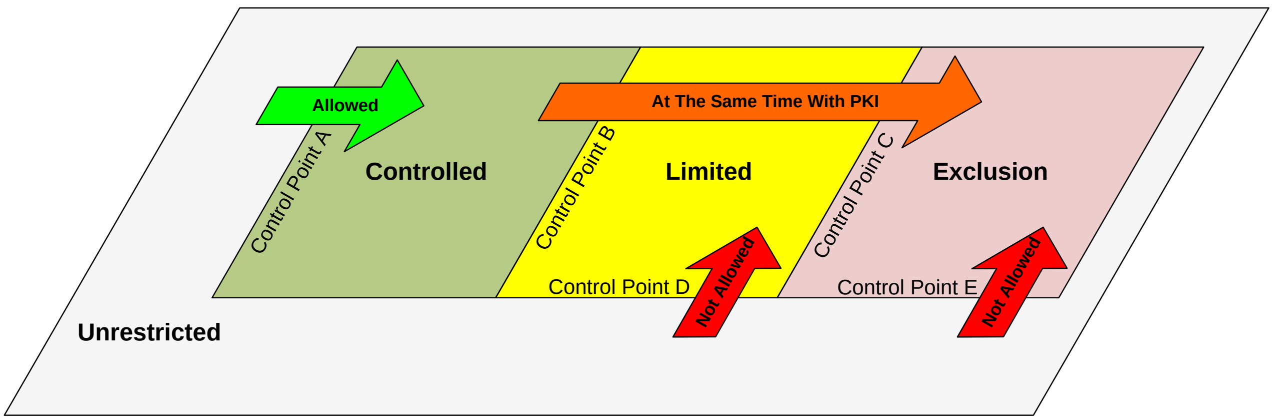
1. Insert PIV or PIV-I Card into reader.
2. Enter PIN.
3. Verify PIN Accepted; (if possible) notify remaining attempts after/if failed PIN.
4. Read data from card:
    a. CHUID
    b. Biometric
    c. If the PKI Authentication Certificate has not been cached, the PKI Authentication Certificate is read from the card.
5. Obtain livescan biometric sample.
6. The livescan biometric sample is sent to the E-PACS Infrastructure.
7. The PKI Authentication certificate and card biometric are sent to the E-PACS Infrastructure.
8. The PACS performs validation functions.
    a. Validate livescan against retrieved biometrics.
    b. Validate biometric and PKI Authentication certificate.
        i. Perform full PDVal and revocation of content signer certificate, which usually comes from the CHUID (see PIA-4 and PIA-5).
        ii. Verify binding between PKI Authentication certificate and biometric (same FASC-N if PIV Card, or same UUID if PIV-I Card).
        iii. Check revocation status of associated PKI Authentication certificate (see PIA-3.5).
        iv. The PKI Authentication certificate expiration date is checked to ensure that the card has not expired (see PIA-3.6).
9. Upon match and verifications, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

10.10.3 Unmitigated Threats

Unmitigated PACS Threats
Biometric Spoofing

10.10.4 Pros, Cons, Issues

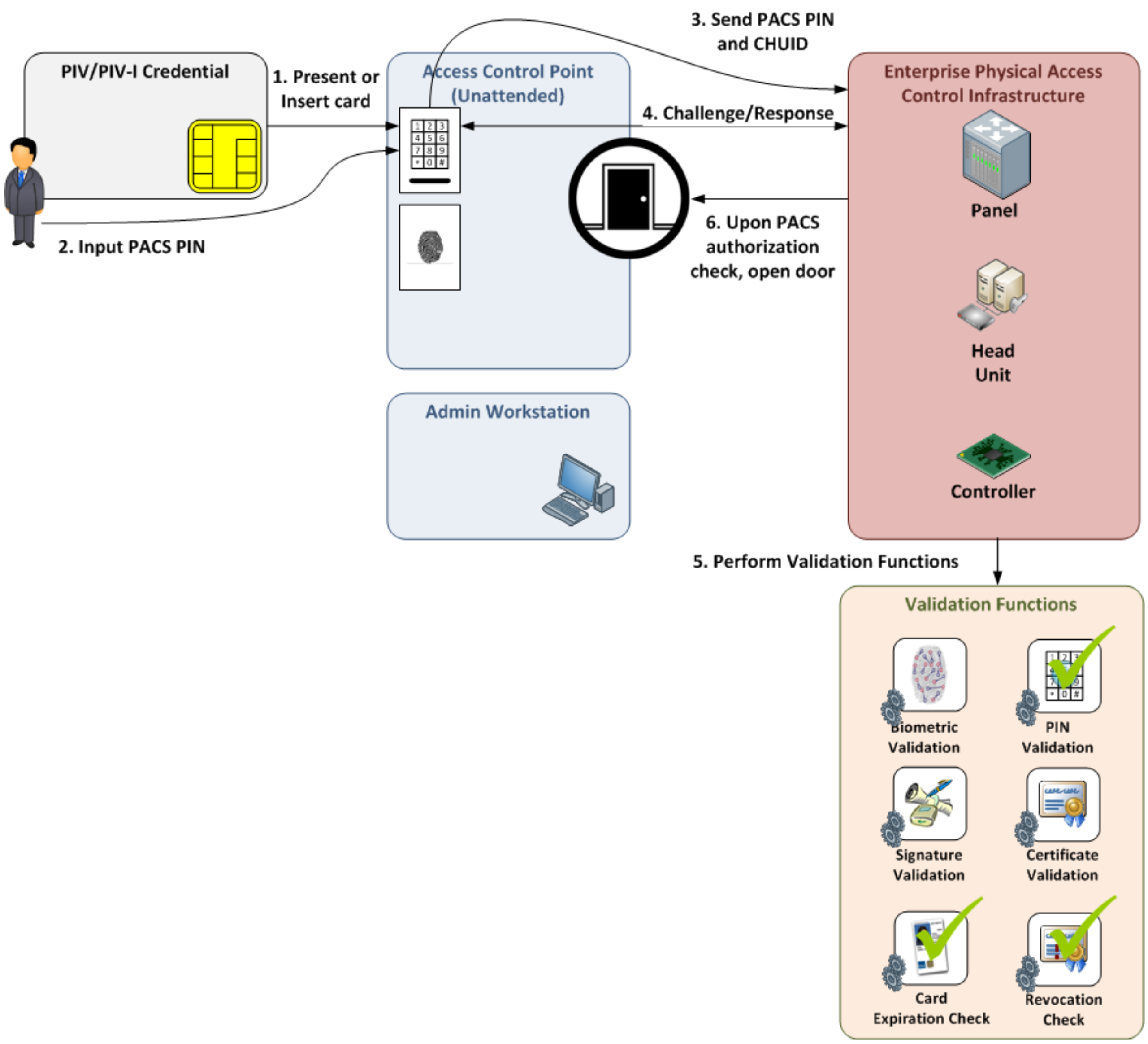
This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area.



10.11 Pattern #11: PIN to PACS

The PACS uses a PIN entered by the cardholder. The PACS verifies that PIN against the PIN associated with the card stored by the PACS. The PACS checks revocation status by validating the unique credential identifier obtained from the CHUID. The PACS also checks the CHUID's expiration date.

10.11.1 Use Case Diagram



10.11.2 Description

This pattern can use the contact or contactless interface. This pattern uses strong PIV Authentication for registration. In addition, this pattern enforces use of different PINs to conform to different authentication / authorization policies.

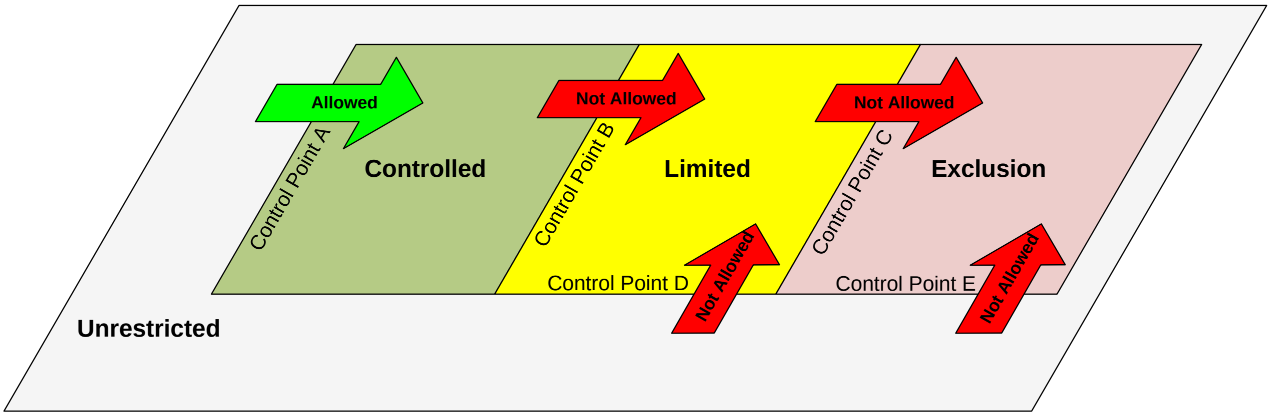
1. Present or insert PIV or PIV-I Card to the card reader.
    a. The CHUID is read electronically from the PIV or PIV-I Card.
2. User is prompted for PACS PIN.
3. The PACS PIN (or its hash) and CHUID are sent to the E-PACS Infrastructure.
4. The PACS performs validation functions.
    a. The unique card identifier (FACS-N or GUID) is extracted from the CHUID, and the PACS checks if the card identifier is active and in good standing (not revoked).
    b. The PACS validates the PIN entered by cardholder against the secure PACS PIN data base.
    c. The CHUID expiration date is checked to ensure that the card has not expired (see PIA-3.6).
5. Upon PIN validation, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

10.11.3 Unmitigated Threats

Unmitigated PACS Threats
Social Engineering

10.11.4 Pros, Cons, Issues

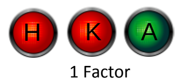
This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area[40].



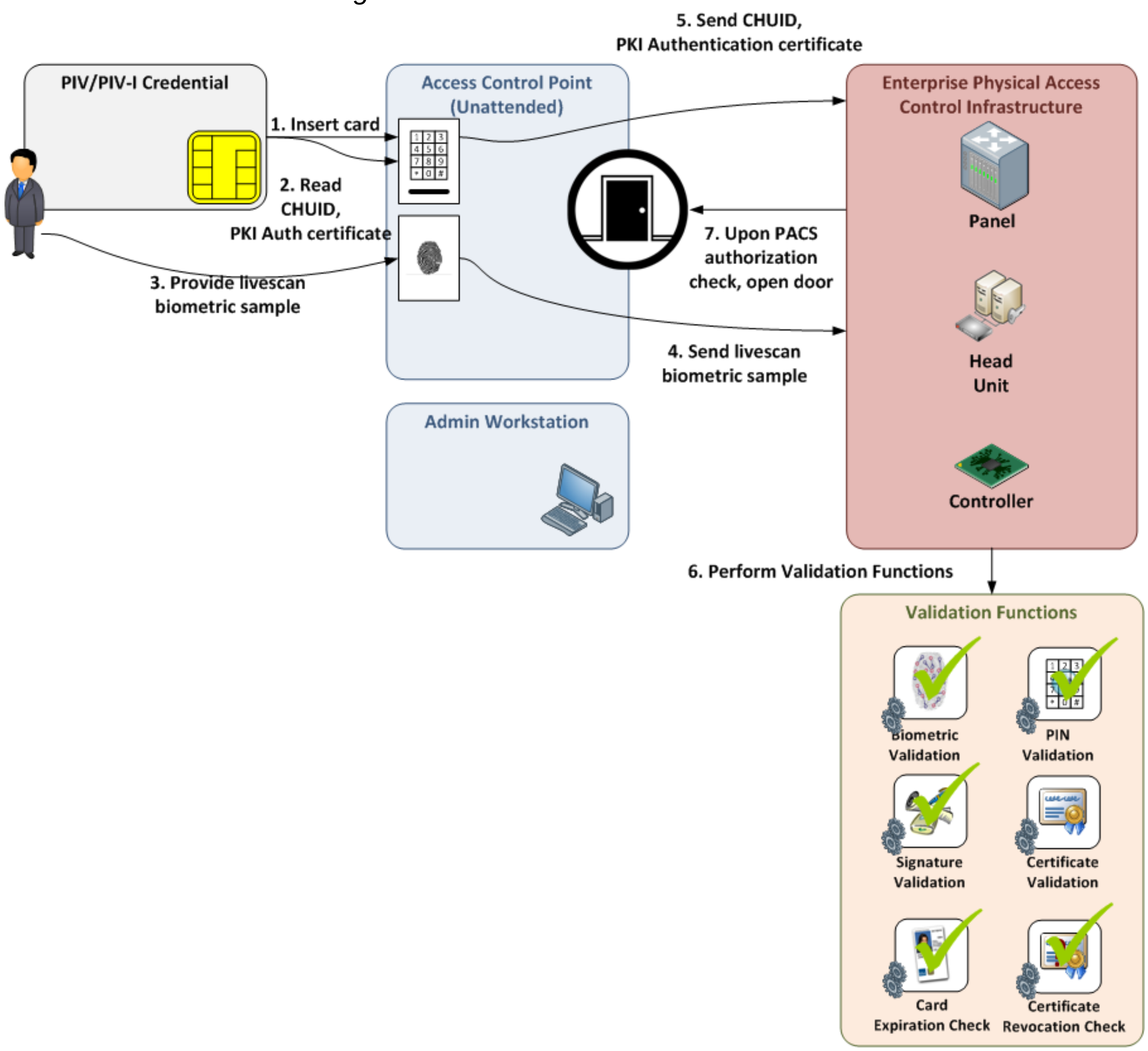
[40] [NIST SP 800-116] does not address this use case, and as such does not provide guidance on movement through areas.

10.12 Pattern #12: BIO to PACS

The PACS uses a biometric submitted by the cardholder. The PACS validates the livescan biometric against the biometric for the cardholder stored in the PACS database. In addition, the PACS performs all necessary validation functions. The PACS validates the associated PKI Authentication certificate (which should use PDVal), checks the revocation status of the PKI Authentication certificate. The PACS also checks the PKI Authentication certificate's expiration date.



10.12.1 Use Case Diagram



10.12.2 Description

This pattern can use the contact or contactless interface. The following sequence is followed for unattended authentication of the PIV biometric. The ordering is flexible.

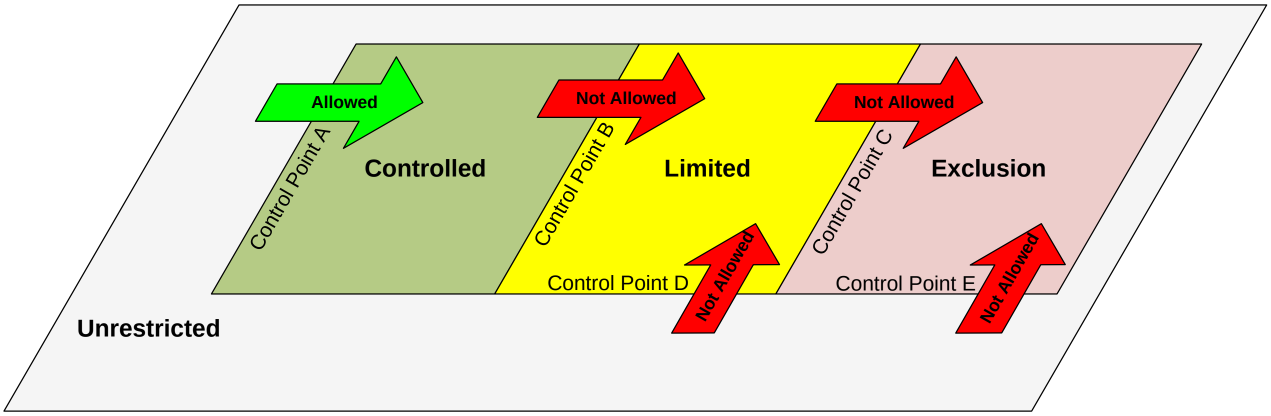
1. Present or insert PIV or PIV-I Card into reader.
2. Read data from card:
    a. CHUID
    b. If the PKI Authentication Certificate has not been cached, the PKI Authentication Certificate is read from the card.
3. Obtain livescan biometric sample.
4. The livescan biometric sample is sent to the E-PACS Infrastructure.
5. The CHUID and PKI Authentication certificate are sent to the E-PACS Infrastructure.
6. The PACS performs validation functions.
    a. PACS uses unique identifier from the CHUID to access biometric stored in the PACS database.
    b. Validate livescan against biometric retrieved from the PACS database.
    c. Check revocation status of associated PKI Authentication certificate (see PIA-3.5).
    d. The PKI Authentication certificate's expiration date is checked to ensure that the card has not expired (see PIA-3.6).
7. Upon match and verifications, the PACS checks whether the authenticated cardholder is authorized to enter.
    b. Upon authorization, the door is unlocked.

10.12.3 Unmitigated Threats

Unmitigated PACS Threats
Biometric Spoofing

10.12.4 Pros, Cons, Issues

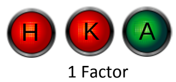
This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area[41].



[41] [NIST SP 800-116] does not address this use case, and as such does not provide guidance on movement through areas.

10.13 Pattern #13: BIO-A to PACS

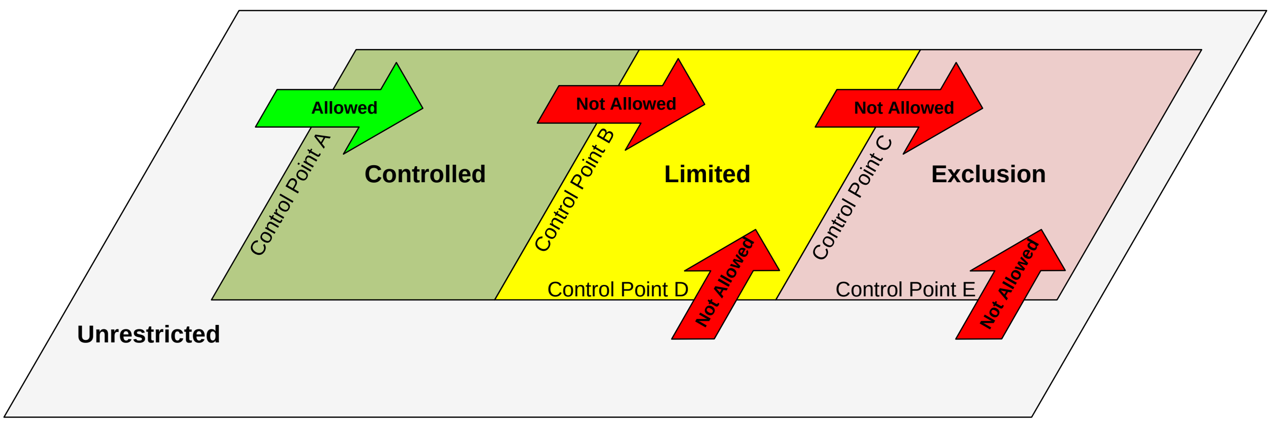
This pattern can be achieved by combining Pattern #1: VIS and Pattern #12: BIO to PACS . In addition to using biometric authentication with the PACS performing all validation steps, the guard supervises submission of the cardholder biometric (to prevent use of fake/synthetic fingerprint), thus increasing the level of trust in the biometric factor. The guard may also verify visually the card used, but this is not considered an additional factor.



There are no unmitigated threats in this pattern.

Unmitigated PACS Threats

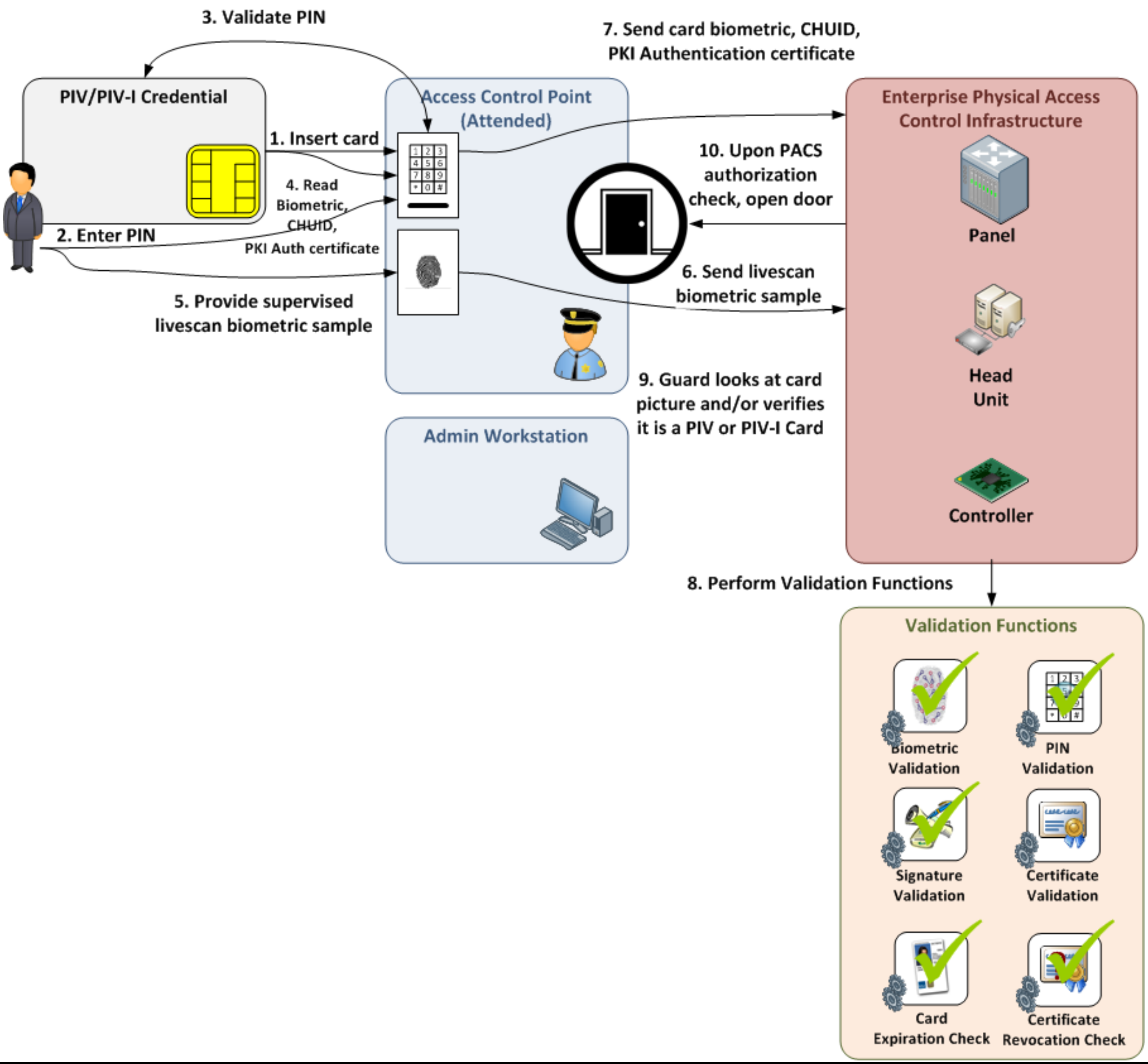
This pattern is one-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Controlled area.



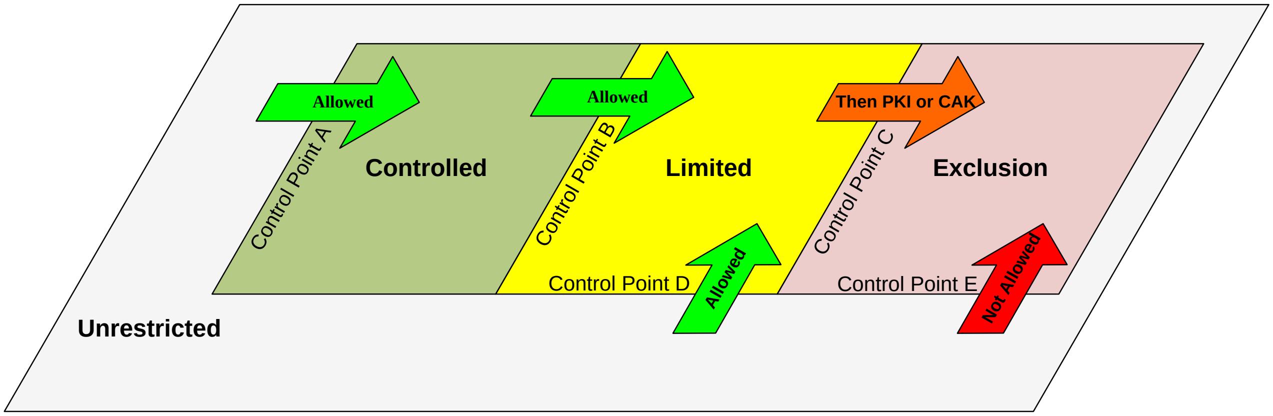
10.14 Pattern #14: BIO-A

This pattern can be achieved by combining Pattern #1: VIS and Pattern #10: BIO. In addition to using biometric authentication with the PACS performing all validation steps, the guard supervises submission of the cardholder PIN and biometric (to prevent use of fake/synthetic fingerprint). Though VIS is zero-factor authentication and BIO is one-factor authentication, combining these two patterns results in two-factor authentication.

10.14.1 Use Case Diagram



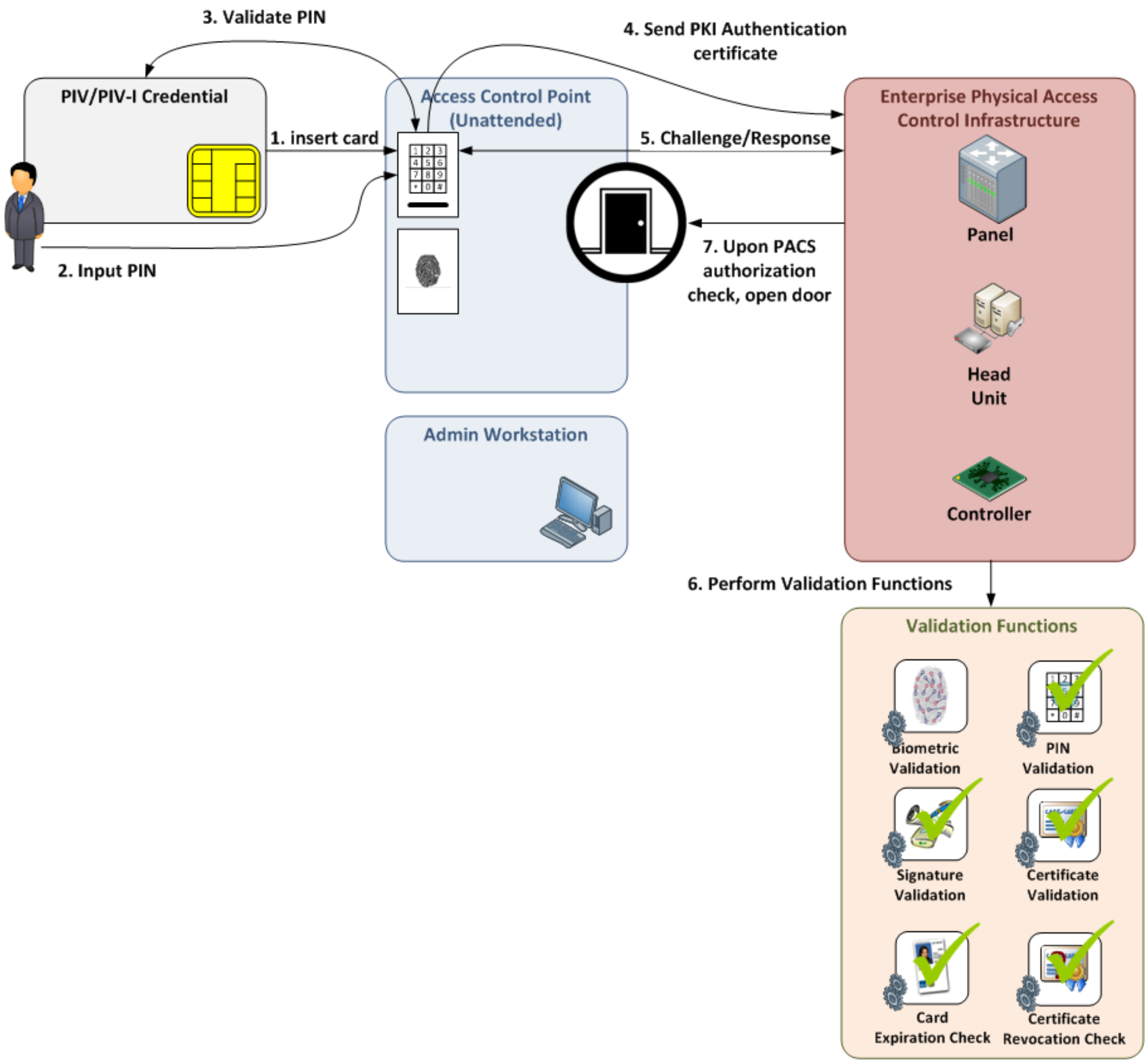
This pattern is sufficient for moving from the Unrestricted area into the Limited area.



10.15 Pattern #15: PKI-Auth

The PACS uses the private key (from the PKI Authentication certificate) in a challenge/response protocol. The PACS validates the PKI Authentication certificate (which should use PDVal), and checks the PKI Authentication certificate's revocation status. The PACS also checks the PKI Authentication certificate's expiration date.

10.15.1 Use Case Diagram



10.15.2 Description

This pattern can use the contact interface. The PIV Card and the PIV-I Card carry a mandatory asymmetric authentication private key and corresponding certificate. The following steps is used to perform authentication using the card's asymmetric authentication key:

1. Insert PIV or PIV-I Card into card reader.
2. Enter PIN.
3. Verify PIN Accepted; (if possible) notify remaining attempts after/if failed PIN.
4. The PKI Authentication certificate is sent to the E-PACS Infrastructure.
5. Challenge / Response:
    a. PKI Authentication certificate is sent to the PACS cryptographic validation function.
    b. PACS sends challenge to card (based on the public key in the PKI Authentication certificate).
    c. Card sends a response using private key on the chip.
    d. The PACS signature validation function validates the card response.
6. The PACS performs validation functions.
    a. PKI Authentication certificate PDVal and revocation check (see PIA-5).
    b. The PKI Authentication certificate expiration date is checked to ensure that the card has not expired (see PIA-3.6).
7. Upon successful challenge/response and PDVal/revocation check, the PACS checks whether the authenticated cardholder is authorized to enter.
    a. Upon authorization, the door is unlocked.

Some of the characteristics of the PKI-based authentication mechanism are as follows:

1. Requires the use of online certificate status checking infrastructure
2. Highly resistant to credential forgery
3. Strong resistance to use of unaltered card by non-owner since PIN is required to activate card
4. Applicable with contact-based card readers.

10.15.3 Unmitigated Threats

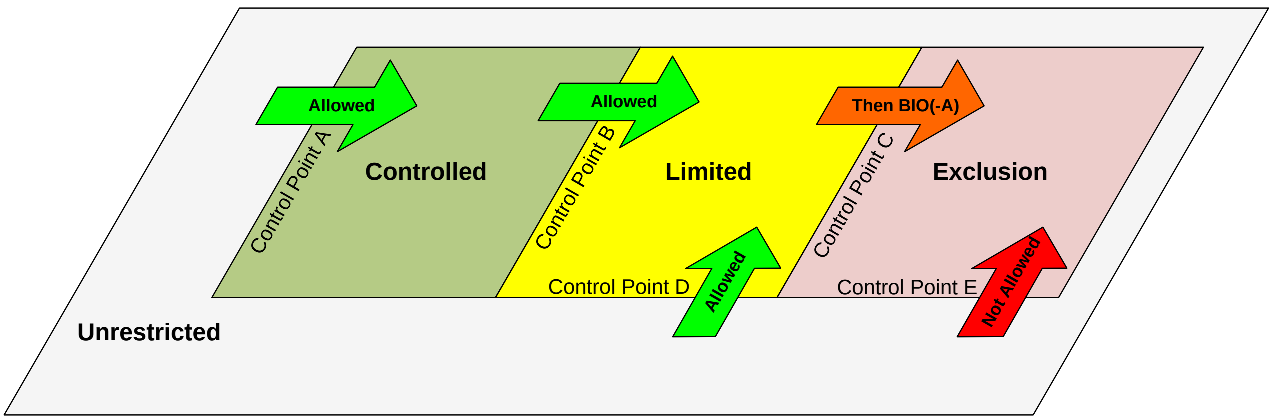
Unmitigated PACS Threats
Social Engineering

10.15.4 Pros, Cons, Issues

This pattern is two-factor authentication (PKI and PIN). Therefore, this pattern is sufficient for moving from the Unrestricted area into the Limited area.

Factor one is possession of a PIV card, verified by the PACS by the active authentication (the challenge response) together with the verification of trusted origin (the path validation).

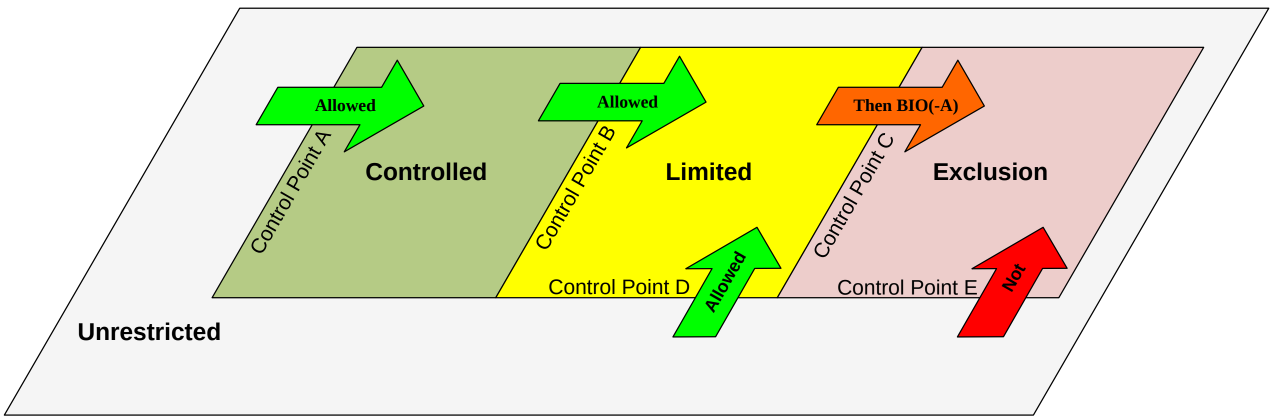
Factor two is knowledge of the PIV PIN. Although the PACS does not see or verify the PIN directly, it knows that the PIV or PIV-I Card will not use the Authentication Key to respond to the challenge unless the PIN has been presented to it and verified. Thus, in responding to the challenge, the PIV or PIV-I Card is able to "transfer the trust" that the Cardholder knows and correctly presented the PIN.



10.16 Pattern #16: Asymmetric CAK + PIN to PACS

This pattern can be achieved by combining Pattern #8: Asymmetric CAK and Pattern #11: PIN to PACS. Please review those patterns to understand this combined pattern. Note that in this pattern, the identifier comes from the CAK certificate instead of the CHUID. The credential number found in the certificate for the CAK must be transmitted to support PIN to PACS. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

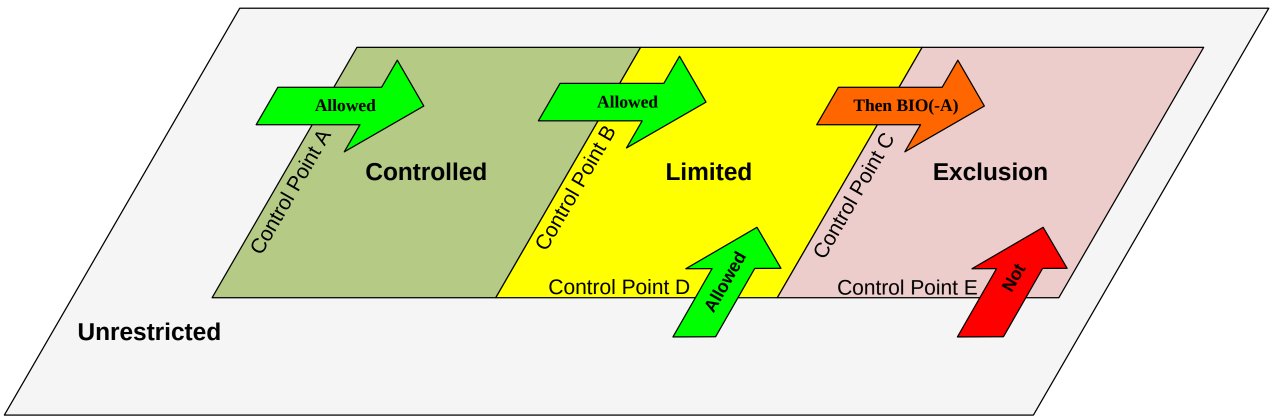
This pattern is two-factor authentication Therefore, this pattern is sufficient for moving from the Unrestricted area into the Limited area.



10.17 Pattern #17: Symmetric CAK + PIN to PACS

This pattern can be achieved by combining Pattern #9: Symmetric CAK and Pattern #11: PIN to PACS. Please review those patterns to understand this combined pattern. Note that in this pattern, the identifier comes from the PKI Authentication certificate instead of the CHUID. The credential number found in the certificate for the PKI Authentication certificate must be transmitted to support PIN to PACS. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

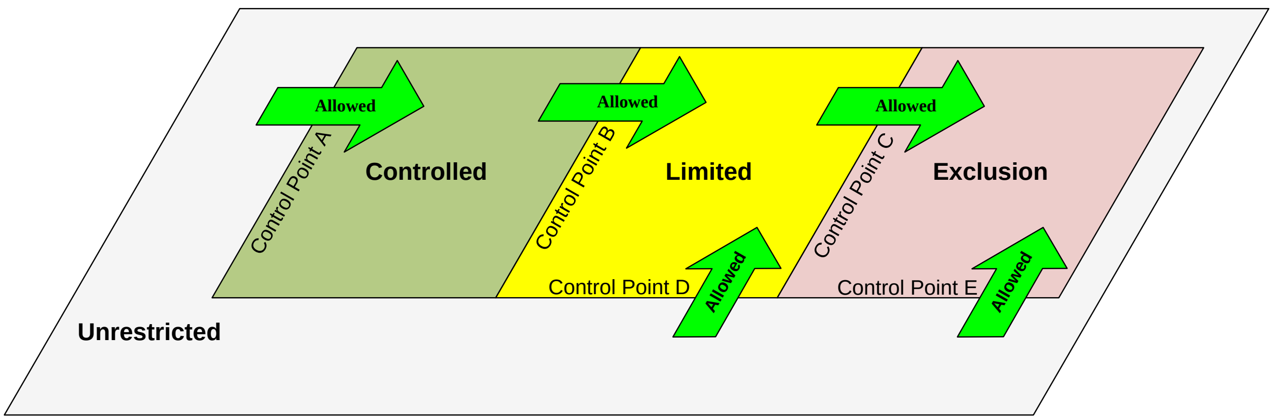
This pattern is two-factor authentication Therefore, this pattern is sufficient for moving from the Unrestricted area into the Limited area.



10.18 Pattern #18: Asymmetric CAK + BIO-A

This pattern can be achieved by combining Pattern #8: Asymmetric CAK and Pattern #14: BIO-A. Please review those patterns to understand this combined pattern. The credential number found in the certificate for the CAK must match the credential number found in the biometric. The contact interface should be used because there are risks if CAK is contactless and BIO is contact. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

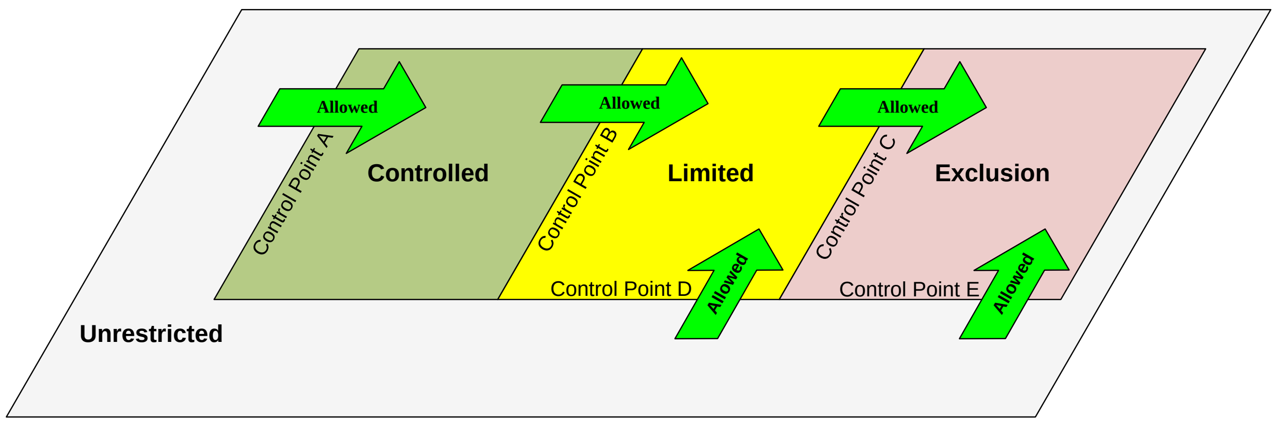
This pattern is three-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Exclusion area.



10.19 Pattern #19: Symmetric CAK + BIO-A

This pattern can be achieved by combining Pattern #9: Symmetric CAK and Pattern #14: BIO-A. Please review those patterns to understand this combined pattern. The credential number found in the certificate for the PKI Authentication certificate must match the credential number found in the biometric. The contact interface should be used because the BIO information is available only on the contact interface. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

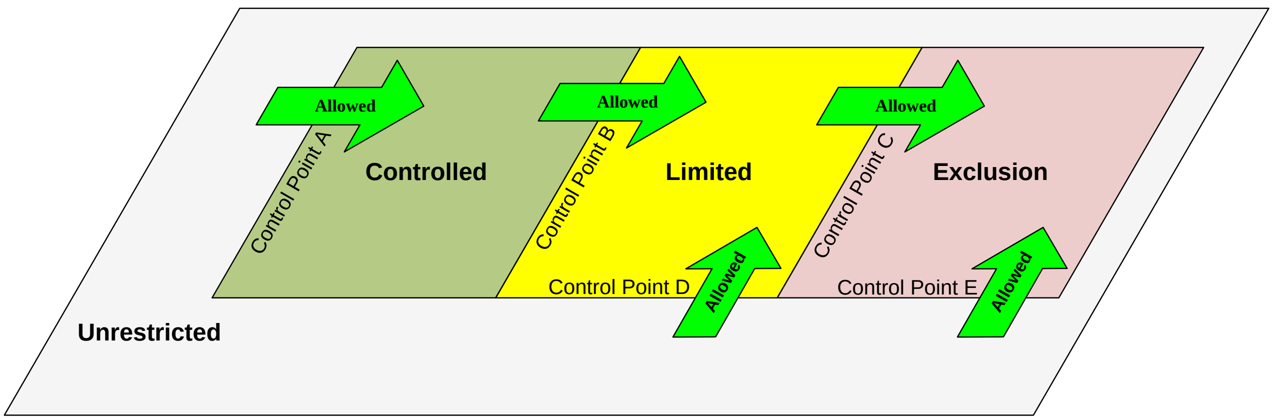
This pattern is three-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Exclusion area.



10.20 Pattern #20: PKI-Auth + BIO-A

This pattern is similar to Pattern #18: Asymmetric CAK + BIO-A. However, in this pattern, the PIV Authentication certificate replaces the CAK certificate in all steps. The credential number found in the certificate for the PIV Authentication certificate must match the credential number found in the biometric. Entry is allowed only after the PACS verifies that the authenticated cardholder is authorized to enter.

This pattern is three-factor authentication. Therefore, this pattern is sufficient for moving from the Unrestricted area into the Exclusion area.



11. Implementation Guidance

Implementation of PACS depends on a number of local decisions based on risk, budget, current state, and operational feasibility. While there will be considerable variations on how individual PACS are implemented or upgraded, there are several key areas that should be addressed by any PACS implementation plan.

[FICAM Roadmap] Chapter 10 includes guidance on planning, designing, and implementing a PACS in accordance with OMB policy and alignment with the FICAM segment architecture. The following sections highlight key areas and relevant considerations for each.

11.1 Determine Facility Security Level

Many PACS implementation decisions are driven by the sensitivity of the facility as a whole. The Interagency Security Committee (ISC) issued [Facility Security Levels] in 2008, which established a common methodology for conducting security assessments for the Federal Government. This ISC document explains how to assess the threats, vulnerabilities, and consequences at a federal facility to determine the Facility Security Level. Additional guidance addressing the key steps and considerations for conducting a Facility Risk Assessment can be found in [FICAM Roadmap] Section 10.1.2.

11.2 Determine NIST SP 800-116 Designation for Each Physical Area

As described in Section 7, [NIST SP 800-116] defines the following designations for physical areas within a facility: Unrestricted, Controlled, Limited, and Exclusion. Section 8 provides further guidance on the application of these designations as part of a local risk management framework. Agencies should establish designations for each physical area of their facilities. Many decision on PACS functionality and authentication patterns will depend on which designation has been determined for a given area.

In addition, agencies should establish policies for these determinations to ensure uniform application. These policies should employ a risk-based approach, considering the Facility Security Level, threats, vulnerabilities, and consequences.

11.3 Key Process Design

A number of key processes have a strong impact on the overall effectiveness of a physical access control strategy. Table 11-1 defines use cases that should be carefully addressed as part of the overall local risk management approach.

Table 11-1, Key Processes

Use Case	Description
Provisioning	Access rights should be provisioned for each physical area controlled by a PACS. Authenticating a credential is not sufficient to make an access control decision, because not everyone whose card can be authenticated necessarily has a right to be in a given area. Agencies should establish effective processes for determining access rights and provisioning those rights into the PACS.

Use Case	Description
	In addition, establishing an automated provisioning capability to populate PACS user attributes and credential information from authoritative data sources is a requirement of the FICAM segment architecture. See [FICAM Roadmap] Section 10.3.1 for additional provisioning to PACS.
Visitors	Visitors for a given facility may not have cards that can be authenticated and/or may not have access rights pre-provisioned for a given facility. Policies and processes should be established for controlling and enabling visitor access. See [FICAM Roadmap] Section 10.5, Visitor Access, for additional information on visitor management.
Temporary Cards	Individuals with legitimate access rights may not have their PIV or PIV-I cards for short periods of time. For example, if cards are forgotten, lost, stolen, or have not yet been issued. Policies and processes for these cases should be established.

It is important to note that addressing these use cases could inadvertently reduce the overall security of a given facility. Each of these use cases may create attack vectors that can be exploited by attackers. Agencies should carefully analyze these key processes to ensure they do not introduce new vulnerabilities.

11.4 PACS Requirements and Design

Once the risks for a given area are well understood, appropriate requirements for PACS functionality can be determined. This document offers two important resources that should be used to determine requirements for target state PACS:

- **Standard Security Controls** – Section 8 defines standard security controls to be implemented by a PACS based on local risk determinations; and
- **Authentication Patterns** – Section 10 describes authentication patterns implemented by PACS for interacting with PIV and PIV-I cards.[42]

It is anticipated that an agency will use the detailed guidance provided in this document related to security controls and authentication patterns in conjunction with guidance provided in [FICAM Roadmap] Chapter 10. Broader guidance related to the architecture and design of a modernized, E-PACS can be found in [FICAM Roadmap] Section 10.2. In addition, descriptions of the key PACS implementation activities across the full system development life cycle and estimated completion times can be found in [FICAM Roadmap] Section 10.1.4.

11.5 Holistic Review

Implementers should periodically review their overall PACS posture. Over time, adjustments to processes and technologies are inevitable. Diligence on individual PACS components is not sufficient to effectively

[42] Note that Section 10 presents a number of authentication patterns that are not recommended and do not constitute "PIV Enablement" required by various OMB directives. See Table 10-1 for summary information.

manage risk over time. The resources described above can be used in independent audits of an overall PACS using the risk-based requirements analyses described above.

APPENDIX A: USE OF SYMMETRIC KEYS WITH PACS CREDENTIALS

This appendix provides guidance for credential issuers willing to use symmetric keys in PACS credentials. The use of symmetric keys is not advocated by HSPD-12, as the requirement of protecting symmetric keys does not provide easy interoperability between independent operators and systems. This appendix does not provide the pros and cons of using a symmetric key over an asymmetric key, but rather describes the minimum security precautions required from a system using symmetric keys.

This appendix does not provide explicit description of the various cards (or card data models) providing symmetric keys, as they can be very different between a PIV Card (CAK is optional and can be symmetric), a PIV-I Card (CAK must be present and must be asymmetric), or Facility Access cards such as iClass, Mifare, DesFire and similar proprietary cards available in the open market.

It may also be useful to note that NIST has indicated that the FIPS 201-2 revision may allow the CAK to have two keys in the same card, one mandatory asymmetric (providing interoperability) and one optional symmetric for use within the issuing agency (providing mutual authentication and a secure session). It is not anticipated that the symmetric mechanisms will be defined as an interoperable mechanism across the federal enterprise.

Useful guidance on key management can be found in [NIST SP 800-57] Parts 1 and 2.

11.6 A.1 USE OF SYMMETRIC KEYS WITH PACS CREDENTIALS

Symmetric keys can be used to provide security services such as confidentiality (e.g. secure session key). Integrity (Message Authentication Code), or Authentication. The following section addresses mainly authentication when a symmetric key is used to authenticate a card, but many existing protocols do provide for the other security functions (integrity as well as confidentiality) as a byproduct of the mutual authentication process. The detailed protocol is not described hereafter and is assumed to be known (as the authentication key itself) by the parties (card and reader).

Smart Card systems have used symmetric key mechanisms for decades quite successfully and have developed various techniques allowing applications to get some benefits of symmetric algorithms[43] while addressing inherent implementation issues. Smart Cards are very good at protecting keys (symmetric as well as asymmetric) but the two main issues that need to be addressed when using symmetric keys in a PACS are:

1. Protection of the key in the system (and its elements) using smart cards; and
2. Minimizing the consequences of a given key being exposed.

The following provides guidance on these two issues It does not try to provide guidance on systems willing to share symmetric keys, as doing so increases tremendously the risk of a given key being exposed, putting at risk all cards and all systems relying on the same shared key. As a consequence, symmetric keys should not be used in an "open" system (having multiple independent authorities) as the requirement of sharing a "master" key between systems does not allow for easy protection of the "master" key.

[43] Mainly speed of execution over asymmetric algorithms for the same key strength.

11.7 A.2 KEY DIVERSIFICATION IN SMART CARD SYSTEMS

The process of diversification of symmetric keys in credentials is a mechanism which uses a main (or master) key in the PACS application (Reader/Terminal/controller) with a unique derived key stored in each credential. When the credential is personalized (or activated to work with a given PACS), it receives a unique symmetric key which is calculated by the personalization system using the master key of the system and a unique reference from the credential (e.g., its credential number, a card manufacturing number, a diversification number) .[44]

When the a credential is later presented to a reader, the PACS calculates the credential key by deriving the credential key from the master key using the diversification value the credential provides. This diversification mechanism limits the exposure of a compromised key of a given credential (no other credential is at risk), and does not put the master key of the PACS application at risk either.

Many smart card data models provide for multiple keys (symmetric of asymmetric) for the same function with can be selected by the card itself (based on its environment), or by the terminal dealing with the card (from a table of key identifiers defined in the application). The PIV data model defined so far is restricted to one key per function, and the key which to be defined in advance without providing any protocol selection for potential multiple keys for a given type of key.[45] Because of this data model restriction in PIV (which does not allow a card to have multiple independent derived keys), the use of symmetric keys, even when diversified, is limited to closed non interoperable systems.

11.8 A.3 MASTER KEY LIFE SPAN IN A PACS

No key should be used forever. All keys (symmetric and asymmetric) should have a given life span. It is very important to define how long a given key is going to be used and have the means in a system to roll over new keys when the old ones expire. PIV provides such mechanisms for the asymmetric keys of the card (certificates valid for 3 years) but does not impose a requirement for symmetric keys when they are used.

This document recommends limiting the life span of a given master key to maximum of five years in all PACS systems. This arbitrary value is based on the fact PIV Cards are issued for five years and they do not allow having more than one symmetric key available. Facility Access cards which do not have the restrictions of the PIV data model (either shorter life span or possibility to update the symmetric key in the card), or PIV Cards in which the issuer keeps the possibility of updating (securely) the symmetric key value should consider to have a shorter life span (e.g. three years or less).

As a consequence, a given PACS may have more than one master key at any time to deal with. Based on the issuing date (or any other parameter available in the card identifier and used to select a given master key over another one), the PASC will know which master key to use to derive the card corresponding key.

It is also possible to use multiple master keys in a given PACS even at the same time. This would, in principle, limit the risk of a given master key of the set being compromised, and as such limit the number of

---

[44] A very simple mechanism to create diversified keys with algorithms which do not have weak keys (e.g., AES) is to use the unique credential number, pad (or hash) it to the block length of the algorithm and cipher it using the master key of the system. The resulting value can be used as the diversified key for the credential.

[45] The PLAID protocol version 8 (RSA 1024) allows to define up to 32 768 authentication keys in one card system.

cards to reissue[46]. This is only a theoretical protection as if multiple master keys are all protected the same way, in the same system, and as such all would likely be compromised at the same time. This technique only prevents a given master key from being "guessed" by an attacker.

11.9 A.4 Protection of secrets (e.g. master keys) in a PACS

The other issue that needs to be addressed in systems using symmetric keys is the protection of the master key within the system itself. As in systems using asymmetric keys for card authentication, the process themselves (e.g. cryptographic functions) as well as the general parameters used (e.g. trusted roots, date and time) have to be protected against tampering. However, in systems requiring mutual authentication (e.g. symmetric as well as asymmetric key based systems) the private/secret key (e.g. master key of the system) requires protection at all time against exposure.

The following describes possible technical architectures for any type of private (or secret) key that needs to be protected in a PACS environment.

1. The master key of a system should be protected using FIPS 140-2 level 3 devices at all times. The master key should never leave such a device, and be loaded securely[47]. The master key in the device should be erased or locked from use when such device is removed from the PACS system (e.g., maintenance, tests). Example of such devices are:

    a. A Hardware Security Module (HSM) attached to the PACS (only one element with the Master key shared over a network);

    b. A secure FIPS 140-2 level 3 approved device in Controllers where master keys are securely loaded from the PACS Head End; and

    c. A secure FIPS 140-2 level 3 in the readers (on the secure side of the reader). This could be a removable Secure Application Module (e.g. smart card) , or a fixed component in the reader, but in any case, the master key should be erased or locked against use when the reader (or the SAM) is not operational in the PACS system. The master key could be loaded securely in the device when the device is operational (i.e., connected to a PACS).

2. The master key of a system should be shared by as few elements as possible. For example, if the master key is protected in a Controller, it may be acceptable to have the calculated card derived key send (securely) to a protected element (also FIPS 140-2 certified) used by a door reader for the final authentication process and a secure session usage.

Many architectural possibilities are possible to protect such keys, and the above is only guidance on some basic principles to abide by. In addition to the basic security principles explained in this appendix, other

[46] When a master key is compromised, all cards which have a derived key from this master key cannot be trusted anymore as it would allow an attacker to generate cards with valid derived keys.

[47] It is also a good practice to have some kind of secure backup mechanism in case the device protecting the master key breaks down.

requirements such as key availability and overall performance should be taken in consideration during design.

11.10 A.5 Registration of credentials using symmetric keys in PACS

As explained earlier, the use of symmetric keys does not provide easy interoperability between independent systems. Moreover, beside the master key itself, it requires the PACS to know the diversification mechanism used for the credentials, as well as the rule of master key assignment to a given credential (see earlier point on multiple master keys over time).

This section has no specific recommendation, but just indicates the need for a given PACS to know all these specific “details” before it can use any credential based on symmetric keys. This is why this section applies mostly to closed systems (PIV or PIV-I Cards used by their own issuer or Facility access cards). All these credentials are known by the issuer and does need any generic interoperable method or be registered in a given PACS.

Nevertheless, it is highly recommended to use the strong identity verification available in the PIV/PIV-I data model to verify the validity of the credential and the legitimate user both at registration time in the PACS and from time to time (e.g. every month or quarter, or on a statistical basis). [48]

[48] Doing such verification using the asymmetric keys of the PIV data model (PKI-Auth or even Asymmetric CAK) would allow detection that a master symmetric key has been compromised in the system.

APPENDIX B: GLOSSARY

Term	Definition
Access Control	The process of granting or denying requests to access physical facilities or areas, or logical systems (i.e., computer networks or software applications). See also "Physical Access Control System."
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence in the identity of users or information systems. That is, achieve sufficient confidence in the binding between the entity and the presented identity.
Authentication Certificate	An authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the authentication key of the Card and a contact reader.
Authentication Factors	Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are: *Something you know* (for example, a password) *Something you have* (for example, an ID badge or a cryptographic key) *Something you are* (for example, a thumb print or other biometric data) Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors.
Authentication Mechanism	The authenticator(s) used to sufficiently prove the user is who he/she says he/she is.
Authentication Pattern	A description of a specific implementation of an authentication mechanism. Patterns are sometimes called use cases. The authentication patterns in this Guidance document are neutral in that recommended and not recommended patterns are presented.
Authenticator	The means used to confirm the identity of a user, process, or device (e.g., user password or token).
Biometric	A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.
Card Authentication Key (CAK)	An authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card authentication key of the Card and a contact or contactless reader.
Card Management System (CMS)	An application that manages the issuance and administration of multi-function enterprise access smart cards. The CMS manages cards, as well as data, applets and digital credentials, including PKI certificates related to the cards throughout their lifecycle.

Term	Definition
Cardholder Unique Identifier (CHUID)	The PACS Implementation Guidance [PACS] defines the CHUID data object; this description is refined in NIST SP 800-73. The PIV Card shall include the CHUID as defined in NIST SP 800-73. The CHUID includes an element, the Federal Agency Smart Credential - Number (FASC-N), which uniquely identifies each card. CHUID elements specific to this standard are described below in Section 4.2.1. The format of the CHUID signature element is described in Section 4.2.2. The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation. The PIV FASC-N shall not be modified post-issuance.
Certificate (X.509 Certificate)	A set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data. The digital representation of information at least: 1) identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it. The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Challenge/Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack.
Compensating Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Credential	A set of data presented as evidence of a claimed identity and/or entitlements.
Cryptographic (Crypto)	Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.
Digital Signature	A nonforgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.

Term	**Definition**
Enterprise PACS (E-PACS)	The FICAM Initiative established the notion of an Enterprise PACS “from that need to leverage US Government investments in HSPD-12 compliance, FIPS 201, and PIV Card technology for physical access solutions across agency and organizational boundaries." Enterprise PACS allows Federal government personnel and their contractors to authenticate their identities as visitors to other agencies' facilities using secure, PKI-enabled Federal PIV card standards. This is done using cards (e.g., PIV Cards, PIV-I Cards) already issued by their own organizations, which are subjected to fine-grained authorization decisions made by the agency or organization they are visiting, and by leveraging many aspects of existing PACS infrastructure.
Federal Agency Smart Credential - Number (FASC-N)	The FASC-N is the primary identification string to be used on all government issued credentials. The key to credibility, non-repudiation and reciprocity is the definition and acceptance of a credential token identification numbering schema for use across all Federal Agencies that is uniquely assigned to one and only one individual. For deployed systems, this is the FASC-N. For emerging systems, it is the GUID. Both are contained in the CHUID for consistent means of access by PACS solutions allowing for ease of migration. The responsibility for issuing this number to federal personnel is decentralized to the various federal agencies, with the ultimate responsibility for ensuring uniqueness residing with each agency’s CIO, or other duly designated agency official. For the FASC-N, this is achieved through an assigned Agency Code and subordinate system code and credential number.
Federation	An association of users, service providers, and identity service providers.
Full Path Validation	See Path Discovery and Validation (PDVal)
Global Unique Identifier (GUID)	The GUID is a mandatory data field defined within the Cardholder Unique ID (CHUID) as specified in [NIST SP 800-73] Part 1. For PIV-I Cards, the GUID field must contain an RFC 4122- conformant UUID value to support large Non Federal Issuer populations.
Identity Management Systems (IDMS)	An automated system of hardware (servers) and software (programs) that provides the workflow management (services) of identity functions, as normatively described in [FIPS 201]. An IDMS is separately layered and/or compartmentalized within one system and/or a modular component of an agency’s centralized system/enterprise. The IDMS will be encapsulated in an environment that is secure, auditable and protect the privacy of personal information. The IDMS establishes the centralized Chain-of Trust that is then integrated into the components of a FIPS 201 enterprise.
Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Term	Definition
Level of Assurance (Assurance Level)	The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned. In terms of [OMB M-04-04] and [NIST SP 800-63-1], four levels: Level 1: LITTLE OR NO confidence Level 2: SOME confidence Level 3: HIGH confidence Level 4: VERY HIGH confidence
Line Supervision	Taking steps to ensure that the line being used for the access control system has sensors and/or resistors to make sure the line isn't being compromised.
Livescan Fingerprinting	The technique and the technology used by law enforcement and private facilities to capture fingerprints and palm prints electronically, without the need for the more traditional method of ink and paper.
National Agency Check with Written Inquiries (NACI)	The basic and minimum investigation required for all new federal employees and contractors, which consists of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name, fingerprint files, and other files or indices when necessary. This investigation also includes written inquiries and searches of records covering specific areas of an individual's background during the past five (5) years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes employment (five (5) years); education (five (5) years and highest degree verified); residence (three (3) years); references; law enforcement (five (5) years); and NACs.
Non-repudiation	The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.
Partial CHUID	Design pattern where Because a PACS cannot transmit a full CHUID from the reader to the panel, the CHUID is truncated before it is sent to the panel. For example, the weigand line is limited to 48 bits so it will not take a full CHUID because there isn't enough room to transmit certain information/fields.

Term	**Definition**
Path Discovery and Validation (PDVal) (Also called "Full Path Validation")	Path Discovery is valuable for clients that do much of the PKI processing themselves and simply want a server to collect information for them. The server is trusted to return the most current information (e.g., certificates, Certificate Revocation Lists) that is available to it (which may not be the most current information that has been issued). Path Validation allows a server to perform a real time certificate validation for a validation time T, where T may be the current time or a time in the recent past. In order to validate a certificate, a chain of multiple certificates, called a certification path, may be needed, comprising a certificate of the public key owner (the end entity) signed by one Certification Authority (CA), and zero or more additional certificates of CAs signed by other CAs. See also Full Path Validation, PIA-5.
Personal Identity Verification – Interoperable (PIV-I) Card	An identity card that meets the technical standards to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows federal relying parties to trust the cards.
Personal Identity Verification (PIV) Card	A government-issued credit card-sized identification that contains a contact and contactless chip. The holder's facial image will be printed on the card, along with other identifying information and security features. The contact chip will store a PKI certificate, the Cardholder Unique Identifier (CHUID), and a fingerprint biometric, all of which can be used to authenticate the user for physical access to federally controlled facilities and logical access to federally-controlled information systems. A PIV Card is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure the PIV Cards are interoperable with and trusted by all Federal government relying parties.
Physical Access Control System (PACS)	Protection mechanisms that limit users' access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader) and may involve human control (e.g., a security guard). A PACS may support many more functions that are out of scope for this document.
PIV-Enabled	A PACS or an authentication mechanism that conforms to [FIPS 201]. For example, a PIV-enabled PACS accepts any PIV Card to prove identity.
Primitive Authentication Pattern	An authentication pattern that does not include signature validation and revocation check steps, which would/should otherwise be done in a more robust version of the same pattern.
Primitive CHUID	Design patter where a CHUID is used without verifying its signature. Verification a signature should include doing PDVal.
Revocation and Status Checking	Actions taken to determine whether a PKI certificate has been revoked or has expired, and therefore is no longer valid.

Term	Definition
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Segment Architecture	A key objective of the FICAM segment architecture is to implement a holistic approach for government-wide identity, credential and access management initiatives that support access to federal IT systems and facilities. By the end of FY 2012, it is intended that Federal Executive agencies will implement a coordinated approach to ICAM across E-Government interactions [Government-to-Government, Government-to-Business, Government-to-Citizen, and Internal Effectiveness and Efficiency (IEE)] at all levels of assurance as defined in OMB M-04-04. The FICAM segment architecture also provides a framework that may be leveraged by other identity management architectural activities within specific communities of interest. The aim is a standards-based approach for all government-wide identity, credential and access management to ensure alignment, clarity, and interoperability.
Symmetric Keys	A shared secret between two or more parties that can be used to maintain a private information link. Since both parties share the same key for encryption and decryption, the keys need to be kept secret. Once somebody else knows the key, it is not safe anymore.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant’s identity.
Universally Unique Identifier (UUID)	The UUID is a unique identifier that can be placed in multiple data fields to uniquely identify the card. For example, the UUID is found in the GUID field of the CHUID, the subjectAltName extension of PIV-I Authentication and PIV-I Card Authentication certificates, and within signed objects on the card (in place of the FASC-N in PIV Cards). The UUID is defined in RFC 4122. On PIV Cards, the GUID may contain a UUID. On PIV-I Cards, the GUID must contain a UUID. The UUID provides a unique numbering scheme. However, the UUID does not require a central organization to manage the namespace.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX C: ACRONYMS

Acronym	Definition
AA	Active Authentication
AD	Accepting Device
AES	Advanced Encryption Standard
AID	Application Identifier
APL	Approved Products List
App	Application
BIO	Biometric
BIO	Biometric
BIO-A	Biometric Attended
C&A	Certification and Accreditation
CA	Certification Authority
CAK	Card Authentication Key
CCTV	Closed Circuit Television
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officers
CMS	Card Management System
CPV	Certificate Path Validation
CRL	Certificate Revocation List
CRUD	Create, Read, Update and Delete
DHS	Department of Homeland Security
DIP	Dual In-line Package
EKU	Extended Key Usage
E-PACS	Enterprise Physical Access Control System
FASC-N	Federal Agency Smart Credential - Number
FBCA	Federal Bridge Certification Authority

Acronym	Definition
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPCON	Force Protection Condition
FPS	Federal Protective Service
FSL	Facility Security Level
FY	Fiscal Year
GSA	General Services Administration
GUID	Global Unique Identifier
HSM	Hardware Security Module
HSPD	Homeland Security Presidential Directive
HTTP	HyperText Transfer Protocol
ICAM	Identity, Credential and Access Management
IdM	Identity Management
IDMS	Identity Management System
IdP	Identity Provider
IEC	International Electrotechnical Commission
IR	Incident Response
ISC	Interagency Security Committee
ISO	International Organization of Standards
IT	Information Technology
JPAS	Joint Personnel Adjudication System
KHz	Kilohertz
LACS	Logical Access Control System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting diode

Acronym	Definition
MA	Maintenance
MHz	Megahertz
MP	Media Protection
NACI	National Agency Check with Inquiries
NFPA	National Fire Prevention Association
NIST	National Institute of Standards and Technology
NPIVP	NIST Personal Identity Verification Program
OCSP	Online Certificate Status Protocol
OID	Object identifier
OMB	Office of Management and Budget
PAC	PACS Access Control
PACS	Physical Access Control System
PAT	PACS Awareness and Training
PAU	PACS Audit and Accountability
PBS	Public Building Service
PCA	PACS Security Assessment and Authorization
PCM	PACS Configuration Management
PCP	PACS Contingency Planning
PDVal	Path Discovery and Validation.
PIA	PACS Identification and Authentication
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKI	Public Key Infrastructure
PLAID	Protocol for Lightweight Authentication of ID
PM	Program Management
POA	Protection of Authenticator

Acronym	Definition
PPE	ACS Physical and Environmental Protection
PPL	PACS Planning
PRA	ACS Risk Assessment
PS	Personnel Security
PSC	PACS System and Communication Protection
PSI	PACS System and Information Integrity
RC	Revocation Check
RF	Radio Frequency
RFC	Request for Comment
SA	System and Services Acquisition
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCVP	Server-based Certificate Validation Protocol
SP	Special Publication
TS	Top Secret
UL	Underwriters Laboratory
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VIS	Visual
VTO	Validation of Trusted Origin

APPENDIX D: DOCUMENT REFERENCES

[Facility Security Levels] *Facility Security Level Determinations for Federal Facilities*
This is a controlled document that is For Official Use Only. Contact Department of Homeland Security Interagency Security Committee for more information.

[FBCA CP] *X.509 Certificate Policy for the Federal Bridge Certificate Authority (FBCA)*
http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[FICAM Roadmap] *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*
http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

[FIPS 140-2] National Institute of Standards and Technology Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules*
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS 180] National Institute of Standards and Technology Federal Information Processing Standards 180, *Secure Hash Standard (SHS)*
http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

[FIPS 200] National Institute of Standards and Technology Federal Information Processing Standards 201, *Minimum Security Requirements for Federal Information and Information Systems*
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[FIPS 201] National Institute of Standards and Technology Federal Information Processing Standards 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[GSA MSO] USAccess Program, *PIV Card Issuer Operations Plan*, General Services Adminstration Managed Services Office
http://www.fws.gov/humancapital/HSPD12/PCI_Operations_Plan%20.pdf

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

[ISO/IEC 7816] International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 7816, *Identification Cards – Integrated Circuit Cards Parts 1-15*
http://www.iso.org/iso/iso_catalogue.htm

[ISO/IEC 14443] International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 14443, *Identification cards -- Contactless integrated circuit cards -- Proximity cards Parts 1-4* *http://www.iso.org/iso/iso_catalogue.htm*

[NIST SP 800-21] National Institute of Standards and Technology Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government* http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

[NIST SP 800-37] National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[NIST SP 800-53] National Institute of Standards and Technology Special Publication 800-53, *Security Controls for Federal Information Systems and Organizations* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[NIST SP 800-57] National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management* http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[NIST SP 800-63-1] National Institute of Standards and Technology Special Publication 800-63-1, *Electronic Authentication Guidance* http://csrc.nist.gov/publications/PubsSPs.html

[NIST SP 800-73] National Institute of Standards and Technology Special Publication 800-73, *Interfaces for Personal Identity Verification (4 Parts)* http://csrc.nist.gov/publications/PubsSPs.html

[NIST SP 800-76] National Institute of Standards and Technology Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification,* http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

[NIST SP 800-78] National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)* http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

[NIST SP 800-79] National Institute of Standards and Technology Special Publication 800-79, *Guidelines for Accreditation of Personal Identity Verification Card Issuers* http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf

[NIST SP 800-85] National Institute of Standards and Technology Special Publication 800-85, *PIV Middleware and PIV Card Application Conformance Test Guidelines* http://csrc.nist.gov/publications/PubsSPs.html

[NIST SP 800-116] National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[NIST SP 800-131] National Institute of Standards and Technology Special Publication 800-131, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[NISTIR 7539] National Institute of Standards and Technology Internal Report *Symmetric Key Injection onto Smart Cards*
http://csrc.nist.gov/publications/nistir/ir7539/nistir-7539-Symmetric_key_injection_final.pdf

[OMB M-04-04] Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

[OMB M-10-15] Office of Management and Budget Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

[OMB M-11-11] Office of Management and Budget Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

[PIV Profile] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Shared Service Providers (SSP) Program
http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf

[PIV-I Profile] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010,
http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf

[RFC 4122] Internet Engineering Task Force Request for Comment 4122, *A Universally Unique Identifier (UUID) URN Namespace*
http://www.ietf.org/rfc/rfc4122.txt

[RFC 5280] Internet Engineering Task Force Request for Comment 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
http://www.ietf.org/rfc/rfc5280.txt

[Security Criteria] *Physical Security Criteria for Federal Facilities*
This is a controlled document that is For Official Use Only. Contact Department of Homeland Security Interagency Security Committee for more information.