Archived Draft Publication

The attached DRAFT document (provided here for historical purposes), released on December 28, 2015, has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-116 Rev. 1**

Title: ***Guidelines for the Use of PIV Credentials in Facility Access***

Publication Date: **June 2018**

- Final Publication: https://doi.org/10.6028/NIST.SP.800-116r1 (which links to https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf).
- Related Information on CSRC:
  Final: https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Draft NIST Special Publication 800-116
Revision 1

A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

Hildegard Ferraiolo
David Cooper
Nabil Ghadiali
Jason Mohler
Vincent Johnson
Steven Brady

This publication is available free of charge

INFORMATION SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-116 Revision 1

A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

Hildegard Ferraiolo
David Cooper
Computer Security Division
Information Technology Laboratory

Nabil Ghadiali
National Gallery of Art
Washington, DC

Jason Mohler
Vincent Johnson
Steven Brady
Electrosoft Services, Inc.
Reston, Virginia

This publication is available free of charge

December 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-116 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-116 Revision 1, 85 pages (December 2015)
CODEN: NSPUE2

This publication is available free of charge

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *December 28, 2015* through *February 1, 2016*

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This recommendation provides a technical guideline to use Personal Identity Verification (PIV) Cards in physical access control systems (PACS); enabling federal agencies to operate as government-wide interoperable enterprises. This recommendation covers the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within [FIPS201].

Keywords

credential; e-authentication; identity assurance level; identity credential; issuance; PACS; PIV authentication mechanisms; PIV cards; PKI; validation

Acknowledgements

The authors of SP 800-116 Revision 1 (Hildegard Ferraiolo and David Cooper of NIST; Nabil Ghadiali of the National Gallery of Art; and Jason Mohler, Vincent Johnson, and Steven Brady of Electrosoft Services, Inc.) wish to thank William MacGregor, Ketan Mehta, and Karen Scarfone for their substantial contribution towards the original version of this publication. The authors also gratefully acknowledge and appreciate the support and contributions by many others in the public and private sectors whose helpful and beneficial comments greatly enhance the utility of this publication. Special thanks to the Interagency Security Committee (ISC), the General Services Administration, the Department of Homeland Security, the Department of Defense, and the Office of Management and Budget for their review and contributions to this document.

Audience

This document is intended for government officials responsible for implementing Homeland Security Presidential Directive-12 (HSPD-12) compliant physical access control systems (PACS). This document will also aid government executives (i.e., decision makers) in evaluating business cases and developing strategies for their departments or agencies. Information in this document is also useful to government contractors and physical security vendors that provide HSPD-12 systems, products, and integration services.

Executive Summary

Prior to Homeland Security Presidential Directive-12 [HSPD-12], the physical access control systems (PACS) deployed in many federal buildings were facility-centric rather than enterprise-centric and utilized proprietary PACS architectures. Therefore, many issued identification (ID) cards operated only with the PACS for which they were issued. The technologies used in these systems typically offered little or no authentication assurance, because the issued ID cards could be easily cloned or counterfeited. Many agencies continue to operate legacy PACS systems. In addition to the lack of interoperability, these PACS technologies present the following challenges:

+ Scalability. Some legacy systems are limited in their capability to process the longer credential numbers necessary for government-wide interoperability.

+ Security. Legacy 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 offer little or no authentication assurance.

+ Validity. Legacy 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.

+ Efficiency. Use of personal identification numbers (PIN), public key infrastructure, and biometrics with some deployed PACS are managed on a site-specific basis. Individuals must enroll PINs, keys, and biometrics at each site. Since PINs, keys, and biometrics are often stored in a site database, they may not be technically interoperable with PACS at other sites.

[HSPD-12] sets a clear goal to improve PACS through the use of government-wide standards. Federal Information Processing Standard 201 [FIPS201] defines characteristics of the identity credential that can be interoperable government-wide. In the context of [HSPD-12], the term *interoperability* means the ability to use any Personal Identity Verification (PIV) Card with any application performing one or more PIV authentication mechanisms. [FIPS201] defines authentication mechanisms at four E-Authentication assurance levels (LITTLE or NO, SOME, HIGH, and VERY HIGH), and standardizes optional credential elements that extend trust in the PIV System to functions beyond authentication. A gap remains, however, between the concepts of authentication assurance levels and their application in many PACS environments. To close this gap, this document:

+ Discusses the different PIV Card capabilities so that the risk-based assessment can be aligned with the appropriate PIV authentication mechanism.

+ Uses the concept of “Controlled, Limited, Exclusion” areas to employ risk-based PIV authentication mechanisms for different areas within a facility.

+ Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations.

+ Recommends to federal agencies an overall strategy for the implementation of PIV authentication mechanisms with agency facility PACS.

Since the areas accessible via different access points within a facility do not all have the same security requirement, the PIV authentication mechanisms selected should be consistent with, and integral to, the overall security requirements of the protected area. A single facility may need multiple authentication mechanisms. Therefore, the designation of "Controlled, Limited, Exclusion" areas, detailed in Section 5.3, is applied to the protected area. Specifically, this document recommends PIV authentication mechanisms for "Controlled, Limited, Exclusion" in terms of authentication factors as shown in Table ES-1. Some agencies may have different names for their security areas, however each agency should establish their criteria to implement authentication consistent with this document.

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

Table ES-1 - Authentication Factors for Security Areas

PIV authentication mechanisms should be implemented in accordance with Table ES-1. Figure ES-1 illustrates the innermost perimeter at which each PIV authentication mechanism may be used based on the authentication assurance level of the mechanism. The combined effect of Table ES-1 and Figure ES-1 determines exactly what mechanisms may be used (see Section 5.3). An exhaustive list of possible uses of PIV authentication mechanisms against protected areas is provided in Appendix D.

[FIPS201] identifies a number of authentication mechanisms supported by mandatory features of PIV Cards. These mechanisms include Authentication using PIV Visual Credentials (VIS), Authentication using the Cardholder Unique Identifier (CHUID), Authentication with the Card Authentication Certificate Credential (PKI-CAK), Authentication Using Off-Card Biometric Comparison (BIO), Attended Authentication Using Off-Card Biometric Comparison (BIO-A), and Authentication with the PIV Authentication Certificate Credential (PKI-AUTH). In addition, PIV Cards may optionally support a number of other authentication mechanisms; these include Authentication with the Symmetric Card Authentication Key (SYM-CAK) and Authentication Using On-Card Biometric Comparison (OCC-AUTH). Access points should not rely solely on an authentication mechanism that requires optional card features as it is not guaranteed that the optional features to be used for authentication are present on all cards. Both the authentication mechanisms that are supported by all PIV Cards and the authentication mechanisms that require optional card capabilities are described in Section 5.

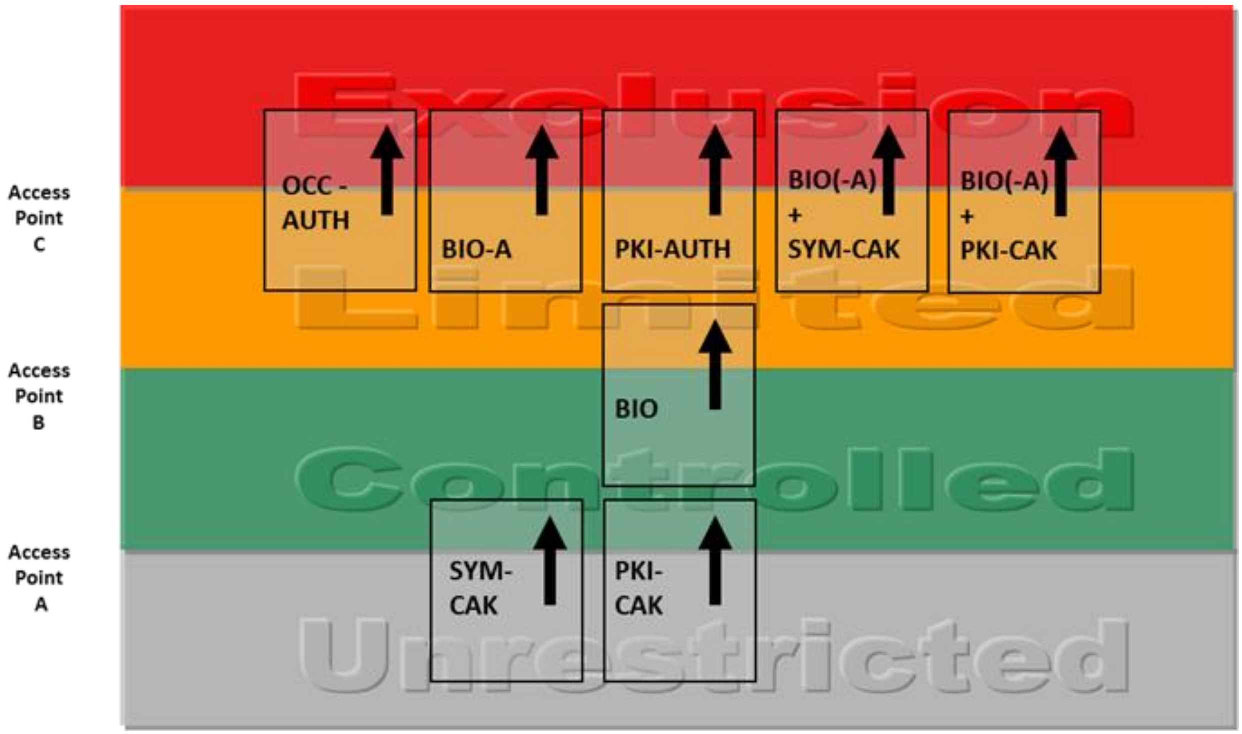

Figure ES- 1: Innermost Use of PIV Authentication Mechanisms

A risk-based migration strategy should be planned and implemented to achieve PIV enabling. This document recommends a model that allows agencies to incrementally PIV-enable access points. The model is defined in terms of maturity levels as follows:

+ 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 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 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 cards are not accepted for access to any areas at this level.

Table of Contents

List of Appendices

List of Figures

List of Tables

1. Introduction

1.1 Background

Homeland Security Presidential Directive-12 [HSPD-12] mandated the establishment of a government-wide standard for identity credentials to improve physical security in federally-controlled facilities.[1] To that end, [HSPD-12] required all government employees and contractors be issued a new identity credential based on [FIPS201], *Personal Identity Verification (PIV) for Federal Employees and Contractors*. Following [FIPS201], this credential is referred to herein as the PIV Card.[2]

[HSPD-12] explicitly requires the use of PIV credentials "in gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems." The PIV Card employs microprocessor-based smart card technology, and is designed to be counterfeit-resistant, tamper-resistant, and interoperable across Federal Government facilities. Additionally, the [FIPS201] standards suite defines the authentication mechanisms as transactions between a PIV Card and a relying party. [FIPS201] does not, however, elaborate on the uses and applications of the PIV Card. This document provides guidelines on the uses of PIV Cards with physical access control systems (PACS).

Legacy PACS technologies deployed in some federal buildings are facility-centric rather than enterprise-centric and often utilize proprietary PACS architectures. Historically, a security advantage was seen in not having the design of the security system published or readily accommodating substitution. For this and other reasons, many legacy PACS are not interoperable. Moreover, lack of agency card technology standards and use of local credential numbering systems are key factors that limit interoperability of legacy PACS across agencies. In other words, an identity credential issued for use with one legacy PACS may not have the capability to be used by another. To enhance security and promote interoperability, it is essential to develop an efficient and cost-effective strategy to migrate legacy PACS to standardized methods as defined in [FIPS201]. The application of cryptographic authentication and integrity methods allows the security of authentication to be improved, the design of authentication to rely on open standards, and the need for secrecy regarding authentication to be concentrated on cryptographic keys.

Full compliance with [HSPD-12], and the use of PIV authentication mechanisms for access to federal facilities and systems as required by [HSPD-12], should be the principal goals of a department or agency implementation plan. Recognizing that implementation will take time, migration goals and plans should be developed to PIV-enable PACS installations, while meeting continuity of operations and resource constraints. Plans may include change management strategies such as:

+ Retrofit or upgrade the existing PACS to use PIV Cards.

---

[1] Federally controlled facilities as defined in Section 1D of OMB Memorandum [M-05-24]

[2] Federal agencies may refer to PIV Cards by other names, for example, "Common Access Cards (CAC)," "LincPass," "identity badges," or "access cards." In this document, all such credentials issued by an accredited PIV Card Issuer are called PIV Cards.

+ Coexistence of PIV-enabled and existing PACS in leased multi-tenant facilities.

1.2 Purpose and Scope

The purpose of this document is to describe a strategy allowing agencies to PIV-enable their PACS, and migrate to government-wide interoperability. Specifically, the document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal Government facilities and assets. With the intent to facilitate and encourage greater use of PIV Cards, this document:

+ Describes the desired characteristics of a target implementation of PIV-enabled PACS.
+ Describes trust and infrastructure challenges that must be overcome to achieve government-wide credential interoperability.
+ Discusses the PIV Card capabilities so that a risk-based assessment can be aligned with the appropriate PIV authentication mechanism.
+ Recommends to federal agencies an overall strategy for the implementation of PIV authentication mechanisms with agency facility PACS.
+ Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations.

As stated above, this document focuses on the use of PIV Cards to gain access to federal buildings and facilities. This document does not address non-PIV authentication mechanisms.

Although the ergonomic design of PACS components is outside the scope of this publication, the 1998 Amendment to Section 508 of the Rehabilitation Act has special relevance to PACS components [SECTION508]. PACS access controls are intended to be unavoidable. [SECTION508] should be considered early during projects that integrate the PIV System with PACS. [SECTION508] should be considered as it applies to enrollment software, smart card and biometric readers, monitoring systems, and access control point sensors and actuators. Note [FIPS201], Section 6.2.1 footnote 31, states “when biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism.” Further information can be found at [SECTION508], in [FIPS201], and in [SP800-76], *Biometric Specifications for Personal Identity Verification*.

Many other aspects of physical access control are outside the scope of this publication. Authorization (i.e., granting permission within a PACS for an identified person to pass access control points) is a critical security function, but is out of scope for the PIV System. Other out-of-scope functions include area protection, intrusion detection, egress, monitoring and tracking (other than at access control points), and enforcement of access control decisions. It is understood that PACS may also be integrated with surveillance systems, fire control systems, evacuation systems, etc., within a facility. This document does not address the integration of PACS with other facility-centric information technology (IT) systems, although it has been written to minimize conflicts during such integration. Therefore, if the integration of the measures outlined in this document creates a life-safety risk, organizations will need to mitigate these risks before applying the measures.

The evaluation of specific PACS architectures or implementations is also outside the scope of this publication, as is the standardization of PACS. The creation of specific migration plans for each agency and facility is also not the intent of this document, although it offers advice on the construction of such plans. Unless normatively referenced, this document is a best practice guideline.

> **Recommendation 1.1:** This document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal Government facilities and assets. Agencies should seek recommendations on PACS architectures, authorization, and facility protection from other sources.

2. Threat Environment

The PIV System is intended to enhance security and trust in identity credentials, but no practical system can guarantee perfect security. This section discusses known technical threats to PIV authentication mechanisms, especially the CHUID authentication mechanism, which has been downgraded in [FIPS201] to indicate that it provides “LITTLE or NO” confidence in the identity of the cardholder because of these threats. Methods of attack are described in general terms, and this is not an exhaustive list of possible attacks. Attackers often succeed by exploiting overlooked or newly introduced vulnerabilities in operational systems.

The PIV System protects the trustworthiness of the PIV Card data objects through PIV 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 Card, the PACS, and the PIV 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.

The factors critical to sustained trust in the PIV System are:

+ The strength of cryptographic operations.
+ The protection of private and secret keys by system components.
+ The successful decryption and/or signature verification of data objects at expected times.
+ The continuous implementation of access rules by the PIV Card.
+ The dependable operation of other system elements in the PIV System and the PACS.

To execute a PIV authentication mechanism, the cardholder presents his or her card to the PACS. The presentation of the PIV Card occurs outside the security perimeter to which access is requested. When the presentation occurs at the outermost perimeter of a facility, the cardholder is in an Unrestricted area, and various technical attacks on PACS are easily carried out. Special security precautions must be taken to ensure protection of these devices at the outermost perimeters of the facility. Even at interior perimeters, the degree of protection provided by enclosing perimeters may be modest when the means of attack can be easily concealed. Possible attack vectors include identifier collisions, revoked PIV Cards, visual counterfeiting, skimming, sniffing, social engineering, electronic cloning, and electronic counterfeiting. These methods of attack, as well as others, are discussed below.

2.1 Identifier Collisions

By definition, a unique identifier for a PIV Card is a data artifact with a fixed value unique to one particular PIV Card. PIV Card Issuers (PCIs) create unique identifiers during the card issuance process. The presence of unique identifiers allows a PIV Card to be uniquely identified by a relying system, such as a PACS. If the unique identifier is ever truncated, compressed, hashed, or modified, information could be lost. If information is lost from the unique identifier before it is compared against access control list (ACL) entries, multiple cards may generate the same reduced identifier. This is called an *identifier collision*. A collision means that multiple PIV Cards will appear to belong to the same person, and will all be granted the same access privileges.

The PIV Card mitigates the risk of collision by defining a unique FASC-N Identifier for the purposes of physical access control decisions. To prevent collisions, all access control decisions based on the FASC-N should be made by comparing the 14 decimal digit FASC-N Identifier, and optionally the values of additional FASC-N fields, against the ACL entries. [FIPS201] added the mandatory Card UUID, which is also a unique identifier that can be used reliably in access control decisions. See Section 5.4 for PIV identifiers.

2.2 Revoked PIV Cards

PIV Cards may be revoked for a number of reasons, including a lost or stolen card. A revoked PIV Card could continue to open doors with the CHUID authentication mechanism long after the card has been revoked. As described in [FIPS201], the check for revocation should be performed by a status check, using either the Online Certificate Status Protocol (OCSP) or certificate revocation lists (CRL), on the PIV Authentication certificate or the Card Authentication certificate. Credential validation (see Section 5.5) is required by [FIPS201] for all PIV authentication mechanisms, however, validation of the CHUID and biometric credentials do not include a revocation check. If a PIV Card is reported as lost and then revoked by the issuer, a PACS relying on the CHUID authentication mechanism will continue to accept the CHUID until the user is de-authorized in each of those systems. If a PACS caches the status of PIV Cards, the cached status of a revoked PIV Card will remain "valid" until the cache is refreshed. The process for PACS de-authorization is not required or defined by [FIPS201], raising the possibility that online credential validation may not be implemented, or not effectively implemented, where the CHUID authentication mechanism is employed.

The PIV System mitigates the risk of use of a misappropriated PIV Card (which has been successfully reported and revoked) through the process of credential validation. Section 5.5 of [FIPS201] states that "the presence of a valid, unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not revoked." In the CHUID authentication mechanism, only the CHUID data object is read from the PIV Card, and a reader cannot check the status of a PIV Authentication certificate on the basis of the CHUID alone. Therefore, it is recommended that path validation of the PIV Authentication certificate or the Card Authentication certificate be done at PIV registration, and periodically repeated by the PACS as long as registration is maintained. Implementation methods are further discussed in Section 5.5 and Section 5.6.

2.3 Visual Counterfeiting

PIV Cards used in the VIS authentication mechanism are visually inspected by a security guard. A visual counterfeit mimics the appearance, but not the electronic behavior, of an actual PIV Card. A PIV replica may be created by color photocopying or graphic illustration methods and color printing to blank stock. Because of the required presence of one or more security features on the PIV Card, a visual counterfeit is unlikely to pass close examination, provided guards are trained to recognize security features. However, ID cards may receive only cursory examination when used as "flash passes."

> *The PIV Card mitigates the risk of visual counterfeiting through its capability for rapid electronic authentication, and to a lesser degree, by the presence of one or more security features on the surface of the card. Given the ready availability of high-quality scanners, graphic editing software, card stock, and smart card printers, electronic verification is strongly recommended, either in place of the VIS authentication mechanism or in combination with it. (Note that [FIPS201] downgraded the VIS Authentication mechanism to indicate that it provides "LITTLE or NO" confidence in the identity of the cardholder.)*

2.4 Skimming

A contactless PIV Card reader with a sensitive antenna can be concealed in a briefcase, and is capable of reading [ISO/IEC 14443] contactless smart cards like the PIV Card at a distance of at least 25 cm, as demonstrated in [SKIMMER]. The range of a skimmer is limited primarily by the requirement for the skimmer to supply power to the PIV Card by inductive coupling. A concealed skimmer could immediately obtain the free-read data from the PIV Card through the contactless interface. [FIPS201] introduced the concept of an optional virtual contact interface (VCI), which allows all data on the PIV Card that is not protected by a PIN to be read once this interface is established. [SP 800-73], *Interfaces for Personal Identity Verification*, specifies an optional pairing code that can be used to authenticate the card reader to a PIV Card before the card establishes a VCI session. If agencies deploy PIV Cards that support establishing a VCI without requiring the submission of a pairing code, all data on these cards that is not protected by a PIN is vulnerable to skimming.

> *The PIV Card mitigates the risk of skimming by implementing access rules that prevent the release of biometric and other data over the contactless interface when a VCI has not been established, by requiring the use of a pairing code in order to establish a VCI. The risk of skimming can also be mitigated by employing shielding techniques that positively deactivate the PIV Card when not in use. The electromagnetically opaque holder mentioned in Section 2.11 of [FIPS201] is one such technique.*

2.5 Sniffing

When a PIV Card is presented to a contactless reader at an access point, the reader supplies power to the PIV Card through inductive coupling and a series of messages is exchanged between the PIV Card and reader using radio frequency (RF) communications. A sniffer is a passive receiver that does not supply power to the smart card. A sniffer can operate at greater distance than a skimmer (sniffing at a distance of about 10 m has been reported), because a legitimate reader powers the PIV Card at the nominal distance of a few centimeters, while the sniffer's RF receiver is farther away. Potentially, a sniffer could capture the entire message transaction between the contactless reader and the PIV Card.

> *The PIV Card mitigates the risk of sniffing by the same access rules that prevent the release of biometric and other data over the contactless interface. The CHUID can be sniffed, however, when used over a contactless interface. Shielding techniques that positively deactivate a PIV Card when not in use cannot mitigate the risk of sniffing, because a PIV Card must be activated to perform a legitimate authentication transaction.*

When a PIV Card that supports secure messaging[3] communicates with a contactless card reader, the card reader can leverage the secure channel, which would protect data objects being read from the risk of a sniffing attack.

2.6 Social Engineering

If an attacker persuaded the cardholder to give them possession of the PIV Card, the attacker could quickly copy all of the information that was not protected by the PIN. An attacker could also attempt a remote attack similar to well-known phishing attacks by creating a web page that asks the subject to “insert PIV Card and enter PIN” for an apparently legitimate purpose. If the cardholder complies, under some assumptions the attacker could capture the cardholder’s PIN and all of the PIV data objects.

The PIV Card mitigates the risk of social engineering attacks by blocking the release of all private and secret keys, and by requiring two-factor authentication (PIV Card and PIN) to perform cryptographic operations with the PIV Authentication key. Moreover, the PIV Card is blocked upon exceeding the allocated number of bad PIN tries. Additional technical and procedural controls may be needed to counter PIV phishing.

2.7 Electronic Cloning

If an attacker has successfully conducted a skimming, sniffing, or social engineering attack, he or she possesses verbatim copies of some of the data objects from an issued PIV Card. The objects that are signed (e.g., the certificates and CHUID) retain their signatures, and the signatures are valid if the original card is valid. The attacks described, however, cannot copy the private or secret keys needed for cryptographic authentication methods. The attacker is thus able to create a partial clone of the PIV Card that would succeed in a CHUID authentication, but is not able to create a clone that would succeed in the PKI-CAK or PKI-AUTH authentication mechanisms.

The PIV Card mitigates the risk of electronic cloning by providing alternative authentication mechanisms. It is strongly recommended that agencies use an authentication mechanism other than the CHUID authentication mechanism (e.g., PKI-CAK), since [FIPS201] deprecates the use of the CHUID authentication mechanism as it provides ‘LITTLE or NO’ confidence in the identity of the cardholder. Relying systems currently implementing the CHUID authentication mechanism should phase out the mechanism as soon as possible.[4] See Section 5.3.1 for recommendations on a transition strategy.

[3] Secure messaging is an optional mechanism specified in [SP 800-73] that provides confidentiality and integrity protection for the card commands that are sent to the card as well as for the responses received from the PIV Card.

[4] Using the transition strategies described in Section 5.3.1 will result in use of the CHUID authentication mechanism being gradually decreased until it is entirely eliminated by September 2019 once all valid PIV Cards issued without Card Authentication certificates have completed their five-year life cycle and have been replaced with cards containing Card Authentication certificates.

2.8 Electronic Counterfeiting

An attacker could construct a battery-powered, microprocessor-based device that emulates a PIV Card for purposes of the CHUID authentication mechanism. The attacker could program the microprocessor to generate and test CHUIDs repetitively against a PACS reader, changing the FASC-N credential identifier on each trial. This approach would not require prior capture of a valid CHUID, but since the counterfeit CHUIDs would not possess valid issuer signatures, a successful exploit depends on the absence of signature verification in the CHUID processing done by the reader.

The PIV Card mitigates the risk of electronic counterfeiting by storing a CHUID with a digital signature field. Electronic counterfeiting will be extremely difficult if CHUID signature verification is performed as required in [FIPS201]. Moreover, since many CHUIDs may be presented while an attacker probes for a valid CHUID, the PACS should employ methods to detect, alarm, and block repeated unsuccessful CHUID presentations.

2.9 Other Threats

The PIV and PACS systems are complex, and this brief discussion has focused on properties of the PIV Card. A number of other attack vectors have not been discussed in detail, including sophisticated technical attacks against the integrity of the PIV Card, PIV System, or PACS components, and cryptanalysis of the PIV cryptographic algorithms. While the impact of successful attacks such as these could be moderate to high, the probability of success is believed to be extremely low.

Recommendation 2.1: *This section emphasizes the technical risks associated with the legacy CHUID authentication mechanism. If the CHUID authentication mechanism is used without restriction, operational risk increases as the value of targets and the availability of cloning and counterfeiting tools increase.* [FIPS201] *deprecates the use of the CHUID authentication mechanism since it provides 'LITTLE or NO' confidence in the identity of the cardholder, and so relying systems should phase out use of this authentication mechanism as soon as possible. NIST recommends transitioning away from the CHUID authentication mechanism using the strategy described in Section 5.3.1.*

3. Limitations of Legacy Physical Access Control Systems

[FIPS201] and its supporting special publications impose specific requirements on PACS interfaces with PIV Card and PIV System. These requirements will present technical challenges in migrating to PIV Card use in the areas of cardholder identification, card-to-reader interface, and authentication protocol. The following sections explore how [FIPS201] requirements differ from the capabilities of PACS that are not PIV-enabled.

3.1 Cardholder Identification

Legacy PACS use cards with data formats that are often proprietary to the specific enterprise. Many of the legacy PACS use an ID number based on a 26-bit standard, which is comprised of an 8-bit site code and a 16-bit unique card ID number with 2 bits assigned to parity (the parity bits add confidence that the data transmission has no errors). The 8-bit site code accommodates 256 unique sites and the 16-bit card ID number accommodates 65 536 unique users for that site. Larger ID numbers are used by some legacy systems but they are not necessarily interoperable.

A PACS based on the 26-bit format is deployed as a standalone solution at a dedicated site. Typically, these solutions are managed locally, and an individual with an access card for one site cannot use the same card at a second site and must obtain a second card. [FIPS201] changes this dynamic because the credential is issued through a separate process instead of as part of the PACS deployment. Legacy PACS need to be upgraded or re-provisioned to support at least a 14-decimal-digit FASC-N Identifier or a 16-byte Card UUID (see Appendix C).

3.2 Door Reader Interface

PACS readers come in varying configurations and offer multiple interface options for the card and the controller. [FIPS201] standardizes the use of the [ISO/IEC 14443] interface for the contactless reader to card communication. Note that the card reader may require additional conformance testing for federal acquisition. An authority for such conformance testing is the General Services Administration (GSA) FIPS 201 Evaluation Program [FIPS 201 EP], which defines tests and maintains a list of approved products. Not all existing PACS use this interface, so some agencies may have to plan to migrate from their legacy environment to the [ISO/IEC 14443] conformant interface. Alternatively, an agency may use the PIV Card's contact interface based on [ISO/IEC 7816].

The interface from the door reader to the controller also comes in different configurations. [FIPS201] does not specify which protocols can be used for this interface, as long as 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 [FIPS201] defines data elements that 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 or the full 16-byte Card UUID will be supported. Note that any change to this interface may also necessitate changes to the physical wiring and cabling infrastructures.

3.3 Authentication Capability

Legacy PACS readers use proximity or magnetic stripe technology to interface with identity cards and use proprietary protocols to communicate data. Some of these proprietary protocols employ cryptography, but their use is limited to the local site. [FIPS201] specifies identity credentials that can be used for a new generation of identity management technology for building access. [FIPS201] and its supporting special publications define the credential data model and the card-to-reader interface, and also provide requirements for implementing the digital certificates.

[FIPS201] added a standardized contactless and contact interface, PIN, biometric fingerprints, optional iris images, and cryptography to the card that could be used to attain a higher level of identity authentication assurance. The capability to perform bi-directional data communication is fundamental to the deployment of secure building access. Adding cryptography to the cards permits agencies to validate the data objects on the card and authenticate the cardholder. Adding credential expiration and credential validation requirements also strengthens access control decisions. At the same time, [FIPS201] provided the opportunity to migrate building access systems from LITTLE or NO confidence levels to VERY HIGH confidence levels. Legacy PACS may need upgrades to take advantage of these features and functions, in coordination with the following guidelines and authorities:

+ [FIPS201] assurance levels.
+ The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard [ISC-RMP].
+ OMB M-04-04, E-Authentication Guidance for Federal Agencies [M-04-04].

[FIPS201] redefines the requirements for building access in a fundamental way: instead of each facility issuing an access card solely for that facility's PACS architecture, a facility relies on the PIV Card that was issued by the same, or a different, agency certified by the Federal Government. The facility still has control over the user's access privileges, but the technology has been standardized to optimize interagency interoperability and the credential has been issued to the user as part of the [FIPS201] identity management process.

3.4 Wiring

Selecting a particular reader type and its interface with the controller requires careful attention to wiring. Existing wiring should be assessed for its ability to meet the requirements of new readers and controllers and take into consideration performance. The existing wiring may be a limiting factor due to its capacity to transmit data and original specifications. Many recently installed systems use higher bandwidth cables, which are typically sufficient for a PIV-based access control system. In some environments, advanced signaling methods operating at higher speeds with lower signal-to-noise margins can necessitate upgrades to the wiring.

3.5 Software Upgrades

Vendors may be able to upgrade their PACS software to minimize the hardware changes needed for a legacy PACS to accept PIV Cards. Software or firmware upgrades to controllers or door readers may be available to agencies. PACS suppliers should be asked if software or firmware upgrades supporting PIV Cards are a possibility. If available, the agency should ensure that the software upgrade will have no adverse effect on the PACS system or any interconnected systems.

3.6 Legacy PACS Cards and PIV Card Differences

The list below compares the basic differences in the technology offerings between the legacy PACS cards and the PIV Card.

+ Some legacy PACS use site-specific card technology, with the result that a card cannot be used at sites with incompatible PACS. For example, a magnetic stripe card cannot be used at a proximity card site, and a magnetic stripe card from one vendor cannot be used at a site with magnetic stripe equipment from another vendor.
+ Legacy PACS readers can read an identifying number from a card, but in most cases they do not perform a cryptographic challenge/response exchange. Many non-PIV PACS cards can be copied easily.
+ When two sites use compatible legacy card technology, the risk of duplicate site identifiers for cards is always present. Without government-wide coordination of identifiers, the same identifier could be used on multiple cards at different sites.
+ To achieve government-wide coordination of cardholder identifiers, enough identifiers must be available for all government-issued credentials. Many legacy PACS have a limit on the number of sites (256) and the number of users per site (65 536) that is too small for government-wide use and can lead to the same identifiers being issued to different individuals.
+ Legacy PACS control expiration of credentials through an expiration date stored in a site database, whereas with PIV Cards expiration dates can be obtained from the cards themselves. There is no simple way to synchronize the expiration of credentials for a federal employee or contractor with access to multiple sites unless all sites are tied into a centralized enterprise-wide PACS (e-PACS).
+ Use of PINs, public key infrastructure, and biometrics with legacy PACS is managed on a site-specific basis at the PACS server. Individuals must enroll PINs, keys, or biometrics at each site. Since PINs, keys, and biometrics are often stored in a site database, they may not be technically interoperable with the requirements of other sites.

[FIPS201]-conformant PIV-enabled PACS eliminate or substantially reduce each of these limitations, relative to legacy PACS installations.

4. The PIV Vision

[HSPD-12] begins, "Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated." [HSPD-12] continues, in Paragraph 4, "As promptly as possible… the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities."

[HSPD-12] directs federal departments and agencies to improve identification and authentication of federal employees and contractors requiring access to federally controlled facilities through the widespread application of [FIPS201]. The standard defines the characteristics of the PIV System. This section describes the benefits that are expected from the use of the PIV System, to the maximum extent practicable, for authenticating people to PACS managed by the United States Government.

This section focuses on the benefits of electronic verification and direct integration with an electronic PACS. The [FIPS201] authentication mechanisms that can be performed electronically are PKI-CAK, SYM-CAK, BIO, BIO-A, PKI-AUTH and OCC-AUTH. The VIS authentication mechanism cannot be verified electronically and provides "LITTLE to NO" confidence in the identity of the cardholder. It should not be used when another mechanism is practical.

4.1 Interoperability

In this publication, the term interoperability means the ability of a PACS to use any PIV Card issued by any agency to authenticate the cardholder by performing one or more PIV authentication mechanisms. The data objects and keys placed on a PIV Card during issuance use specific cryptographic algorithms selected from the acceptable algorithms in [SP800-78], *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. A PACS application can interrogate the card to learn which algorithms are used. To attain full interoperability, a relying PACS application will need to support all acceptable algorithms, key lengths, and key material that could be presented, either by a PIV Card or by the PIV infrastructure.

The interoperability goal of a PIV-enabled PACS can be stated:

1. Any PIV Card can provide proof of identity to any electronic PACS (access is granted only if the identity is so authorized).

2. After a successful authentication, the authentication mechanism provides the cardholder's authenticated identity (see Section 5.4) to the relying party.

To achieve interoperability, the PACS should at least observe the following conditions:

+ If the PKI-CAK authentication mechanism is performed by a PACS application, the PACS should support all of the asymmetric algorithms permitted for the asymmetric CAK, as specified in Table 3-1 of [SP800-78], i.e., RSA 2048 and ECDSA P-256, and the PACS should accept all valid Card Authentication certificates.

+ If the PKI-AUTH authentication mechanism is performed by a PACS, the accepted algorithms will be the same as PKI-CAK, but the PACS will accept only PIV Authentication certificates and require PIN entry.

+ If authentication using off-card biometric comparison is performed (BIO or BIO-A), the PACS should support all of the signature algorithms and key sizes permitted by Table 3-2 of [SP800-78].

+ PINs required for PIV authentication mechanisms are strings of six to eight decimal digits. For PKI-AUTH, BIO, and BIO-A authentication mechanisms, a PIN entry device must acquire the PIN from the cardholder and present it to the PIV Card for activation.

+ The PACS supports at least one PIV authentication mechanism that is supported by all PIV Cards. For example, a PACS may use the PKI-AUTH authentication mechanism to authenticate all cardholders. Alternatively, the PACS may use the BIO authentication mechanism to authenticate most cardholders, but use the PKI-AUTH authentication mechanism to authenticate those cardholders from whom fingerprints could not be collected.

The PIMM presented in Section 7.6 can be used to measure progress towards the interoperability goal. When PIV implementation is complete, all installed PACS readers are required to be from the approved products list of the [FIPS 201 EP], and each will be capable of one or more PIV authentication mechanism, such that each PACS reader will be capable of authenticating any PIV cardholder using a PIV authentication mechanism, including those with PIV Cards that do not implement any of the optional card capabilities.

The ability of a PIV Card and cardholder to authenticate at a reader does not mean they will be granted access—it means only that the cardholder has been identified, with the assurance level of the authentication mechanism employed, by the reader. A cardholder must authenticate and be authorized to be granted access. Authorization policies and mechanisms are outside the scope of [FIPS201].

Recommendation 4.1: To obtain the full benefit of PIV interoperability, PIV project managers should ensure that relying systems have the capability to use all cryptographic algorithms that apply to the authentication mechanism(s) performed. Departments and agencies are required to procure and deploy [HSPD-12] products from the [FIPS 201 EP] Approved Products List where applicable,[5] and can use the PIMM presented in Section 7 to measure progress toward the goal of interoperability.

[5] The Evaluation Program directly supports the acquisition process for implementing HSPD-12. OMB Memorandum [M-06-18] directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability.

4.2 Qualities of the Complete Implementation

The PIV System implementation will be complete when the following qualities have been achieved.

1. PIV authentication mechanisms are used wherever they are applicable, in accordance with [HSPD-12] and [FIPS201].
2. Electronic authentication (as opposed to VIS authentication) is the common practice.
3. Electronic validation of the PIV Card is done at or near the time of authentication.[6]
4. All PIV Card access control decisions are made by comparing the selected PIV identifier to access control list (ACL) entries. See Section 5.4 and Appendix C for details.
5. PIV authentication mechanisms are applied based on the impact assessed for the area.
6. Cryptographic and biometric authentications are applied widely in moderate- and high-impact [FIPS199] areas.
7. Agencies exhibit reciprocal trust in the process assurance of PCIs.
8. Both new and upgraded PACS applications accept PIV Cards as proof of identity for user registration/provisioning, user authentication, or both.
9. Authentication transactions have been optimized; especially at access points that only require one-factor authentication and that have high throughput requirements.

[HSPD-12] declares its goals are to "…enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy," and states specific criteria to be met by the implementation:

> "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

The Federal Information Security Modernization Act [FISMA] mandates the standardization of security management practices for information systems. The foundational concept of [FISMA] security management is impact assessment and impact-based planning ("impact" being a generalization of "exposure" to monetary and non-monetary damage). [FIPS201] follows this methodology by implementing authentication mechanisms at four E-Authentication confidence

[6] In some cases, validating PIV Cards at the time of authentication is not practical. In these instances, it is possible to maintain a local cache of validated PIV Cards, provided that the cache is updated regularly.

levels (LITTLE or NO, SOME, HIGH, and VERY HIGH). A gap remains, however, between the concepts of impact and confidence levels. This document suggests a method to close this gap through the use of risk-based planning and the establishment of "Controlled, Limited, Exclusion" boundaries for appropriately protecting facility assets or resources.

Interoperability of PIV Cards and PIV authentication mechanisms is not a guaranteed consequence of the technical standard. Government-wide interoperability also requires federal agencies to exhibit reciprocal trust in the processes of PCIs and the service quality of the PIV Card validation and revocation infrastructure. Reciprocal trust is enabled by the requirements for the PIV issuance process stated in [FIPS201], and supported by the accreditation process methodology described in [SP800-79], *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*. Trust is built when the technical standard is thorough, unambiguous, and grounded in practical requirements; when the conformance and audit processes are documented and uniformly practiced; and when positive PIV System audit results are available to the community of relying parties.

> **Recommendation 4.2:** Once all appropriate authentication mechanisms are satisfied, access control decisions are made by comparing the selected PIV identifier (see Section 5.4) against the ACL entries.

> **Recommendation 4.3:** As agencies develop risk-based implementation plans, they will create and evolve plans for PIV Card issuance and application integration. They might consider which of the nine qualities are most relevant to agency goals and priorities, and derive further project objectives, metrics, and milestones from those qualities. They should also consider the relation of [HSPD-12] to [FISMA] requirements, and examine the potential for cost tradeoffs where PIV can replace more expensive authentication methods.

4.3 Benefits of the Complete Implementation

The complete PIV System will be an identity infrastructure that is attractive to federal agencies, application owners, and contractors because of these benefits:

+ Enhanced trust. PIV Cards will be issued in accordance with standardized, audited processes, which will exceed the best practice level for low- and moderate-impact applications today, and equal best practice reached for high-impact applications.

+ Resistance to misuse and cloning. Electronic validation of the PIV Card, using digital signatures, makes it tamper-resistant. Cryptographic challenge/response protocols make the PIV Card counterfeit-resistant. Biometric authentication makes the PIV Card non-transferable.

+ Status and revocation. PIV Card Issuer process assurance will extend beyond the issuance action to PIV Card validation and revocation services. These services are required elements of the PIV infrastructure, and will be implemented, monitored, and audited with the same care as the PIV issuance process.

+ Standard identity infrastructure. Application developers will assume, as a default, that registration and authentication will use a PIV Card identity, reducing development cost, registration time, and the application learning curve for new subjects.

+ Integrated system. PACS will be fully integrated with other PIV system components that perform provisioning, enrollment, and finalization.

+ Fewer passwords. A single PIV Card provides a small set of authentication methods that are applicable to many applications and in many contexts. This means significantly fewer passwords and account enrollments.

Each of these points both enhances security and creates efficiency of operation. Reducing passwords and password helpdesk calls, reusing identity enrollment across multiple applications, collapsing redundant status and revocation processes (separate processes for revocation on termination across multiple applications), and replacing authentication credentials that are easily shared or transferred will reduce operating costs borne by federal agencies. Availability of a skilled workforce familiar with the standardized PIV identity infrastructure, implementation of PIV issuance with a standardized identity verification methodology, the existence of high-availability online services for PIV Card status and validation, and pre-enrollment in a graduated, multi-factor authentication scheme all enhance security current practice in many applications. The replacement of password (single-factor) authentication with PIV Card (up to three-factor) authentication is a fundamental advance in authentication assurance.

Biometric enrollment is mandatory for the PIV Card. Every government employee and contractor who can provide at least one fingerprint image of acceptable quality will be pre-enrolled for biometric authentication.[7] Iris images may also be collected from a PIV applicant. In the complete PIV System, the marginal cost for biometric enrollment to the application owner, relative to other authentication mechanisms, is near zero, enabling more applications to gain the benefits of biometric authentication.

Recommendation 4.4: Operational metrics should be designed to measure actual benefits over the operational lifetime of the PIV System. They may be derived by formulating each of the expected benefits above as a service quality metric, e.g., for "integrated system," service quality could be defined as the percentage of PACS registrations that are performed automatically by provisioning from the PIV issuance system.

4.4 Infrastructure Requirements

The qualities and benefits of the complete PIV System can only be achieved if its implementation is supported by general advances in infrastructure used by PACS. The following areas have significant influence on the rate at which the complete PIV System integration can be achieved by PACS, and should therefore be supported by PACS upgrades and new PACS procurements:

[7] Section 6.2.1 of [FIPS201] states "When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism." Also, see Sections 3.2, 3.3 and 3.4 of [SP800-76].

1. Fast, two-way communication between readers and controllers or panels.
2. Fast network communication between readers, controllers, or panels and PIV status and validation services.

Point (1) allows readers to access cached validation status during access control transactions. Point (2) allows controllers or panels to cache the validation status. Points (1) and (2) combined could allow readers direct access to PIV status and validation services, if needed.

> **Recommendation 4.5**: Maximum benefit will be obtained from the PIV System when it is adequately supported by infrastructure. Infrastructure upgrades may be justified, especially to improve communication between PACS system elements (e.g., support two-way communication).

5. PIV Authentication Mechanisms

This section provides a discussion of the PIV authentication mechanisms and their application in PACS environments. PIV authentication mechanisms offer a range of security measures (of different throughputs) that can be applied in a PACS environment. This section first describes a measurement scale for authentication assurance relevant to PACS. Then it discusses security offerings of each PIV authentication mechanism and their combinatory effects on identity authentication. Finally, this section provides recommendations on the use of PIV authentication mechanisms in a PACS environment.

5.1 Authentication Factors

One of the functions of the PACS application is to verify the identity of the cardholder presenting a PIV Card. The PACS application may perform one or more authentication mechanisms using the PIV Card to establish confidence in the identity of the cardholder. The authentication of an identity is based on the verification of one, two, or three of these 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 or irises by a cardholder.

The PIV authentication mechanisms operate in several different ways as defined in [FIPS201], [SP800-73], and [SP800-76]. For example, the CHUID data object may be read from the PIV Card and its signature verified (CHUID authentication mechanism). A private key on the PIV Card may be used to sign a challenge (PKI-CAK and PKI-AUTH authentication mechanisms). A valid biometric from the card may be compared against a live scan (BIO, BIO-A, and OCC-AUTH authentication mechanisms).

PIV authentication mechanisms may be performed by different entities, referred to here as verifiers. For example, a PACS application verifies the signature on a data object, the signing of a challenge using a private key, or the comparison of biometric templates. The verifier can also be the PIV Card itself. For example, the PIV Card verifies the PIN or the fingerprint (in the case of OCC). The PACS should only trust the PIN verification by the PIV Card if it has verified that the card is a valid PIV Card.

The confidence in the cardholder's identity increases with the number of factors used to authenticate the PIV Card. Table 5-1 and Table 5-2 provide lists of PIV authentication mechanisms and their authentication factors when used on the contact and contactless interfaces, respectively. Note that there are a few authentication mechanisms that are recognized as unique combinations in these tables. This is due to the fact that neither BIO(-A) nor PKI-CAK nor SYM-CAK individually provide the "something you know" authentication factor, but when BIO(-A) is used together with either PKI-CAK or SYM-CAK, PIN verification provides this factor since the card has been verified to be a valid PIV Card. Many different combinations of the PIV authentication mechanisms are possible and an exhaustive list of combinations is provided in Appendix D.

Note that an authentication mechanism is not considered to provide any factors of authentication if the authentication is not successful. For example, in the case of the PKI-AUTH and PKI-CAK authentication mechanisms, if the PACS application is unable to validate the authentication certificate from the presented card or does not receive a response to its challenge that can be verified using the public key in the certificate, then the PACS application cannot count the authentication attempt towards meeting the requirements for granting access to an area.[8]

As noted in Section 4.1, in order to achieve interoperability, each access point in a PACS needs to support at least one PIV authentication mechanism that is supported by all PIV Cards. In Table 5-1 and Table 5-2, the authentication mechanisms represented in **bold** are the authentication mechanisms that can be implemented using only features that are mandatory for PIV Cards issued under FIPS 201-2. Of these authentication mechanisms, however, only PKI-AUTH (when used in conjunction with the PIV Card PIN) and CHUID + VIS are currently supported by all PIV Cards. PKI-CAK will be supported by all valid PIV Cards after August 2019, once all PIV Cards (issued under FIPS 201-1) without Card Authentication certificates have expired.

While the CHUID + VIS authentication mechanism does provide interoperability its use is deprecated, since it provides “LITTLE or NO” confidence in the identity of the cardholder. However, CHUID + VIS may be used until September 2019 as part of a strategy to migrate to a stronger authentication mechanism, such as PKI-CAK, as described in Section 5.3.1.

While the Cardholder Fingerprints data object needed for the BIO and BIO-A authentication mechanisms is mandatory, it may not be possible to collect usable fingerprints from some cardholders. So, PACS that use BIO(-A) to authenticate cardholders should be prepared to use an alternative authentication mechanism with PIV Cards that have no minutiae in the Cardholder Fingerprints data object (see Section 4.4.3 of [SP800-76]). PKI-AUTH is the recommended alternate authentication mechanism.

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)
CHUID + VIS	x			1
BIO			x	1
SYM-CAK	x			1
PKI-CAK	x			1
BIO-A	x		x	2
PKI-AUTH	x	x[**]	x[***]	2
OCC-AUTH	x		x	2

[8] If the authentication mechanism fails for a reason that indicates that the presented card is not valid, then the failed authentication attempt should raise an alarm.

[**] If the PIN is used to satisfy the security condition for use, then the PKI-AUTH authentication mechanism provides the following 2 factors of authentication: (i) something you have (i.e., the card) and (ii) something you know (i.e., the PIN).

[***] If OCC is used to satisfy the security condition for use, then the PKI-AUTH authentication mechanism provides the following 2 factors of authentication: (i) something you have (i.e., the card) and (ii) something you are (i.e., on-card biometric match). Note that OCC is an optional PIV Card feature. As result, PKI-AUTH does not support interagency interoperability when OCC is used to satisfy the security condition of use. Use of the PIV Card PIN, on the other hand, enables the PKI-AUTH authentication mechanism to achieve interagency interoperability.

SYM-CAK + BIO(-A)	x	x	x	3
PKI-CAK + BIO(-A)	x	x	x	3

Table 5-1 - PIV Authentication Mechanisms on the Contact Interface

Table 5-2 provides a list of PIV Authentication mechanisms that are appropriate for use over the contactless interface. Note that there are some authentication mechanisms listed in Table 5-1 for use over the contact interface that are not listed in Table 5-2. The authentication mechanisms that are not listed in Table 5-2 are authentication mechanisms that would require the use of secure messaging when performed over the contactless interface, but that do not require the use of secure messaging when performed over the contact interface. Since support for secure messaging is optional, these authentication mechanisms do not support interagency interoperability when performed over the contactless interface, but (with the exception of SYM-CAK + BIO(-A)) do support interagency interoperability when performed over the contact interface, and so use of the contact interface is preferable for these authentication mechanisms.

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)
CHUID + VIS	x			1
SYM-CAK	x			1
PKI-CAK	x			1
OCC-AUTH	x		x	2

Table 5-2 - PIV Authentication Mechanisms on the Contactless Interface

Each of the PIV authentication mechanisms is described further in the following sections.

5.1.1 Authentication using PIV Visual Credentials (VIS)

Visual authentication entails inspection of the topographical features on the front and back of the PIV Card. The human guard checks to see that the PIV 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 the training, skill, and diligence of the guard (to match the face in spite of changes in physical appearance – beard, mustache, hair coloring, eye glasses, etc.) – counterfeit IDs can pass visual inspections easily. Digital scanners, printers, and image editing software have made counterfeiting easier. Moreover, the visual verification of security features does not scale well across agencies since each agency may implement different security features. For these reasons, [FIPS201] has downgraded this authentication mechanism to indicate that it provides "LITTLE or NO" confidence in the identity of the cardholder.

5.1.2 Authentication using the Cardholder Unique Identifier (CHUID)

The CHUID, as defined in [FIPS201] and [TIG SEPACS], is one of the mandatory data objects on PIV Cards. The CHUID contains two data elements, the FASC-N and the Card UUID, that uniquely identify the PIV Card. The CHUID also uniquely identifies an individual since each PIV Card is issued to an individual. The CHUID data object is signed by the issuer so alterations or modifications to a CHUID can be detected. An expired CHUID, failure of signature verification or path validation results in a failed authentication attempt that does not admit a cardholder for access.

The CHUID is a free read object on the PIV Card; and thus it can be read or cloned easily. Because of the risk of cloning, the CHUID authentication mechanism provides "LITTLE or NO" confidence in the identity of the cardholder. For this reason, the CHUID authentication mechanism has been deprecated in [FIPS201] and is expected to be removed in a future revision of the standard.

> **Recommendation 5.1:** Agencies currently implementing the CHUID authentication mechanism are highly encouraged to transition to another PIV authentication mechanism as soon as possible (see Section 5.3.1 for a suggested migration strategy).

5.1.3 Authentication with the Card Authentication Certificate (PKI-CAK)

The asymmetric Card Authentication key, as defined in [FIPS201], is one of two mandatory asymmetric authentication keys present on the PIV Card. As the name implies, the purpose of the PKI-CAK authentication mechanism is to authenticate the card and therefore its possessor. Unlike the CHUID authentication mechanism, the PKI-CAK authentication mechanism is highly resistant to cloning, since cloning would require obtaining a copy of the private key. PKI-CAK also provides protection against use of a revoked card as authentication fails and cardholder access is denied when certificate validation indicates that the certificate has been revoked. Similarly, failed signature verification or path validation results in a failed authentication attempt that does not admit a cardholder for access.

The PKI-CAK authentication mechanism is unique among the PIV authentication mechanisms since it is the only PIV authentication mechanism that provides at least SOME confidence in the identity of the cardholder that can be performed over the contactless interface using only card features that are mandatory under [FIPS201].

> **Recommendation 5.2:** NIST recommends that agencies transition to use of the PKI-CAK authentication mechanism at access points that only require single-factor authentication. (See Section 5.3.1 for a suggested transition strategy.)

5.1.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK)

The SYM-CAK authentication mechanism is similar to the PKI-CAK authentication mechanism, except that it uses the optional symmetric Card Authentication key to authenticate the card and it does not provide protection against use of a revoked card. Due to its optionality and its use of a single symmetric key that needs to be shared, stored and protected with reader components, SYM-CAK is not suitable as an interoperable authentication mechanism as mandated by [HSPD-12], and therefore is only suitable for use in authenticating PIV Cards issued by the same agency that operates the PACS.

5.1.5 Unattended Authentication Using Off-Card Biometric Comparison (BIO)

PACS may perform off-card biometric authentication using the fingerprint information or the optional iris images stored on the PIV Card.[9] The biometric on the PIV Card is signed by the issuer, so the authenticity of the biometric can be checked by the PACS. Verification of the signature on the biometric data object, and matching of the reference biometric template with the sample biometric template, is performed by the PACS application. The verification of signature and matching of biometric results in one-factor authentication. This authentication mechanism does not include authentication of the PIV Card.

Potentially, a biometric template could be placed on a fake card – so neither the “something you have” nor “something you know” factors are validated. As a result, this document rates the BIO authentication mechanism as a one-factor (“something you are”) authentication mechanism. BIO combined with a cryptographic challenge/response authenticates the PIV Card and thus achieves three-factor authentication (see Section 5.1.9).

> **Recommendation 5.3:** Biometric readers, especially those used at access points to Limited and Exclusion areas, should have a proven capability to accept live fingers and reject artificial fingers. Biometric readers, especially unattended readers in an Unrestricted area, should be physically hardened to protect against direct electrical compromise.

5.1.6 Attended Authentication Using Off-Card Biometric Comparison (BIO-A)

The BIO-A authentication mechanism is the same as BIO authentication but an attendant supervises the use of the PIV Card and the submission of the PIN and the sample biometric by the cardholder. Some fingerprint biometric readers have been shown to accept fake or synthetic fingerprints; others may allow access to internal wiring with relative ease. The presence of an attendant during BIO-A authentication serves to mitigate these risks. Moreover, the presence of an attendant also provides increased assurance, relative to BIO, that a fake card is not being used, which accounts for an additional authentication factor of “something you have.” Since the PIN is verified by the PIV Card and the card itself is not verified by PACS, the “something you know” authentication factor is not validated. In summary, the BIO-A authentication mechanism benefits from a presence of visual, but not from a strong challenge/response authentication, with the PIV Card. Therefore, BIO-A is considered a two-factor authentication mechanism.

5.1.7 Authentication with the PIV Authentication Certificate (PKI-AUTH)

The PIV Authentication key, as defined in [FIPS201], is a mandatory asymmetric key present on the PIV Card. A PACS that performs public key cryptography-based authentication with the PIV Authentication key uses the PKI-AUTH authentication mechanism. Use of PKI-AUTH provides two-factor authentication, since the cardholder must present the card (something you have) and either enter a PIN (something you know) or submit a fingerprint (something you are) to unlock the card in order to successfully authenticate.

---

[9] As noted in Section 4.2.3.1 of [FIPS201], neither the fingerprint templates nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images collection is optional. When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism. Agency security policy may require additional authentication mechanisms in consideration of impact-based security management.

Similar to the PKI-CAK authentication mechanism, the PKI-AUTH authentication mechanism involves validation of the PIV Authentication certificate. The validation protects against use of a revoked card as authentication fails and cardholder access is denied when certificate validation indicates that the certificate has been revoked. Similarly, failed signature verification or path validation results in a failed authentication attempt that does not admit a cardholder for access.

5.1.8 Authentication Using On-Card Biometric Comparison (OCC-AUTH)

The PIV Card may optionally implement on-card biometric comparison (OCC). With OCC, biometric comparison data is stored on the card and cannot be read, but may be used by the card to authenticate the cardholder.

The OCC-AUTH authentication mechanism is implemented by performing OCC over secure messaging. The PACS authenticates the PIV Card as part of the process of establishing secure messaging, and the response from the PIV Card indicating that OCC was successful can be verified since the response includes a message authentication code. Therefore, OCC-AUTH provides two-factor authentication – something you have (i.e., the card via establishment of the secure messaging protocol with the PACS application) and something you are (i.e., a fingerprint via OCC). The OCC-AUTH authentication mechanism is highly resistant to cloning. However, it does not protect against use of a revoked card. Additionally, not all PIV Cards support OCC-AUTH, as both secure messaging and OCC are optionally card capabilities.

5.1.9 (PKI-CAK | SYM-CAK) + BIO(-A) Authentication

Three-factor authentication may also be achieved by combining BIO(-A) with either PKI-CAK or SYM-CAK. In this case, the PKI-CAK or SYM-CAK authentication mechanism is used to authenticate the PIV Card and therefore the entry of the PIN to access the biometric fingerprint template can now be trusted.

As with the PKI-CAK authentication mechanism when performed alone, the PKI-CAK + BIO(-A) authentication mechanism is highly resistant to cloning. The mechanism also protects against the use of a revoked card as the authentication fails and the cardholder is denied access when certificate validation indicates that the PIV Card has been revoked. SYM-CAK + BIO(-A) is also highly resistant to cloning but does not protect against the use of a revoked card. Unlike PKI-CAK, SYM-CAK relies on an optional PIV Card feature, so the SYM-CAK + BIO(-A) authentication mechanism does not support interagency interoperability.

5.2 Multi-Factor Authentication

Possession of a valid PIV Card as evidenced by visual inspection of the card, reading a signed object from the card, or performing challenge/response authentication with the card, provides one-factor authentication. For this reason, the VIS, CHUID, SYM-CAK and PKI-CAK authentication mechanisms provide one-factor authentication. VIS provides weak one-factor authentication since the card verification is subjective. CHUID also provides weak one-factor authentication since it can be cloned. The BIO authentication mechanism provides one-factor authentication since the reference biometric template is compared against the sample biometric template without verifying the authenticity of the card itself. The PKI-AUTH authentication mechanism provides two-factor authentication since it requires possession of the PIV Card and knowledge of the PIN or a fingerprint that matches the OCC data. OCC-AUTH achieves two-factor authentication as the authenticity of the card is verified through secure messaging and thus the on-card biometric match can be trusted. The BIO-A authentication mechanism provides two-factor authentication since the reference biometric template is compared with the sample biometric template in the presence of an attendant. For BIO(-A), knowledge of the PIN can only be considered as a factor of authentication by combining this mechanism with either the PKI-CAK or SYM-CAK authentication mechanism. This is because once the PIV Card is authenticated the verification of the PIN can be trusted. The next section describes the use of multi-factor authentication in the PACS environment.

5.3 Selection of PIV Authentication Mechanisms

A risk-based approach should be used when selecting appropriate PIV authentication mechanisms for physical access to Federal Government buildings and facilities. Determining risk to the facility is beyond the scope of this document; however, an agency may use a Facility Security Level (FSL) Determination[10] to derive the FSL for its facilities. There is no simple one-to-one mapping between the FSL and the authentication mechanism(s) that should be employed. An FSL I campus facility may have a need for nested perimeters due to localized high-value assets. An FSL III facility may not have any high-value assets but may be larger in population. An FSL V facility may need the highest level of authentication assurance at all access points except the public entrance to a visitor center.

For these reasons, it is recommended that authentication mechanisms be selected on the basis of protective areas established around assets or resources. This document adopts the concept of “Controlled, Limited, Exclusion” areas as defined in [PHYSEC]. Procedurally, proof of affiliation is often sufficient to gain access to a Controlled area (e.g., an agency’s badge to that agency’s headquarters’ outer perimeter). Access to Limited areas is often based on functional subgroups or roles (e.g., a division badge to that division’s building or wing). The individual membership in the group or privilege of the role is established by authentication of the identity of the cardholder. Access to Exclusion areas may be gained by individual authorization only. Federal Government facilities can be identified and categorized in these areas and correspond generally to LOW (for Controlled), MODERATE (for Limited), and HIGH (for Exclusion) impact assets or resources [FIPS199]. This document recommends that Table 5-3 be used to determine the minimum number of authentication factors needed to satisfy security requirements of the area.[11]

[10] FSL determination is the criteria and process used in determining the security level of a Federal facility, as described in “The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard” [ISC-RMP].

[11] As noted in Section 5.1, the security requirements of an area may only be satisfied by authentication mechanisms that are performed successfully (e.g., all signatures can be verified and all certificates are currently valid (not expired or revoked)).

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

Table 5-3 - Authentication Factors for Security Areas

Figure 5-1 illustrates the innermost perimeter at which each PIV authentication mechanism may be used based on the authentication assurance level of the mechanism. Table 5-3 and Figure 5-1 both express constraints on the authentication mechanism that may be selected. The combined effect of Table 5-3 and Figure 5-1 determines exactly what mechanisms may be used. An exhaustive list of possible uses of PIV authentication mechanisms within protected areas is provided in Appendix D.

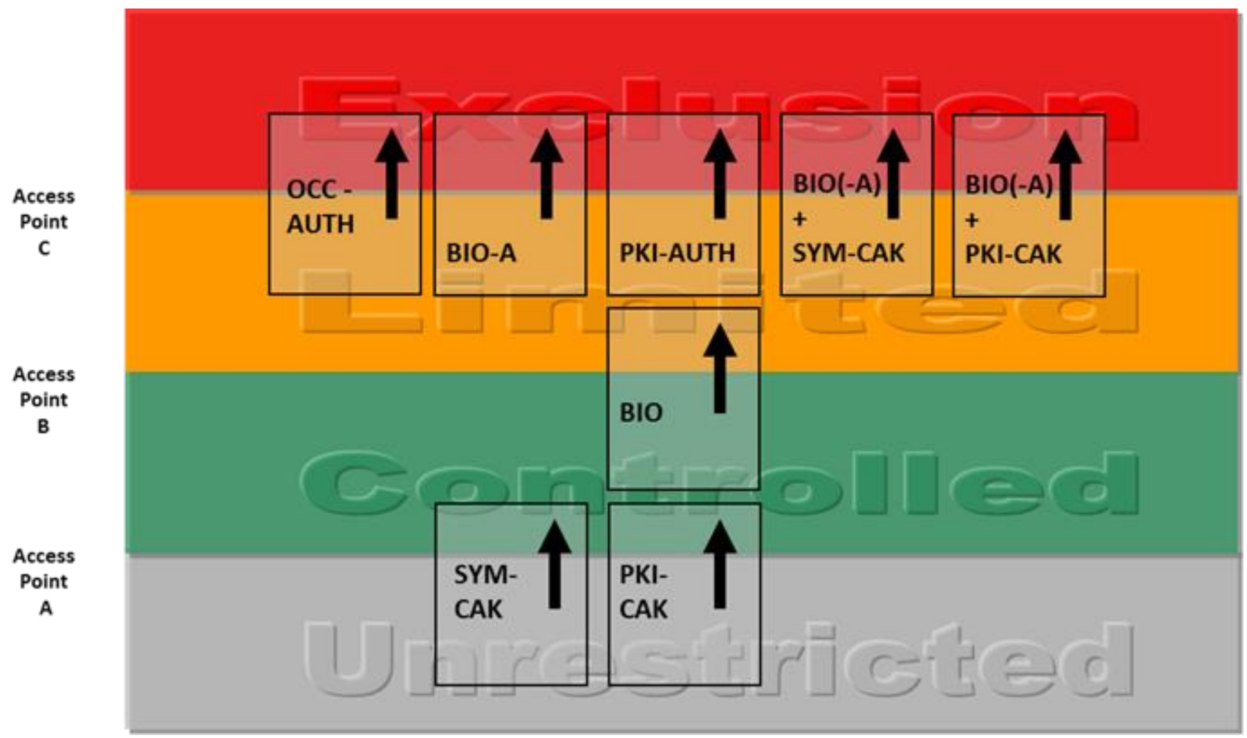

Figure 5-1: Innermost Use of PIV Authentication Mechanisms

The figure should be interpreted with the following notes:

Note 1. “BIO(-A) + PKI-CAK” means a combined authentication mechanism performing PKI-CAK and BIO or PKI-CAK and BIO-A at the same access point, both using the contact interface of the PIV Card. The term “combine” means that more than one independent authentication mechanism must successfully authenticate the presenting person, at the same access point, before access is permitted.

Note 2. Authentication mechanisms shown at a perimeter in Figure 5-1 may also be used alone at a perimeter farther out, subject to the requirements in Table 5-3, but not the reverse. If authentication mechanisms are combined in ways not shown in Figure 5-1, at least one of the combined mechanisms must be allowed by Figure 5-1 at the security perimeter of use.

Note 3. In a particular facility, a single perimeter may separate areas with a difference of more than one impact level. A single perimeter may allow access from Unrestricted to Limited, Unrestricted to Exclusion, or Controlled to Exclusion areas, and in these cases, the PIV authentication mechanisms should be combined to achieve necessary authentication factors to enter the innermost area.

Note 4. Within a Controlled or Limited area, an access point to an adjacent area at the same impact level may employ any of the authentication mechanisms shown in Figure 5-1.

Note 5. Within an Exclusion area, an access point to an adjacent area at the same impact level should use two or three-factor authentication.

Note 6. In most cases, Figure 5-1 and these notes allow flexibility in the selection of specific authentication mechanisms. A decision should be made based on the local security policy and operational considerations.

Notes (3) and (5) ensure that two-factor authentication is always employed to enter Limited areas, and three-factor authentication is employed to enter Exclusion areas. It also ensures that credential validation is done in either case.

Notes (4) and (5) add some flexibility in the case of discretionary access control among areas at the same impact level.

The previous version of this document included the combined VIS + CHUID authentication mechanism as an option to transitioning from Unrestricted to Controlled areas. VIS + CHUID, however, is not included in this version of the document since both VIS and CHUID provide “LITTLE or NO” confidence in the identity of the cardholder. Agencies currently implementing the CHUID + VIS authentication mechanism need to transition to another PIV authentication mechanism as soon as possible. Section 5.3.1 provides a migration strategy that ends the use of the CHUID authentication mechanism by September 2019. If a PACS continues to use the CHUID authentication mechanism after September 2019, then the official that signs the Authorization to Operate needs to indicate acceptance of the risks (see Sections 2.7 and 2.8).

PIV authentication mechanisms can be mapped to perimeter crossings in many ways, provided that the requirements of this section are met. Figure 5-2 below provides some examples of mapping PIV authentication mechanisms to the perimeter crossings within a facility.

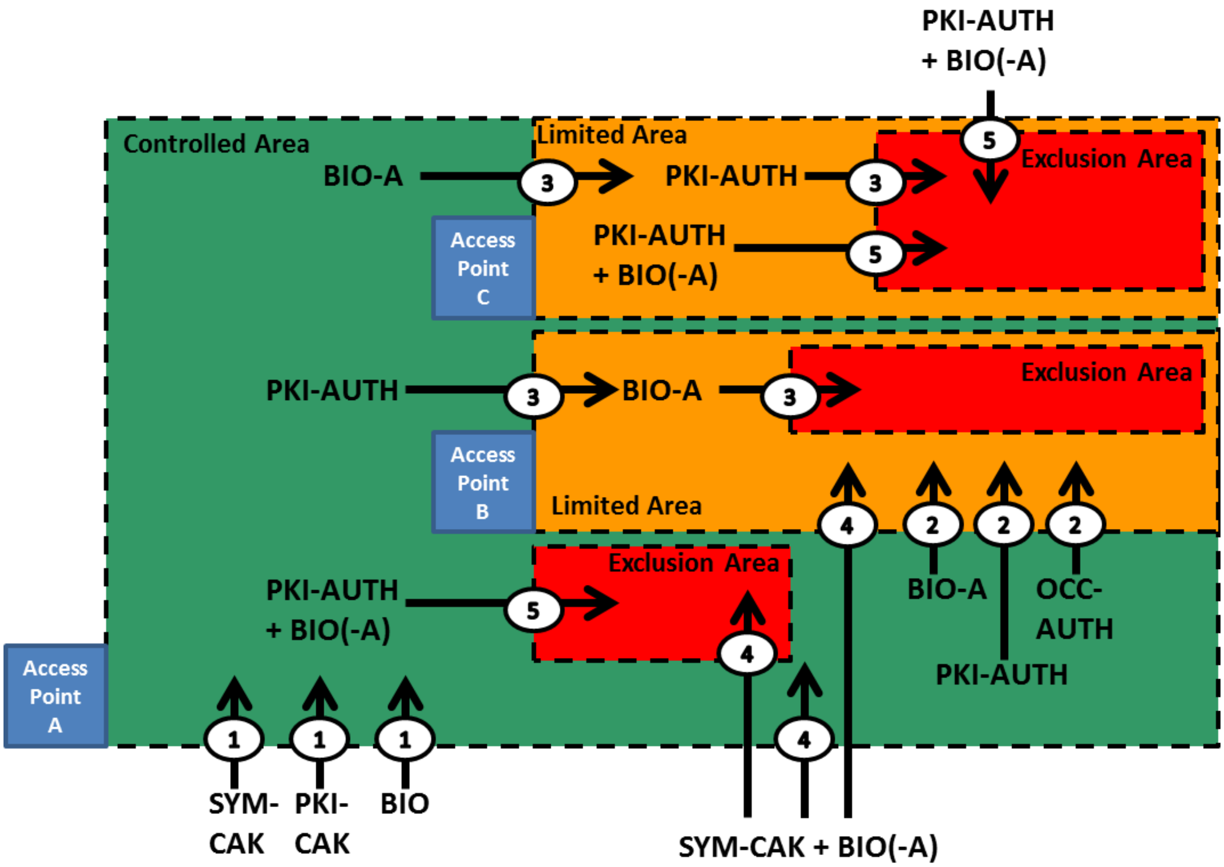

Figure 5-2: Examples of Mapping PIV Authentication Mechanisms

Figure 5-2 illustrates five different examples. Other sequences of authentication mechanisms are possible. Refer to Appendix D for a complete list of possible combinations of PIV authentication mechanisms that could be used in federal agency facility environments. Each example below is labeled with a number and is described as follows:

1. The PKI-CAK, SYM-CAK and BIO authentication mechanisms provide one-factor authentication and can be used to cross from Unrestricted to Controlled areas.

2. The BIO-A, PKI-AUTH and OCC-AUTH authentication mechanisms provide two-factor authentication and can be used to cross into Limited areas. The example shows these authentication mechanisms to cross from Controlled to Limited areas.

3. Authentication in context can be leveraged if the “Controlled, Limited, Exclusion” areas are nested. This example shows that if the BIO(-A) authentication mechanism is used to access the Limited area, then the PKI-AUTH authentication mechanism may be used to control access to the Exclusion area without requiring the cardholder to repeat the BIO(-A) authentication mechanism. Conversely, if the PKI-AUTH authentication mechanism was used to access the Limited area, then BIO-A authentication may be used to control access to the Exclusion area. Authentication in context can be leveraged only when the PACS can store and recall recent access control decisions. This in turn would

require a cardholder to authenticate at the outer perimeter prior to the inner perimeter. The risk of piggybacking, in which a person follows a cardholder through a door without authenticating, may thus be mitigated by authentication in context.

4. This example shows that an authentication at one level may be used at lower levels. This example shows the SYM-CAK + BIO(-A) authentication mechanism may be used to cross from Unrestricted to Controlled, Unrestricted to Limited, or Unrestricted to Exclusion.

5. This example shows that authentication in context is not always possible and a single perimeter may separate areas with a difference of more than one impact level.[12] The example shows that combined PKI-AUTH + BIO(-A) authentication mechanism may be used to cross from Unrestricted to Exclusion, Controlled to Exclusion, or Limited to Exclusion. Note that the three-factor authentication rule is observed in all possible crossings.

Figure 5-2 shows some legitimate examples of mapping PIV authentication mechanisms to the perimeter crossings. There are also authentication mechanisms that do not meet the requirements of Table 5-3. For example, the PKI-CAK or SYM-CAK authentication mechanism should not be used to access Limited or Exclusion areas. Limited and Exclusion areas require either two or three-factor authentication, while the PKI-CAK and SYM-CAK mechanisms only provide one-factor authentication. Also, sometimes combining authentication mechanisms does not add up to the required authentication factors. For example, PKI-CAK + PKI-AUTH is not a valid authentication mechanism to access Exclusion areas. Note that PKI-CAK + PKI-AUTH only provides two factors (“something you have” and “something you know”) of authentication.

Recommendation 5.4: Authentication assurance will be increased if a PACS uses relevant information from previous access control decisions (“context”) when making a new access control decision. For example, if a cardholder attempts to pass from a Controlled to a Limited area, the PACS could require that the cardholder was recently allowed access to the Controlled area. Historically, rigorous implementation of this concept required person-traps and exit tracking, but partial implementations have significant value, and could be strengthened by new technology and systems integration.

5.3.1 Migrating Away from the Legacy CHUID Authentication Mechanism

The CHUID authentication mechanism was included in the initial FIPS 201 to enable electronic authentication with legacy systems, but was deprecated in FIPS 201-2, and is expected to be removed in the next revision, because of its security concerns, as described in Section 2.7 and Section 2.8. In addition, both the CHUID and VIS authentication mechanisms were downgraded in FIPS 201-2 to indicate that they provide LITTLE or NO assurance in the identity of the

[12] Although a single perimeter could separate areas with a difference of more than one impact level, this practice may be judged high risk and be prohibited by local security policy.

cardholder. For these reasons, use of the CHUID authentication mechanism, even in combination with VIS, is no longer recommended. Departments and agencies are strongly encouraged to transition to other authentication mechanisms as soon as possible.

It is understood, however, that an immediate transition away from use of the CHUID authentication mechanism will not be feasible in many cases. While Section 5.1 describes several authentication mechanisms, PKI-CAK is the only authentication mechanism providing at least SOME assurance in the identity of the cardholder that has the potential to provide fast authentication and that can be implemented using only card features that are mandatory under FIPS 201-2. However, at the moment, not all PIV Cards support the PKI-CAK authentication mechanism since the Card Authentication certificate was optional prior to FIPS 201-2. Rather than using CHUID + VIS to authenticate all cardholders until all valid PIV Cards have Card Authentication certificates, a gradual transition to alternative authentication mechanisms is recommended. Two strategies for transitioning away from use of the CHUID + VIS authentication mechanism are described below, one for use with PIV Cards that have been preregistered with the PACS before they are used at an access point and one for use with PIV Cards that have not been preregistered. Preregistration is recommended, when possible, since it allows for some aspects of the authentication to be performed in advance (see Sections 5.5 and 5.6, and Appendix A), thus reducing transaction times when PIV Cards are presented at access points.

If a PIV Card is registered with the PACS before it is used at an access point, then the authentication mechanism to use with the card at entry points to Controlled areas may be determined at the time of registration. If the PIV Card was issued by the agency that controls the PACS and the card has a symmetric Card Authentication key, then the SYM-CAK authentication mechanism may be used.[13] Alternatively, if a Card Authentication certificate is present on the card, then the PKI-CAK authentication mechanism should be used. In the absence of a Card Authentication certificate, the card should be validated during the registration process using the PKI-AUTH authentication mechanism in order to ensure that it is a valid PIV Card, and not a card produced via visual counterfeiting and electronic cloning, as described in Sections 2.3 and 2.8. If the card is determined to be valid, then the CHUID + VIS authentication mechanism may be used.

If a PIV Card that has not been preregistered with the PACS is presented at an entry point to a Controlled area and the PACS allows use of cards that have not been preregistered, then the system should first try to read the Card Authentication certificate from the card, and use the PKI-CAK authentication mechanism if the certificate is present. In the absence of the Card Authentication certificate, the card should be authenticated using the CHUID + VIS authentication mechanism.

FIPS 201-2 requires all PIV Cards issued after September 2014 to include a Card Authentication

[13] Since the SYM-CAK authentication mechanism does not provide protection against use of a revoked card, agencies using this authentication mechanism would need to have processes in place to deauthorize use of PIV Cards in the PACS when cards are revoked.

certificate. So, using the transition strategies described above, use of the CHUID + VIS authentication mechanism should gradually decrease until it is entirely eliminated by September 2019 once all valid PIV Cards have completed their five-year lifecycle and have been replaced with cards containing the Card Authentication certificate.

5.4 PIV Identifiers

Once the cardholder is authenticated, the next step is making an access control decision. Access control decisions can be made by comparing PIV identifiers against access control list (ACL) entries. Examples of PIV identifiers used in access control decisions include the FASC-N (entire or part of), the Card Universally Unique Identifier (UUID), and the optional Cardholder UUID.

When deciding on the identifier to be used for access control decisions, agencies should consider the advantages and disadvantages of each type. Some of these decisions include the need to be able to grant access to holders of PIV Cards issued by another agency, and whether the agency will grant access to holders of PIV-Interoperable Cards (PIV-I Cards[14]).

Table 5-4 illustrates the pros and cons of using each identifier:

PIV Identifier	Pros	Cons
FASC-N	• Available on all PIV Cards • Access control permissions can be based on one or more fields within the FASC-N	• ACL entries may need to change every time a PIV Card is re-issued. (See Appendix C) • Not available on PIV-I Cards
Card UUID	• Available on all PIV-I Cards • Available on all PIV Card issued under FIPS 201-2	• ACL entries have to be updated every time a PIV or PIV-I Card is re-issued • May not be available on PIV Cards issued under FIPS 201-1
Cardholder UUID	• ACL entries do not have to be updated every time a cardholder is issued a new card	• Not available all cards since it is optional • Only appears in the CHUID data object

Table 5-4 - PIV Identifiers

The FASC-N is a required data element on the PIV Card, which enables agencies to use it as an identifier for access control decisions. An advantage of the FASC-N over the Card UUID and the Cardholder UUID is that ACLs can be based on one or more fields within the FASC-N (see Appendix C). The FASC-Ns on PIV-I Cards, however, cannot be used in access control decisions, since they are not assigned in a manner than ensure uniqueness.

[14] PIV-I Cards are defined in [PIV-I NFI] and further clarified in [PIV-I FAQ] and [PIV-I CP]. The intent of [PIV-I NFI] is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and their applications, and that may be trusted for particular purposes at the discretion of the relying Federal departments and agencies.

The Card UUID is a required data element for PIV-I Cards that enables departments and agencies to identify a PIV-I cardholder. The Card UUID is also a required data element for PIV Cards issued under FIPS 201-2. So, after August 2019, once all PIV Cards issued under FIPS 201-1 have expired, PACS will be able to use the Card UUID in ACLs with all PIV and PIV-I Cards.

The Cardholder UUID is an optional data element introduced in FIPS 201-2. Unlike the FASC-N and Card UUID, the Cardholder UUID is a persistent identifier for the cardholder that does not change when the cardholder receives a replacement card. So, for cards that have a Cardholder UUID, use of the Cardholder UUID can avoid the need to update ACL entries every time a cardholder is issued a new card. However, since the Cardholder UUID only appears in the CHUID data object, use of this identifier to make access control decisions would tend to increase transaction times, as there would be a requirement to authenticate the cardholder (e.g., using PKI-CAK), then read and validate the CHUID data object, and then compare an identifier in the CHUID data object to an identifier in the data object used during the authentication in order to ensure that both data objects were issued to the same card (e.g., comparing the Card UUID in the CHUID to the Card UUID in the Card Authentication certificate). An alternative would be store both the Cardholder UUID and either the FASC-N or Card UUID in the ACL, grant access if the card's FASC-N or Card UUID is present on the ACL, and only check the Cardholder UUID if the presented FASC-N or Card UUID is not on the ACL. If the Cardholder UUID is found on the ACL, then the corresponding FASC-N or Card UUID should be updated in the ACL for use in future transactions.

5.5 PACS Registration

Before a PACS may grant access to a cardholder, the cardholder must be authorized for access in the PACS. Authorization may be granted to a group of individuals, such as all PIV cardholders, or all PIV cardholders sponsored by a specific agency (see Appendix C). If authorization is granted to specific individuals, information about the cardholder (see Section 5.4) must be added to the PACS server's authorization database.

If online credential validation is performed by the PACS at the time of each authentication (see Section 5.6), the PACS might not need to store any information about the cardholder other than the authorizations and transaction audit log. If a caching status proxy is employed, information about the cardholder, including the cardholder's certificate, must be added to the server's database. Where one-factor authentication is sufficient, the Card Authentication or PIV Authentication certificate may be used. Where at least two-factor authentication is required, the PIV Authentication certificate should be used.

When the individual is enrolled using a caching status proxy, the enrollment station obtains the PIV Authentication or Card Authentication certificate from the PIV Card, validates the certificate (including checking the certificate's revocation status), and sends a challenge to the card to verify that it holds the private key corresponding to the certificate. The authentication certificate is then added to the server's database, along with any other information about the individual that the server maintains (e.g., the individual's authorizations).

Since certificate revocation is used as a mechanism to indicate that a PIV Card should no longer be considered valid, the caching status proxy should periodically revalidate all of the certificates in its database and deactivate the access privileges of any individual whose certificate has expired or has been revoked. Revalidation should be performed by the caching status proxy at least once per day. Once the decision has been made to revoke a PIV Card, agencies may employ local deauthorization methods to supplement certificate revocation and achieve a more rapid local effect.

> **Recommendation 5.5:** The CHUID may be collected at registration, but it should not be retained. A stored CHUID presents a risk, because it can be copied and used to gain access at access points that have not yet migrated away from use of the CHUID authentication mechanism. Data elements (e.g., the FASC-N and Global Unique Identifier (GUID)) may be extracted from the CHUID and retained, as may a hash of the CHUID. *NIST strongly recommends against the storage of complete CHUIDs in relying systems.*

> **Recommendation 5.6:** PKI-AUTH and PKI-CAK authentication mechanisms should be implemented by a PACS reader capable of full certificate path validation, either online or using a caching status proxy. Agencies should consider using online status checks when the most up to date PIV Card status is necessary or if access is being granted to Exclusion areas. If a caching status proxy is used, the certificates should be captured when the PIV Card is registered to the PACS.

5.6 Credential Validation and Path Validation

Credential validation is the process of determining if a presented identity credential is valid, i.e., was legitimately issued and has not expired or been revoked.

[FIPS201] requires that any credential used in an authentication mechanism be checked to ensure that it was legitimately issued. However, not all credentials on the PIV Card include an expiration date. So, when performing the BIO, BIO-A, OCC-AUTH or SYM-CAK authentication mechanism, an additional credential needs to be checked in order to verify that the PIV Card has not expired or been revoked. This additional credential may be the CHUID, the PIV Authentication certificate, or the Card Authentication certificate.

The preferred option is to validate one of the authentication certificates. Section 5.5 of [FIPS201] states "*The presence of a valid, unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not revoked*." The footnote in Section 6.2.2.1 of [FIPS201] further says, "*The PIV Authentication certificate or Card Authentication certificate may be leveraged to verify that the card is not expired*." These statements imply that the validity of the PIV Card can be determined by performing path validation (see below) on the PIV Authentication certificate or Card Authentication certificate.

Particularly in the case of the authentication certificates, online credential validation is extremely valuable to relying parties because it retrieves the most up-to-date credential status, that block access of fraudulent PIV Cards that have been lost or stolen. However, online, on-demand credential validation may not always be practical. Some reasons include: (i) a noticeable delay in response time and (ii) absence of network connectivity to the certification authority. In these circumstances, it may be possible for PIV Cards of interest to be registered with a caching status proxy. The caching status proxy polls the status of all registered cards periodically, and caches the status responses from their issuer(s). Relying parties will see quick query-response service from the caching status proxy. The cache status should be updated at least once every 24 hours.

> **Recommendation 5.7:** Online credential validation should be implemented for all of the PIV authentication mechanisms whenever most up-to-date status is necessary.

> **Recommendation 5.8:** Caching techniques should be used to implement credential validation to get improved performance or when online, on-demand credential validation is not possible. It is also recommended that the cached data be protected against tampering.

> **Recommendation 5.9**: Credential status checks that indicate that the certificate has been revoked should always prevent a cardholder from access.

Data objects read from the PIV Card by a reader must not be fully trusted as authentic (i.e., produced by a PCI) and unmodified until their digital signatures are verified. Most data objects in a PIV Card Application have embedded digital signatures (i.e., all certificates, the CHUID, fingerprint templates, facial image, iris images, and security object). The authenticity of data objects that do not have embedded digital signatures (e.g., Printed Information Buffer) can be verified since hashes of these data objects are included in the Security Object.

Path validation (or *trust path validation*) is the process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. The public key of a trust anchor is implicitly trusted by the relying party (generally, this means it was installed into the relying system by means of a trusted process, such as a direct device-to-device copy). Full trust in a PIV authentication mechanism requires that path validation succeed for each PIV data object used by the mechanism.[15]

[FIPS201] requires that path validation be performed for all PIV authentication mechanisms, since these authentication mechanisms can be fully trusted only if path validation is performed. In the absence of path validation, an impostor could forge a fingerprint template and a CHUID object, for example, with signatures from a phony certification authority. BIO authentication would succeed with this counterfeit PIV Card, and the forgery would not be detected.

> **Recommendation 5.10:** Credential validation must be performed on all signed data objects required by the authentication mechanism in use. Path validation of a certificate should employ either online or cached status checks depending on the authentication use case, the PACS environment and the performance requirements. Because path validation is a part of credential validation, both services can be

[15] If a data object is not used in the authentication mechanism being performed, path validation need not be performed on the data object's digital signature for the authentication result to be fully trusted.

economically implemented by a single PACS service component.

5.7 Lost PIV Card or Suspicion of Fraudulent Use

If a lost PIV Card is found by a person other than the cardholder, or if a pattern of PIV Card activity raises suspicions of fraudulent use, the security office of the issuing agency, or of the cardholder’s duty station, should be notified. The security office (issuing and local duty station) will determine if further investigation is warranted and if the PCI should be asked to revoke the PIV Card.

6. PACS Use Cases

[HSPD-12] requires that PIV credentials include graduated criteria, from least secure to most secure, for authentication to ensure flexibility in selecting the appropriate level of security for each application. PIV credentials, as defined in [FIPS201], offer a range of security, which is discussed in Section 5. This section provides recommendations for the appropriate use of graduated security in PIV credentials for the PACS.

PIV credentials can be used at federally-owned buildings or leased spaces, single or multi-tenant occupancy, commercial spaces shared with non-government tenants, and government-owned contractor-operated facilities. This includes existing and new construction or major modernizations, standalone facilities, and federal campuses. Thus, PIV credentials apply to facilities requiring varying levels of security with differing security requirements.

To begin, the agency must know the security requirements for its facility. Since this is beyond the scope of this document, it is assumed that the agency has completed its facility security risk assessment. It is also assumed that the agency is using the FSL determination [ISC-RMP] to derive the security requirement for its facility. The FSL takes into account size and population, as well as several other factors that capture the value of the facility to the government and to potential adversaries. Other factors, including mission criticality, symbolism, and threat to tenant agency, are also considered. For the purposes of protecting assets and placement of proper security measures, size and population may not be as important as the mission criticality, symbolism, and threat to the tenant agency. Although there is no simple one-to-one mapping between FSL and the authentication mechanism(s), the FSL indicates the general risk to the facility. Based on the FSL, an agency should identify and categorize PACS perimeters as protecting Controlled, Limited, or Exclusion areas. Appropriate security measures can then be implemented based on the areas identified for the facility in consultation with the real property authority and legal authority. This section provides example use cases of PIV authentication mechanisms in the following facility environments:

+ Single-Tenant Facility—A facility that only includes a federal tenant, or multiple components of the same department or agency that fall under one “umbrella” for security purposes.
+ Multi-Tenant Facility—A facility that includes tenants from multiple federal departments and agencies, but no non-federal tenants.
+ Mixed-Multi-Tenant Facility—A facility that includes tenants from multiple federal departments and agencies as well as one or more non-federal tenants.
+ Single-Tenant Campus—Federal facilities with two or more buildings surrounded (and thus defined) by a perimeter.
+ Multi-Tenant Campus—Two or more federal facilities located contiguous to one another and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads or gates, entrances to connected facilities, etc. May also be referred to as a “Federal center” or “Complex.”

6.1 Single-Tenant Facility

In single-tenant facilities, a single tenant defines its own security requirements and controls its own security measures. Implementation of security measures is uniform. The facility may be an owned or a leased space. If the space is leased, the tenant usually can impose security requirements based on its needs. This type of facility may range from FSL I to FSL V. Therefore, it may have LOW, MODERATE, or HIGH value assets to protect. Facilities evaluated at FSL I or II may not implement PACS and may continue without PACS. Facilities evaluated at FSL III or above should implement PACS. These facilities may have general access areas where individual identification and authentication is not possible, or necessary. In this case, the agency should establish at least one perimeter beyond which individual authentication is required and conducted with PACS. Figure 6-1 is an example of a single-tenant facility. The figure shows a building with multiple floors occupied by one tenant. The one security perimeter is the lobby where the cardholder authentication takes place. This one-perimeter facility should be designated as a Controlled, Limited, or Exclusion area and the appropriate authentication mechanisms should be selected from Figure 5-1.

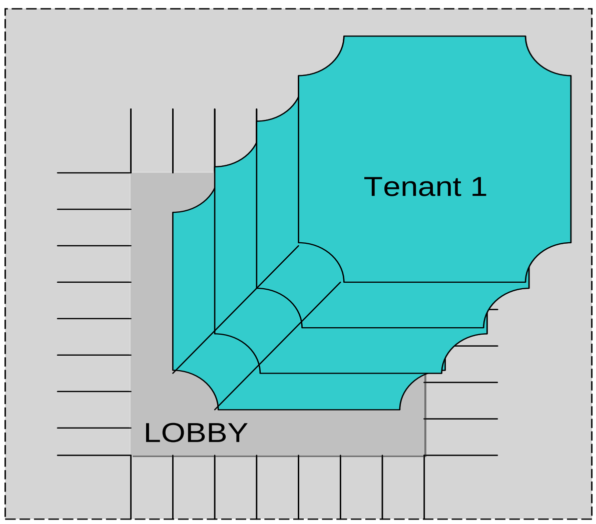

Figure 6-1: Single-Tenant Facility

6.2 Multi-Tenant Facility

The challenge with a multi-tenant facility is to meet the security policies and requirements of the individual tenants in the facility. Some tenants may need higher security than others. The security policies may not be uniform and cannot be imposed upon others. In this situation, a collective (also known as the Building Security Committee) determination has to be made by the designated officials (representatives for each federal tenant), the owning or leasing department or agency, and the security organization responsible for the facility to identify appropriate areas within the facility. In the end, the decision may be to implement the highest necessary security for the entire facility or to apply the lowest security to the facility while affording individual agencies additional security at their interior perimeters.

If the highest security is implemented for the entire facility, there is one security perimeter and the security posture is no different from a single-tenant facility. Otherwise, the multi-tenant facility may be viewed as an outer and inner perimeter where different security can be implemented. The outer perimeter is the most common security measure that all the tenants agreed to and the inner perimeter is an agency-specific security measure. For example, the facility may designate Controlled area at the outer perimeter but one of the tenant agencies may require Exclusion area protection. Access to the building may be generally satisfied with a Controlled area authentication mechanism, but the individual agency should implement an Exclusion area authentication mechanism for access to its floor(s). In this example, the building is the outer perimeter while access to an individual floor is the inner perimeter.

Since there are multiple tenants in the facility, it is strongly recommended that each individual tenant designate its own "Controlled, Limited, Exclusion" areas and employ appropriate [FIPS201] authentication mechanisms as in Figure 5-1. Since by definition the multi-tenant facility hosts Federal Government employees and contractors, the outer perimeter can be PIV-enabled and individual agencies may piggyback on the authentication performed at the outer perimeter. Figure 6-2 is an example of a multi-tenant facility. The building lobby is the outer perimeter implementing PIV-enabled PACS, while the individual tenants implement additional security perimeters for stronger cardholder authentication.

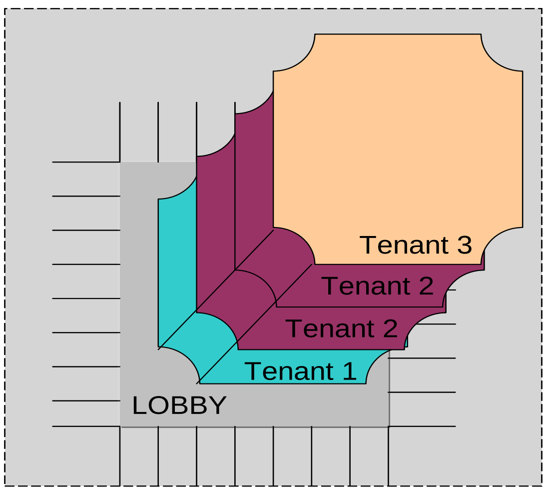

Figure 6-2: Multi-Tenant Facility

6.3 Mixed-Multi-Tenant Facility

The mixed-multi-tenant facility use case is an example of a facility with a mix of PIV cardholders and non-PIV cardholders. Therefore, some tenants in this facility may not possess PIV Cards for authentication. It may be difficult if not impossible to develop one acceptable security policy for all the tenants. The federal tenants in this facility should ensure they have leverage to implement necessary PIV authentication mechanisms for access to their space. The tenant agencies should designate their own "Controlled, Limited, Exclusion" areas and then evaluate if the facility's PACS will accommodate their security needs. Each Federal Government tenant should ensure an appropriate PIV authentication mechanism from Table 5-1 or Table 5-2 is implemented for its designated areas. If the facility's PACS cannot accommodate agencies' security needs, the tenant agencies should establish their own PACS. This may be considered an inner perimeter to the facility. In this case, the outer perimeter (i.e., access to the building) does not provide any authentication context. The individual agency should manage its own PACS server and user access. In many cases, the tenant agency will not have the authority to implement security measures independently; however, relationships in place should be used to negotiate security measures.

In the event that it is not possible to establish individual PACS and the facility is evaluated at FSL III or above, the tenant should consider the risk involved with inadequate security and make future plans to improve security posture in accordance with the PIMM model in Section 7.

6.4 Single-Tenant Campus

As opposed to a single-tenant facility, a campus is a collection of buildings, labs, and parking spaces that are geographically co-located within a large perimeter. The large perimeter is typically a fenced compound with a gate through which federal employees, contractors, and visitors gain access. This type of a facility may be assessed at FSL III or above simply due to its population and size. All the areas within the campus may not have the same security requirements. Some spaces may be generally accessible to campus visitors, while some may be specialized spaces such as a high-security lab or a chemical storage area that require a higher level of security protection. In this scenario, one security measure for all spaces might be overbearing and hamper business processes. The campus environment can be further characterized as one big perimeter (outer perimeter) and multiple smaller (inner) perimeters. There are interdependencies between these perimeters that are further elaborated through the “Controlled, Limited, Exclusion” areas.

In the campus environment, a cumulative effect of authentication is achieved as an individual traverses boundaries from Unrestricted to Controlled to Limited to Exclusion areas. In other words, authentication performed to gain access to a Controlled area should not be repeated to gain access to a Limited area. Instead, a complementary evidence of identity should be used to achieve multi-factor authentication of the individual who requests access to the Limited area. The same logic applies to the Exclusion area.

Spaces within a campus may have varying degrees of security. The campus may be subdivided into “Controlled, Limited, Exclusion” areas. Moreover, a campus may have one or more areas that are subdivided. A single Controlled or Limited area may be divided into sub-areas for purposes of discretionary or Need-To-Know access control. As a matter of local policy, the use of single-factor authentication may be sufficient to access sub-areas within the same Controlled or Limited area.

The following sections discuss the use of PIV authentication mechanisms in a campus environment with multiple perimeters. This document does not address non-PIV authentication mechanisms.

6.4.1 FSL I or II Campus Facility

Figure 6-3 depicts a security posture of an FSL I or II campus facility. It includes one or more Controlled areas that are available to authorized personnel. Since an FSL I or II campus facility can be considered a low-risk area, a PACS may or may not be maintained to preclude unauthorized entries. When PACS is maintained, SOME confidence in the identity of the cardholder should be achieved. Implementation of PIV authentication mechanisms for Controlled areas would be an appropriate countermeasure for security at this facility. PKI-CAK, SYM-CAK, and BIO are the three recommended authentication mechanisms in this environment. Note that these authentication mechanisms validate "something you have" or "something you are" (one-factor authentication).

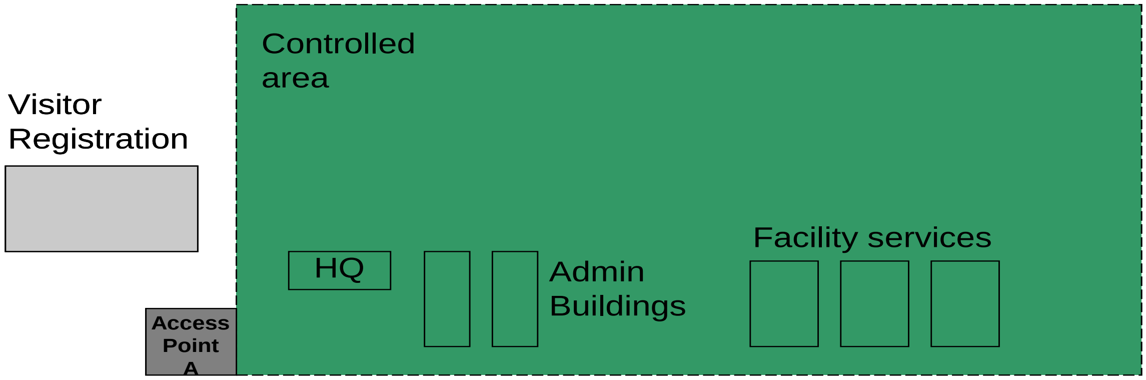

Figure 6-3: FSL I or II Campus Facility

6.4.2 FSL III Campus Facility

Figure 6-4 depicts a security posture of an FSL III campus facility. It includes one or more Controlled areas as well as Limited areas that are restricted to specific groups of individuals. Since an FSL III campus facility can be considered a moderate-risk facility, a PACS should provide additional security to the more valuable assets. HIGH confidence in the identity of the cardholder should be achieved for access to the Limited area. Note that the entire facility does not need the highest level of security. Access to the Limited area should be complemented with the authentication already completed at the Controlled area. Implementation of BIO(-A), PKI-AUTH or OCC-AUTH authentication mechanisms would be an appropriate countermeasure for the Limited area.[16] Note that these authentication mechanisms validate "something you are" or "something you know" (another factor in authentication).

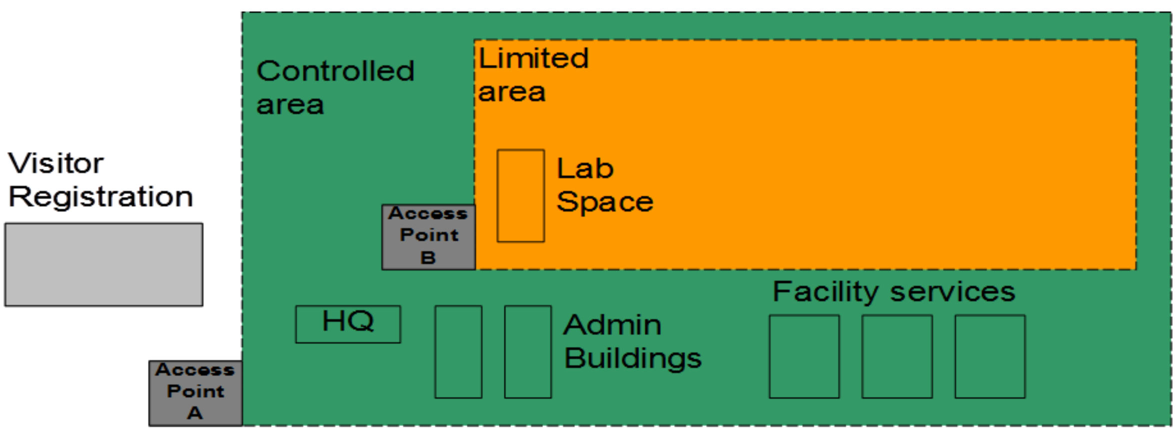

Figure 6-4: FSL III Campus Facility

---

[16] Use of the BIO authentication mechanism for access to the Limited area would require the ability to use authentication in context where it is known that the cardholder needed to perform the PKI-CAK, SYM-CAK, BIO-A, PKI-AUTH, or OCC-AUTH authentication mechanism in order to access the Controlled area.

6.4.3 FSL IV or V Campus Facility

Figure 6-5 depicts a security posture of an FSL IV or V campus facility. It includes one or more Controlled areas, Limited areas, and Exclusion areas that are restricted to specific groups of individuals.

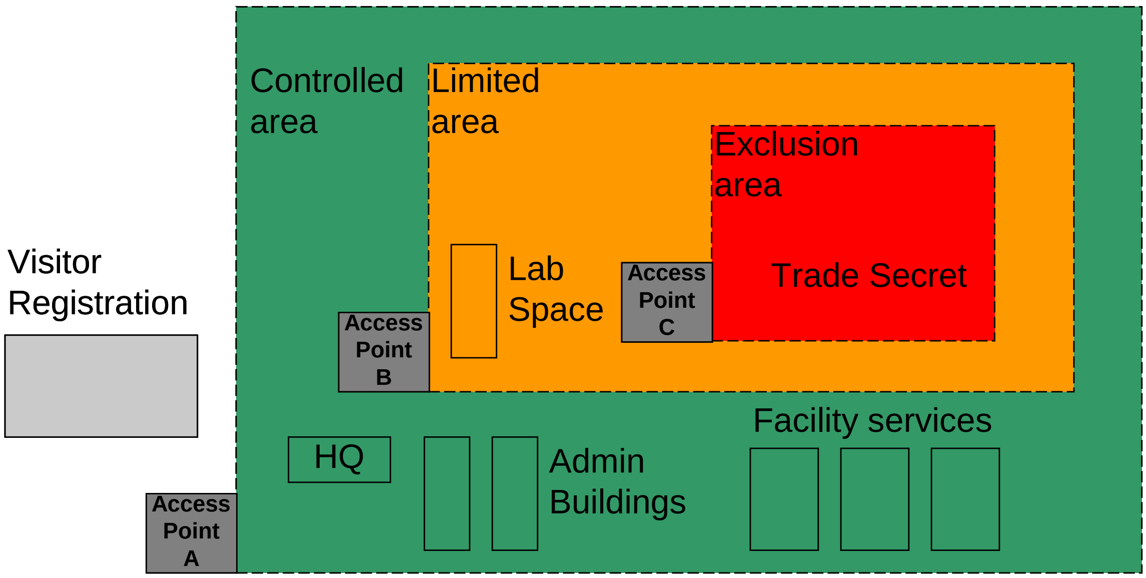

Figure 6-5: FSL IV or V Campus Facility

Although there is not a simple one-to-one mapping between FSLs and PACS authentication assurance levels at access control points, generally higher-risk areas will need stronger identity assurance. Since an FSL IV or V facility is considered a high-risk area, a PACS should achieve VERY HIGH confidence in the identity of the cardholder for access to the Exclusion areas. Note that the entire facility does not need the highest level of confidence in the identity of the cardholder. For access to the Exclusion areas, three-factor authentication should be achieved. This can be accomplished in multiple ways, as shown in Figure 5-2.

6.5 Multi-Tenant Campus

The multi-tenant campus environment is similar to the single-tenant campus except that individual tenants will have their own security policies and the enforcement may be different. A tenant may benefit from the authentication mechanism(s) implemented at the outer perimeter; however, agencies may implement their own PACS within their space. In this case, if an agency were to benefit from other agencies' PACS, its PACS should have communication links with other PACS on the campus.

Once again, each individual tenant within a campus should designate its own Controlled, Limited and Exclusion areas and identify appropriate PIV authentication mechanism(s) required for access to its space (see Figure 5-1). The tenants can then determine if they can simply use the campus PACS application, if they should add security by implementing an additional PIV authentication mechanism, or if they should implement a stand-alone PACS. Each individual tenant should ensure that appropriate PIV authentication mechanism(s) from Figure 5-1 are implemented for its designated areas.

6.6 Role-Based Access Control

Authorization of identities enrolled in a PACS is viewed as separate from cardholder authentication. PACS may grant access only to cardholders who were enrolled and authorized in the PACS server prior to presenting their credentials for authentication, or they may make on-the-fly[17] access control decisions by evaluating the information on presented PIV Cards against a set of access control rules. Because PIV Cards contain only a few mandatory subject attributes (just the Agency Code, Employee Affiliation, and Investigation Status Indicator) that may be used for role-based access control, role or group permissions will usually be derived from off-card information.

> **Recommendation 6.1:** Because having on-card role and permission information would raise difficult challenges concerning update and revocation, PACS permissions should generally be stored in a PACS facilities-based component, such as a panel or controller database.

6.7 Temporary Badges

[HSPD-12] mandated a common identification and verification standard for federal employees and contractors for physical access to federally controlled facilities and logical access to federally controlled information systems. OMB Memorandum M-05-24 [M-05-24] clarifies the eligibility requirements for a PIV Card. Temporary employees and contractors are those individuals employed 6 month or less. These individuals are not required to receive a PIV Card and agencies are permitted to issue non-PIV Cards to these individuals. In addition, PIV cardholders who have forgotten their cards may be issued a non-PIV Card on a temporary basis. Temporary badges will thus be necessary (although in smaller numbers than before) for the indefinite future.

An agency or facility should consider the relationship of temporary badges to PIV Cards and their PACS system(s) when selecting temporary badge products. Factors to consider during the procurement process include:

+ The [M-05-24] requirement that temporary badges be visually and electronically distinguishable from PIV Cards.
+ Capabilities and costs of enrollment stations, which will likely be local to the facility for best turnaround time.
+ The interoperability of temporary badges with PIV readers and authentication mechanisms (especially PKI-CAK for physical access).
+ The assignment of unique identifiers (FASC-N or UUID) to temporary badges, to foster interoperability with PIV readers.
+ The suitability of contactless-only temporary badges for physical access.

---

[17] Although making on-the-fly access control decisions is acceptable, it should be noted that this could introduce considerable delay in the end-user authorization process; and is therefore not recommended.

+ The performance, cost, and security tradeoffs between disposable and reusable temporary badges.

Many approaches to temporary badges are possible. However, a smart-card based solution that leverages current infrastructure and interoperates with federal PIV Card readers and their applications is recommended.

6.8 Disaster Response and Recovery Incidents

In addition to the use of a PIV credential for cardholder authentication during routine everyday use, the PIV credentials may also be used for access to federal facilities and federally controlled areas internal to disaster response and recovery incident scenes. Federal agencies should consider access for personnel from agencies with responsibilities under the National Response Framework, National Incident Management System, National Infrastructure Protection Plan, and the National Continuity Policy Implementation Plan when identifying and categorizing PACS perimeters as protecting Controlled, Limited, and Exclusion areas. Subsequently, agencies should apply appropriate (in accordance with Table 5-3) PIV authentication mechanisms to the areas to ensure that incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other manmade disaster can be electronically authenticated in order to attain movement internal to federally controlled facilities and areas within the incident scene.

7. Migration Strategy

Earlier sections provide the tools agencies will need to prepare a migration plan for PIV-enabling their PACS environment. This section discusses how these tools may be used to aid agencies with developing a migration plan.

7.1 Project Planning

Planning for a migration to PIV-enabled PACS should be viewed as an opportunity to modernize a legacy PACS. Given the threat environment, as described in Section 2, migrating to PIV-enabled PACS enhances security, fosters trust among agencies, and creates cost efficiencies. This section provides a strategy for developing migration plans, as shown in Figure 7-1.

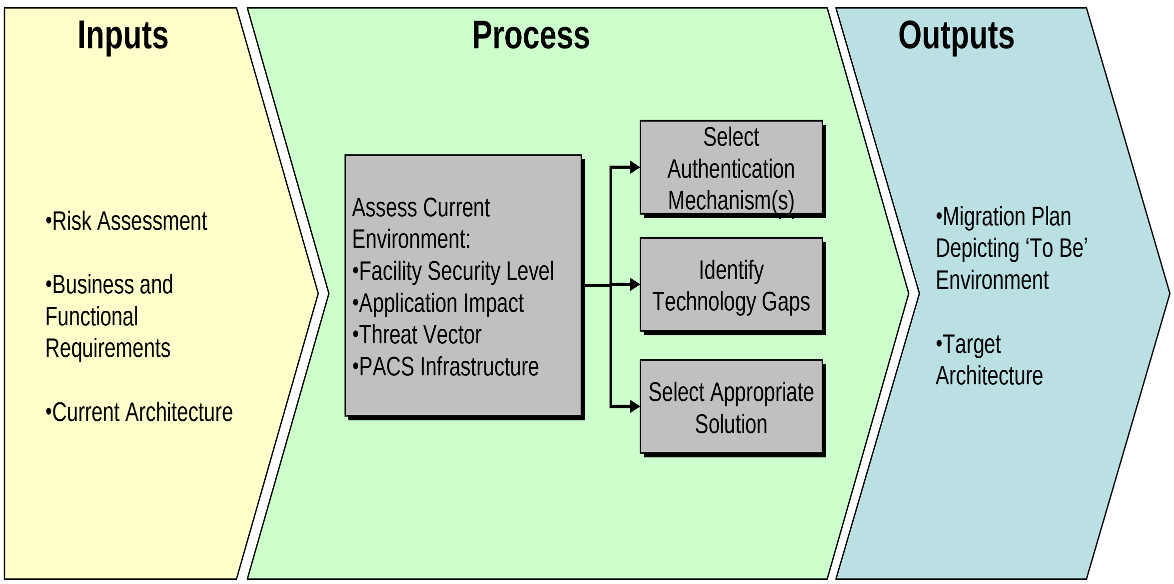

Figure 7-1: Migration Strategy

Planning should be risk-based. Not all access points will require the same level of authentication assurance. Therefore, it is important to start with the risk assessment, which distills into PACS requirements. A migration plan can then be developed to help the agency transition to the desired PIV-enabled PACS environment.

7.2 Risk Assessment

Risk assessments provide a method of prioritizing the criticality of assets (or the impact of the loss of assets), threats, and countermeasure strategies. A structured process allows for the documentation of risks by subject matter experts based on their judgments and assumptions. The final product is a broad set of priorities, both physical and cyber, that contribute to the protection of the critical systems or functions.

The input to this assessment is the understanding of risks in the current environment. Specifically, knowledge of existing vulnerabilities and the impact of attacks should be attained. Section 2 provides attack vectors that must be well understood and acted upon. The goal should be to embed the countermeasures against the identified threats in migration to PIV-enabled PACS. [HSPD-12] requires the standard to provide graduated levels of security in PIV credentials. Note that the combination of one or more authentication mechanisms must be employed to mitigate the counterfeiting, skimming, sniffing, social engineering, and cloning threats.

7.3 Business and Functional Requirements

Each agency has a unique operational environment. Agencies vary in size, organizational structure, and geographic topography. Moreover, their PACS requirements are driven by their mission and by risk and vulnerability assessment. These factors resulted in pre-HSPD-12 PACS environments that were site-specific and hardly interoperable with other agency implementations. [HSPD-12] added two requirements to these implementations, namely enhanced security and government-wide use of common identification. In other words, an identity credential issued by agency A must be usable by agency B. Note that [HSPD-12] leaves the authorization decision to individual agencies. Section 4 provides characteristics of a PIV-enabled PACS system that substantiates the goals of [HSPD-12]. Agencies are encouraged to use these characteristics to determine business and functional requirements applicable to their environment.

7.4 Develop Migration Plan

Developing a migration plan requires a vision for PIV-enabled PACS operations. Specifically, a new business process needs to be charted by those with legacy PACS to address the use of PIV credentials. This business process will be dependent on the flexibility available in changing the current environment. Some agencies may be renting spaces where access control is managed by someone else. In the end, however, an agency should have a plan to use the PIV Card.

The OMB Circular Number A-11, Part 7, Section 300: *Planning, Budgeting, Acquisitions, and Management of Capital Assets* establishes policy for the planning, budgeting, acquisition, and management of federal capital assets, and provides introduction on budget justification and reporting requirements for major IT investments for federal agencies. OMB Circular A-11 spells out the requirements for supporting several legislative directives including, but not limited to, the Clinger-Cohen Act of 1996, which requires agencies to use a disciplined capital planning and investment control process to acquire, use, maintain and dispose of information technology. In particular, the Clinger-Cohen Act specifically instructs the head of each executive agency to establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all of its major investments in information systems.

In migration planning, agencies should first determine the level of identity assurance required to gain access to their resources. Guidelines on determining the level of identity assurance and selecting a corresponding authentication mechanism are provided in Section 5 of this document. Once authentication mechanisms are selected, agencies will need to identify technology gaps in the existing system. The gaps may be in the existing readers, control panels, or PACS servers. Section 6 discusses prominent scenarios and provides recommendations on filling technology gaps.

It is recommended that agencies plan to ultimately reach the highest level of authentication assurance that displays all the qualities identified in Section 4.2. For this, guidance is provided in the following section to enable agencies to progress in stages.

7.5 Migration Strategy & Tactics

Continuity of operations planning is essential to the success of a migration from legacy PACS to PIV-enabled PACS. Planning lays the strategic framework that makes tactical, moment-to-moment change management possible without catastrophic disruptions. This section suggests sample strategies that can help the tactics succeed.

1. Encourage the project staff to train themselves. In parallel with project planning, create opportunities for the project staff to learn by doing on a small scale.
2. Budget the project carefully. The total cost of ownership of a complete PIV-enabled PACS system may be less than that of an upgraded system.
3. In order for any PIV implementation to be successful, cross-departmental collaboration is imperative. The needs of operational units left out of the process may not be fully understood.
4. Look for project synergies. For example, PACS modernization may contribute to facility monitoring, and emergency access policies for First Responders may trigger reevaluation of PACS role models and authentication methods.
5. Develop a relationship with a senior partner. A "senior partner" should be farther along in implementation, or have deeper expertise, than your organization.
6. Consider acquiring access system components that are software and hardware upgradeable to meet anticipated future requirements. For example, an agency may not see the need for contact interfaces at this time; however, it should look to purchase products that either have a dual-interface (contact and contactless capability) or plug-in for contact card readers. The agency may have a choice to add contact readers without replacing the reader infrastructure.
7. Use the extra bandwidth to support remote monitoring and diagnosis, off-loading of service elements, credential validation, cryptographic key management, and so on.
8. Initially, buy multifunction readers that read both legacy and PIV Cards and can perform all PIV electronic use cases—they can be used anywhere. Care should be taken to avoid identifier collisions between two technologies. The agency should design to the highest authentication assurance level that it thinks it may require in the future.
9. Keep performance in mind. Deploy systems integrators that are certified[18] and aim to improve transaction performance.

[18] More information about GSA-certified HSPD-12 service providers can be found at http://www.idmanagement.gov/qualified-hspd-12-service-providers.

10. As experience and the number of deployed readers grow, select more restricted and cost-effective readers implementing just the required authentication mechanisms.

11. Avoid long-term, side-by-side operation of legacy and PIV technologies.

7.6 PIV Implementation Maturity Model (PIMM)

In a document focused on the integration of PIV authentication mechanisms with PACS systems, it is impossible to provide detailed recommendations on project planning for PACS modifications or upgrades. The planning space is simply too large, due to the variations in local requirements, the asset inventory and impact assessment, project size, the installed base of electronic PACS systems, requirements for integration with other facilities' infrastructure subsystems, etc.

Instead, we recommend in this section a PIMM that can be used to measure the progress of a facility or an agency towards a complete PIV implementation. The PIMM should be applied only to facilities that have established a requirement for an electronic PACS.

The PIMM is organized around the assumption of three enclosing perimeters: the Controlled area, the Limited area, and the Exclusion area, shown in Figure 5-1. In a general sense, Controlled, Limited and Exclusion areas may be considered as the security perimeters consistent with protection of low, moderate, and high impact assets, respectively. The following PIMM maturity levels begin by achieving some capability and experience with PIV-based PACS:

1. Maturity Level 1—Ad Hoc PIV Verification. A site has the ability to authenticate PIV Cards by performing required authentication mechanisms on an ad hoc, on-demand basis. For example, card and cardholder authentication is achieved with a handheld device or a specific personal computer, for special or occasional uses.

2. Maturity Level 2—Systematic PIV Verification to Controlled Area. At the outer perimeter of the site (Controlled area), PIV Cards are accepted as proof of identity, possibly in addition to currently deployed non-PIV PACS cards. A visitor registration procedure exists to accept PIV Cards and if necessary convert PIV authentication to a currently deployed non-PIV PACS card.

3. Maturity Level 3—Access to Exclusion Areas by PIV or Exception Only. Access to Exclusion areas (the most sensitive areas) is permitted by PIV authentication or "exception" only. Here, exceptions are the exceptions to PIV issuance (e.g., less than six months association). However, all access to exclusion areas is also subject to authorization, and authorization would typically only be granted to PIV cardholders. The exception case might be applied to exclusion areas for very important person (VIP) visitors, for example. At Level 3, currently deployed non-PIV PACS cards are not acceptable for authentication to Exclusion areas.

4. Maturity Level 4—Access to Exclusion and Limited Areas by PIV or Exception Only. Access to Limited areas (generally, those permitting clearance level- or role-based authorization) is permitted by PIV authentication or exception only. At Level 4, currently deployed non-PIV PACS cards are not acceptable for authentication to

Exclusion or Limited areas. BIO, BIO-A, OCC-AUTH and PKI-AUTH are acceptable authentication mechanisms in Limited Areas for authorized PIV cardholders.

5. Maturity Level 5—Access to Exclusion, Limited, or Controlled Areas by PIV or Exception Only. Access to Controlled areas (showing evidence of organizational affiliation, or registration for a visitor, with or without escort) is permitted by PIV authentication or exception only. At Level 5, currently deployed non-PIV PACS cards are not acceptable for authentication to any areas. That is, only the PIV Card is an acceptable credential for federal employees and contractors.

The first two recommended maturity levels achieve some capability and experience with PIV authentication mechanisms. This capability may exist in parallel with deployed PACS, and after Level 2, the facility has achieved a capability to accept PIV Cards from visitors for access to Controlled areas. The next three maturity levels displace deployed PACS to Exclusion, Limited, and Controlled areas, beginning with the highest-impact areas (with, presumably, the smallest number of access control points and authorized subjects) and moving to the Controlled area (with the largest number of access control points and authorized subjects). At Level 5, the entire facility has been converted to PIV authentication mechanisms at all access points, and/or all subjects, where it is required and appropriate.[19]

Maturity levels are progressive: for example, achieving Level 2 requires satisfying all of the requirements of Level 1 in addition to the requirements of Level 2. Maturity levels can be applied to individual facilities, or by extension to multiple facilities within a bureau or agency. When applied to multiple facilities, a maturity level is achieved when each of the facilities in the group has achieved the maturity level individually.

7.7 PIV-in-PACS Best Practices

[HSPD-12] mandates the establishment of government-wide identity credentials and the use of these credentials in gaining physical access to federally controlled facilities. This implies that a PACS application installed at these facilities should interoperate with the credential standardized by [FIPS201], the PIV Card, issued by any government agency. The PIV Card interface and data model requirements are fully specified through [FIPS201] and companion documents. For the PACS application (or PIV-enabled PACS application), the following best practices are recommended.

+ PACS application providers to employ products that are approved through the [FIPS 201 EP] for relevant product categories.

+ For each access transaction, once the applicable authentication mechanisms are satisfied, all PACS access decisions are based on the utilization of an acceptable PIV identifier (see Section 5.4).

[19] Note that some use of methods other than [FIPS201] authentication mechanisms will continue because not everyone is eligible or required to have a PIV Card.

+ The PACS application that uses PKI-AUTH or PKI-CAK authentication mechanisms should support all of the asymmetric algorithms specified in Table 3-1 of [SP800-78].

+ Each facility should be mapped to the "Controlled, Limited, Exclusion" model and an assignment of PIV authentication mechanisms to all access control points in accordance with Section 5.1.

+ Signature verification and path validation is performed on all signed data objects for the PIV authentication mechanisms used. Failure of signature verification or path validation results in a failed authentication attempt that does not admit a cardholder for access.

+ Credential validation is implemented for all authentication mechanisms and failure of the validation results in a failed authentication attempt that does not admit a cardholder for access. Caching of validation results (with periodic recheck) is preferred in certain circumstances (see Section 5.6).

+ The CHUID authentication mechanism should be implemented only when combined with the VIS authentication mechanism, and only as part of a strategy to migrate to a stronger authentication mechanism, such as PKI-CAK (see Section 2.9 and Section 5.3.1).

+ Newly purchased systems must support other authentication mechanisms besides the CHUID mechanism (e.g., PKI-CAK).

+ All PACS applications should operate at PIMM Level 5.

Appendix A—Improving Authentication Transaction Times

The deprecation of the CHUID authentication mechanism marks the end for authentication based on reading a static identifier. With the deprecation of the CHUID authentication, however, PACS systems lose a mechanism that is by nature fast. The PKI-CAK authentication mechanism, which, as described in Section 5.3.1, is the most logical replacement for the CHUID authentication mechanism, is computationally expensive. To approach transaction times closer to the CHUID authentication mechanism, optimizations are needed within the PIV Cards as well as with the readers and associated infrastructure. Transaction times for other authentication mechanisms are also important, and many of the recommendations in this section apply to other PIV authentication mechanisms as well.

The steps of the PKI-CAK authentication mechanism can be described as follows:

- The reader obtains information from the PIV Card that allows it to determine an identifier for the card and to determine the card's Card Authentication certificate.
- The reader sends a challenge string to the PIV Card and requests an asymmetric operation in response.
- The card responds to the previously issued challenge by signing it using the Card Authentication private key.
- The relying system (reader or controller) uses the public key from the Card Authentication certificate to verify the response from the card.
- The relying system verifies that the Card Authentication certificate is valid.
- The relying system uses the identifier from the card to make an access control decision.

Each of the steps above presents an opportunity for optimization.

As a starting point, PCIs should consider performance when purchasing card stock, as the card is involved in four of the six steps above. When the PKI-CAK authentication mechanism is performed the PIV Card needs to perform a power-up self-test, perform a private key signature operation using the Card Authentication private key, and transmit data to the reader, so the performance of all of these steps is relevant to the overall performance of the card. [SP800-78] allows the Card Authentication key to be either a 2048-bit RSA key or an elliptic curve cryptography (ECC) P-256 key, and many cards support both cryptographic algorithms. When a card supports both algorithms, the performance of both algorithms should be considered.

> **Recommendation A.1**: Since ECC private key operations are generally faster than RSA private key operations, PCIs should consider issuing PIV Cards with ECC Card Authentication keys rather than RSA.

The performance of the PIV Card is partially dependent upon the reader. The PKI-CAK authentication mechanism is usually performed over the contactless interface, with the PIV Card being powered by the reader's magnetic field, and cards will operate more slowly when they are underpowered. Improper installation of the reader may lead to the card being underpowered, and it may also create interference that makes communication between the card and the reader unreliable, which would also lead to increased transaction times.

> **Recommendation A.2**: Make use of Qualified HSPD-12 Service Providers[20] to ensure that PACS components are properly installed and that readers are property tested and tuned to provide optimal performance.

In order to maximize performance, the PIV Card needs to be held correctly within the reader's magnetic field. So, departments and agencies should provide information to their cardholders on the proper way to present their cards to the readers. Placing an image on the reader depicting the proper orientation of the card may also be helpful.

Preregistration of PIV Cards can help to speed up many of the steps in the PKI-CAK authentication mechanism. If the card's Card Authentication certificate was obtained during the preregistration process then it doesn't need to be read from the card at the time of authentication.[21] Instead, the reader can obtain an identifier from the card (e.g., by reading the initial portion of the CHUID and extracting the FASC-N, GUID, or Cardholder UUID) and can then use the identifier to look up the certificate in the local cache. In addition, status information for the Card Authentication certificate may be obtained from a caching status proxy rather than performing certificate validation at the time of authentication.[22]

In many PACS systems, data is transferred from the reader to the controller using the Wiegand protocol, which is very slow and only allows for one-way communication. Replacing the cabling between the reader and the controller to support fast two-way communication will provide several benefits: it will speed up the transfer of the card's identifier from the reader to the controller; it will enable the caching of the Card Authentication certificate at the controller; and it will allow the reader to offload more of the processing to the controller. Given that card readers tend to have very little processing power, it may be more efficient, if fast two-way communication is available, for the reader to send the results of the challenge to the controller rather than performing the signature verification itself.

> **Recommendation A.3**: Consider the benefits of upgrading the communications infrastructure between readers and controllers and then using the improved communication to move processing steps to the component that can perform the step most efficiently.

---

[20] Information about Qualified HSPD-12 Service Providers can be found at http://www.idmanagement.gov/qualified-hspd-12-service-providers.

[21] The PACS should be prepared to handle cases in which the Card Authentication certificate on the card was replaced (due to re-key) after the card was preregistered.

[22] Agencies should consider using online status checks when the most up to date PIV Card status is necessary.

Appendix B—Recommendations

Section 1.2

Recommendation 1.1: This document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal Government facilities and assets. Agencies should seek recommendations on PACS architectures, authorization, and facility protection from other sources.

Section 2.9

Recommendation 2.1: [Section 2] emphasizes the technical risks associated with the legacy CHUID authentication mechanism. If the CHUID authentication mechanism is used without restriction, operational risk increases as the value of targets and the availability of cloning and counterfeiting tools increase. [FIPS201] deprecates the use of the CHUID authentication mechanism since it provides 'LITTLE or NO' confidence in the identity of the cardholder, and so relying systems should phase out use of this authentication mechanism as soon as possible. NIST recommends transitioning away from the CHUID authentication mechanism using the strategy described in Section 5.3.1.

Section 4.1

Recommendation 4.1: To obtain the full benefit of PIV interoperability, PIV project managers should ensure that relying systems have the capability to use all cryptographic algorithms that apply to the authentication mechanism(s) performed. Departments and agencies are required to procure and deploy [HSPD-12] products from the [FIPS 201 EP] Approved Products List where applicable,[23] and can use the PIMM presented in Section 7 to measure progress toward the goal of interoperability.

Section 4.2

Recommendation 4.2: Once all appropriate authentication mechanisms are satisfied, access control decisions are made by comparing the selected PIV identifier (see Section 5.4) against the ACL entries.

Recommendation 4.3: As agencies develop risk-based implementation plans, they will create and evolve plans for PIV Card issuance and application integration. They might consider which of the nine qualities are most relevant to agency goals and priorities, and derive further project objectives, metrics, and milestones from

[23] The Evaluation Program directly supports the acquisition process for implementing HSPD-12. OMB Memorandum [M-06-18] directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability.

those qualities. They should also consider the relation of [HSPD-12] to [FISMA] requirements, and examine the potential for cost tradeoffs where PIV can replace more expensive authentication methods.

Section 4.3

Recommendation 4.4: Operational metrics should be designed to measure actual benefits over the operational lifetime of the PIV System. They may be derived by formulating each of the expected benefits above as a service quality metric, e.g., for "integrated system," service quality could be defined as the percentage of PACS registrations that are performed automatically by provisioning from the PIV issuance system.

Section 4.4

Recommendation 4.5: Maximum benefit will be obtained from the PIV System when it is adequately supported by infrastructure. Infrastructure upgrades may be justified, especially to improve communication between PACS system elements (e.g., support two-way communication).

Section 5.1.2

Recommendation 5.1: Agencies currently implementing the CHUID authentication mechanism are highly encouraged to transition to another PIV authentication mechanism as soon as possible (see Section 5.3.1 for a suggested migration strategy).

Section 5.1.3

Recommendation 5.2: NIST recommends that agencies transition to use of the PKI-CAK authentication mechanism at access points that only require single-factor authentication. (See Section 5.3.1 for a suggested transition strategy).

Section 5.1.5

Recommendation 5.3: Biometric readers, especially those used at access points to Limited and Exclusion areas, should have a proven capability to accept live fingers and reject artificial fingers. Biometric readers, especially unattended readers in an Unrestricted area, should be physically hardened to protect against direct electrical compromise.

Section 5.3

Recommendation 5.4: Authentication assurance will be increased if a PACS uses relevant information from previous access control decisions ("context") when making a new access control decision. For example, if a cardholder attempts to pass from a Controlled to a Limited area, the PACS could require that the cardholder was recently allowed access to the Controlled area. Historically, rigorous implementation of this concept required person-traps and exit tracking, but partial implementations have significant value, and could be strengthened by new technology and systems integration.

Section 5.5

Recommendation 5.5: The CHUID may be collected at registration, but it should not be retained. A stored CHUID presents a risk, because it can be copied and used to gain access at access points that have not yet migrated away from use of the CHUID authentication mechanism. Data elements (e.g., the FASC-N and Global Unique Identifier (GUID)) may be extracted from the CHUID and retained, as may a hash of the CHUID. *NIST strongly recommends against the storage of complete CHUIDs in relying systems.*

Recommendation 5.6: PKI-AUTH and PKI-CAK authentication mechanisms should be implemented by a PACS reader capable of full certificate path validation, either online or using a caching status proxy. Agencies should consider using online status checks when the most up to date PIV Card status is necessary or if access is being granted to Exclusion areas. If a caching status proxy is used, the certificates should be captured when the PIV Card is registered to the PACS.

Section 5.6

Recommendation 5.7: Online credential validation should be implemented for all of the PIV authentication mechanisms whenever most up-to-date status is necessary.

Recommendation 5.8: Caching techniques should be used to implement credential validation to get improved performance or when online, on-demand credential validation is not possible. It is also recommended that the cached data be protected against tampering.

Recommendation 5.9: Credential status checks that indicate that the certificate has been revoked should always prevent a cardholder from access.

Recommendation 5.10: Credential validation must be performed on all signed data objects required by the authentication mechanism in use. Path validation of a certificate should employ either online or cached status checks depending on the authentication use case, the PACS environment and the performance requirements. Because path validation is a part of credential validation, both services can be economically implemented by a single PACS service component.

Section 6.6

Recommendation 6.1: Because having on-card role and permission information would raise difficult challenges concerning update and revocation, PACS permissions should generally be stored in a PACS facilities-based component, such as a panel or controller database.

Appendix A

Recommendation A.1: Since ECC private key operations are generally faster than RSA private key operations, PCIs should consider issuing PIV Cards with ECC Card Authentication keys rather than RSA.

Recommendation A.2: Make use of Qualified HSPD-12 Service Providers[24] to ensure that PACS components are properly installed and that readers are property tested and tuned to provide optimal performance.

Recommendation A.3: Consider the benefits of upgrading the communications infrastructure between readers and controllers and then using the improved communication to move processing steps to the component that can perform the step most efficiently.

[24] Information about Qualified HSPD-12 Service Providers can be found at http://www.idmanagement.gov/qualified-hspd-12-service-providers.

Appendix C—FASC-N Uniqueness

Access control decisions can be made by comparing PIV identifiers (see Section 5.4) against the ACL entries. While any of the PIV identifiers may be used in making access control decisions, within the limitations described in Section 5.4, this appendix discusses the use of the FASC-N, or portions of the FASC-N, for making access control decisions.

Three components of the FASC-N, the Agency Code, System Code, and Credential Number, constitute the FASC-N Identifier. An individual's FASC-N Identifier is unique among all cardholders when the complete three-element subset of the FASC-N is used for comparison. There will be no collisions since all the cardholders have been assigned unique numbers. An ACL pattern may match the entire FASC-N, just the Agency Code, or the Agency Code and System Code (e.g., all PIV Cards issued to one agency, or to one site in one agency) without introducing dangerous collisions or ambiguities across agencies. The values of additional FASC-N fields may be included in the identifiers that are compared against the ACL entries.

This restricts the access control comparison to one of three cases when using the FASC-N:

1. the Agency Code alone (i.e., all PIV Cards with the same Agency Code are accepted);
2. the Agency Code and System Code only (i.e., all PIV Card with the same Agency Code and System Code are accepted); or
3. the Agency Code, System Code, and Credential Number (i.e., a uniquely identified PIV Card).

Any of these cases may also include comparison of additional FASC-N values such as the Credential Series, Individual Credential Issue, Organizational Identifier, or Person Identifier.[25]

The FASC-N data fields are defined as fixed length values of Binary Coded Decimal digits. The complete subset of three data fields is 14 decimal digits in length, as stored on the PIV Card. Other representations of the FASC-N Identifier, for example a binary representation, may be used off card, provided that they are isomorphic with respect to pattern matching. The following examples demonstrate the possible uses of FASC-N in a PIV-enabled PACS application.

C.1 Full FASC-N Comparison

The following table shows a successful match against an ACL pattern consisting of a full FASC-N comparison. These examples show an organization-specific access control policy that includes the comparison of all FASC-N fields.

[25] [SP800-73] allows issuers to populate the FASC-N's Credential Series, Individual Credential Issue, Organizational Identifier, and Person Identifier fields with all zeros, so these fields may not always provide useful information for comparison.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	123456
Credential Series	1	1
Individual Credential Issue	1	1
Person Identifier	1234567890	1234567890
Organizational Category	1	1
Organizational Identifier	0010	0010
Person/Organization Association Category	1	1

The following table shows an unsuccessful match against an ACL pattern consisting of full FASC-N comparison.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	234567
Credential Series	1	1
Individual Credential Issue	1	1
Person Identifier	1234567890	1234567890
Organizational Category	1	1
Organizational Identifier	0010	0010
Person/Organization Association Category	1	1

C.2 FASC-N Identifier Comparison

The following table shows a successful match against an ACL pattern consisting of one specific FASC-N Identifier.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	123456

The following table shows an unsuccessful match against an ACL pattern consisting of one specific FASC-N Identifier.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8367	8377
Credential Number	123456	123456

C.3 Partial FASC-N Comparison

The following table shows a successful match against an ACL pattern consisting of an Agency Code and the System Code. The “x” symbols represent “don’t care” decimal digits.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8391	8391
Credential Number	654321	xxxxxx

The following table shows an unsuccessful match against an ACL pattern consisting of an Agency Code and the System Code.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3628	3728

System Code	8377	8377
Credential Number	123456	xxxxxx

The following table shows a disallowed pattern that is not an initial string of the FASC-N Identifier.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	37xx
System Code	8377	83xx
Credential Number	123456	xxxxxx

C.4 Isomorphic FASC-N Comparison

The following table shows a successful match against an ACL pattern, with the FASC-N Identifier and the upper and lower bounds of the ACL pattern represented in hexadecimal. The match succeeds because the presented FASC-N Identifier is in the closed interval [LB, UB]. This example is the same as the MATCH example of C.2, with a shift in representation from decimal to hexadecimal.

FIELD VALUE	PIV Card FASC-N	ACL Pattern LB	ACL Pattern UB
Hexadecimal Value	21E9E156BBB1	21E9DBE03300	21E9E1D613FF

The following table shows an unsuccessful match against an ACL pattern, with the FASC-N Identifier and the upper and lower bounds of the ACL pattern represented in hexadecimal. The match fails because the presented FASC-N Identifier is not in the closed interval [LB, UB]. This example is the same as the NO MATCH example of C.2, with a shift in representation from decimal to hexadecimal.

FIELD VALUE	PIV Card FASC-N	ACL Pattern LB	ACL Pattern UB
Hexadecimal Value	21010BD3F280	21E9DBE03300	21E9E1D613FF

Appendix D—Possible PIV Authentication Mechanisms in PACS

Section 5.3 provides recommendations for selecting the authentication mechanisms to use at access points. For access to Controlled areas, it considers any PIV authentication mechanism that provides at least SOME confidence in the identity of the cardholder to be acceptable (see Table 6-2 in [FIPS201]). For access to Limited areas, it recommends use of a PIV authentication mechanism that provides either HIGH or VERY HIGH confidence in the identity of the cardholder (see Table 6-2 in [FIPS201]). It also recommends that the single-factor BIO authentication mechanism only be used to grant access to a Limited area if the PACS can ensure that the cardholder needed to authenticate at another access point with a different authentication mechanism in order to get to the Limited access point (authentication in context). For access to Exclusion areas, it recommends use of a PIV authentication mechanism that provides for at least two-factor authentication at the access point (see Table 5-1), and that the PACS ensure that all three factors are authenticated prior to granting access to Exclusion area (possibly through authentication in context).

This appendix provides a complete list of possible PIV authentication mechanism combinations that are available for application to federal facilities. The following acronyms are used in this appendix, where each acronym represents the set of PIV authentication mechanisms that provide the specified factor(s) of authentication.

Acronym	PIV Authentication Mechanisms
H (One factor – something you have)	PKI-CAK, SYM-CAK
A (One factor – something you are)	BIO
HK (Two factors – something you have, something you know)	PKI-AUTH
HA (Two factors – something you have, something you are)	BIO-A, OCC-AUTH, PKI-AUTH[26]
HKA (Three factors – something you have, something you know, something you are)	PKI-CAK+BIO(-A), SYM-CAK+BIO(-A)

Note that the table above only lists individual PIV authentication mechanisms that correspond to each acronym, except for the combinations as identified in Section 5.1. However, other PIV authentication mechanism combinations that provide the same set of authentication factors can be derived. For combined authentication mechanisms it is assumed that the combination is completed using the same interface. For example, in the case of SYM-CAK+BIO, both SYM-CAK and BIO would need to be performed over the contact interface, since BIO is performed over the contact interface as per Table 5-1.

When an access point separates a protective area from an Unrestricted area or when authentication in context cannot be used, Section 5.3 recommends that one of the following be used:

[26] When used with OCC.

- For access to a Controlled area – any authentication mechanism listed above (H, A, HK, HA, or HKA)
- For access to a Limited area – any two- or three-factor authentication mechanism listed above (HK, HA, or HKA)
- For access to an Exclusion area – any three-factor authentication mechanism listed above (HKA)

The tables below show all possible PIV authentication mechanism combinations that may be used when authentication in context can be utilized. The first table shows all possible options for accessing a Limited area when the Limited area can only be accessed from within a Controlled area. It shows that if only "something you are" was authenticated to access the Controlled area (row 2), then the options for granting access to the Limited area are the same as if authentication in context were not available, however, if "something you have" is authenticated to access the Controlled area (row 1), then there is the additional option of only authenticating "something you are" (BIO) before granting access to the Limited area.

	Access Point A (Controlled)	Access Point B (Limited)
1	H, HK, HA, or HKA	A, HK, HA, or HKA
2	A	HK, HA, or HKA

The second table shows all possible combinations when a facility has Controlled, Limited, and Exclusion areas, Limited areas can only be accessed from within Controlled areas, and Exclusion areas can only be accessed from within Limited areas.

	Access Point A (Controlled)	Access Point B (Limited)	Access Point C (Exclusion)
1	H	A or HA	HK or HKA
2	H	HK	HA or HKA
3	H	HKA	HK, HA, or HKA
4	A	HK or HKA	HK, HA, or HKA
5	A	HA	HK or HKA
6	HK	A, HA, or HKA	HK, HA, or HKA
7	HK	HK	HA or HKA
8	HA	A or HA	HK or HKA
9	HA	HK or HKA	HK, HA, or HKA
10	HKA	A, HK, HA, or HKA	HK, HA, or HKA

The "Access Point C" column shows the authentication mechanisms that can be used to access an Exclusion area given the authentication mechanisms used to access the surrounding Controlled and Limited areas (the "Access Point A" and "Access Point B" columns). For example, rows 4 and 5 show (as did row 2 in the first table) that if only "something you are" was authenticated to access the Controlled area, then two- or three-factor authentication is required at the Limited access point (HK, HA, or HKA). Row 4 shows that if HK or HKA is used at the

Limited access point after A (i.e., BIO) is used at the Controlled access point, then any two- or three-factor authentication mechanism may be used at an Exclusion access point, whereas row 5 shows that if HA is used at the Limited access point after A (i.e., BIO) is used at the Controlled access point, then "something you know" needs to be authenticated at the Exclusion access point (HK or HKA).

The third and fourth tables show all combinations in cases in which authentication in context can be used, but there are access points that separate areas that differ by more than one impact level. The third table shows the combinations for cases in which Exclusion areas can be accessed from within Controlled areas, and the fourth table shows combinations for cases in which Limited areas can be accessed from Unrestricted areas and Exclusion areas can be accessed from within those Limited areas.

	Access Point A (Controlled)	Access Point B (Exclusion)
1	H	HKA
2	A or HA	HK or HKA
3	HK	HA or HKA
4	HKA	HK, HA, or HKA

	Access Point A (Limited)	Access Point B (Exclusion)
1	HK	HA or HKA
2	HA	HK or HKA
3	HKA	HK, HA, or HKA

2259
Appendix E—References

[FIPS199] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information System*, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 1/20/15].

[FIPS201] Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. http://dx.doi.org/10.6028/NIST.FIPS.201-2.

[FIPS 201 EP] *FIPS 201 Evaluation Program*. http://www.idmanagement.gov/ficam-testing-program [accessed 2/4/15].

[FISMA] *Federal Information Security Modernization Act of 2014*, Pub. L. 113-283, 128 Stat 3073. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf [accessed 5/18/15].

[HSPD-12] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. http://www.dhs.gov/homeland-security-presidential-directive-12 [accessed 11/5/2015]

[ISC-RMP] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 1st edition, August 2013. http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf [accessed 12/16/2015].

[ISO/IEC7816] (Parts 3:2006, 4: 2013, 5:2004, 6:2004, 8:2004, and 9:2004), *Information technology — Identification cards — Integrated circuit(s) cards with contacts*.

[ISO/IEC14443] (Parts 1:2008, 2:2010, 3:2011, and 4:2008) *Identification cards - Contactless integrated circuit(s) cards – Proximity cards*

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf [accessed 1/20/15].

[M-05-24] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf [accessed 1/20/15].

[M-06-18] OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 2006. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf [accessed 12/03/15].

[SKIMMER] OMB Memorandum M-08-01, *HSPD-12 Implementation Status*, October 2007. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-01.pdf [accessed 1/20/15].

[MINEXII] NIST Interagency Report 7477, Revision II, *MINEX II: Performance of Fingerprint Match-on-Card Algorithms, Phase IV Report*, March 15, 2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908096 [accessed 1/20/15].

[PIV-I CP] Federal Public Key Infrastructure Policy Authority (FPKIPA), *Personal Identity Verification Interoperable (PIV-I) Certification Process*, Version 1.1, January 20, 2015, http://www.idmanagement.gov/sites/default/files/documents/PIVI_Certification_Process_V1.1_0.pdf [accessed 12/03/15].

[PIV-I FAQ] Federal Identity, Credentialing, and Access Management (FICAM), *Personal Identity Verification Interoperable (PIV-I), Frequently Asked Questions (FAQ)*, Version 1.0, June 28 2010. http://www.idmanagement.gov/sites/default/files/documents/PIV-I_FAQ.pdf [accessed 11/30/15].

[PIV-I NFI] Federal CIO Council, *Personal Identity Verification Interoperability For Non-Federal Issuers*, Version 1.1, July 2010. http://www.idmanagement.gov/documents/personal-identity-verification-piv-interoperability-non-federal-issuers [accessed 8/15/15].

[PHYSEC] Field Manual 3-19.30, *Physical Security*. Headquarters, Department of the Army, United States of America, January 8, 2001.

[RFC5280] Request for Comments (RFC) 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF), May 2008. http://www.ietf.org/rfc/rfc5280.txt [accessed 12/03/15].

[SECTION508] *Section 508 of the Rehabilitation Act of 1973, as amended*, 29 U.S.C. §794(d), http://www.section508.gov [accessed 1/20/15].

[SKIMMER] I. Kirschenbaum and A. Wool, "How to Build a Low-Cost, Extended-Range RFID Skimmer," *Proceedings of the 15th USENIX Security Symposium (Security '06)*, Vancouver, British Columbia, Canada, July 31 – August 4, 2006, USENIX Association: Berkeley, California, 2006, pp. 43-57.

https://www.usenix.org/legacy/event/sec06/tech/full_papers/kirschenbaum/kirschenbaum.pdf [accessed 12/03/15].

[SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, August 2013, http://dx.doi.org/10.6028/NIST.SP.800-63-2.

[SP800-73] NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-73-4.

[SP800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013. http://dx.doi.org/10.6028/NIST.SP.800-76-2.

[SP800-78] NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-78-4.

[SP800-79] NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015. http://dx.doi.org/10.6028/NIST.SP.800-79-2.

[SP800-87] NIST Special Publication 800-87 Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008. http://csrc.nist.gov/publications/nistpubs/800-87-Rev1/SP800-87_Rev1-April2008Final.pdf.

[TIG SCEPACS] *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3*, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. https://www.idmanagement.gov/sites/default/files/documents/PACS.pdf [accessed 11/6/2015].

2260

Appendix F—Terminology

The following terms are used in this document.

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access Control List	A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person's identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.
Asymmetric Keys:	Two related keys, a public key and a private key, that are used to perform complementary operations, such as authentication, encryption and decryption, signature generation and signature verification.
Assurance Level (or E-Authentication Assurance Level)	A measure of trust or confidence in an authentication mechanism defined in [M-04-04] and NIST Special Publication (SP) 800-63 [SP 800-63], in terms of four levels: • Level 1: LITTLE OR NO confidence • Level 2: SOME confidence • Level 3: HIGH confidence • Level 4: VERY HIGH confidence
Authentication	The process of establishing confidence of authenticity; in this case, in the validity of a person's identity. In this publication, authentication often means the performance of a PIV authentication mechanism.
Authentication in Context	Authentication in context is a concept in which PACS may benefit from previous authentication within nested areas in a facility. The PACS may use information from previous access control decisions ("context") when making a new access control decision.
Authorization	In this publication, a process that associates permission to access a resource or asset with a person and the person's identifier(s).
Authenticator	A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and biometrics

	are authenticators.
BIO or BIO-A	A [FIPS201] authentication mechanism that is implemented by using a fingerprint or iris images data object sent from the PIV Card to the PACS and which is matched to the cardholder's live scan. Note that the shorthand "BIO(-A)" is used throughout the document to represent both BIO and BIO-A authentication mechanisms.
Building Security Committee	A committee consisting of representatives of Federal tenants in a facility, and possibly the building owner or management. The committee is responsible for building-specific security issues and approval of security policies and practices.
Card UUID	The Card UUID is a UUID that is unique for each card, and is a required data element on all [SP800-73] compliant PIV Cards.
Cardholder	An individual possessing an issued PIV Card.
Cardholder Unique Identifier (CHUID)	A [FIPS201] authentication mechanism that is implemented by transmission of the CHUID data object from the PIV Card to PACS, or the PIV Card data object of the same name.
Cardholder UUID	The Cardholder UUID is a UUID that is a persistent identifier for the cardholder. This UUID is an optional data element on [SP800-73] compliant PIV Cards.
Certificate	A data object containing a subject identifier, a public key, and other information that is digitally signed by a certification authority. Certificates convey trust in the relationship of the subject identifier to the public key.
Certificate Revocation List	A list of revoked public key certificates created and digitally signed by a certification authority. See [RFC5280]
Certification Authority	A trusted entity that issues and revokes public key certificates.
Cloning	In this publication, a process to create a verbatim copy of a PIV Card, or a partial copy sufficient to perform one or more authentication mechanisms as if it were the original card.
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/IEC7816].

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].
Controller (or Control Panel, or Panel)	A device located within the secure area that 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.
Counterfeiting	In this publication, the creation of a fake ID card that can perform one or more authentication mechanisms, without copying a legitimate card (see Cloning).
Credential	In this publication, a collection of information about a person, attested to by an issuing authority. A credential is a data object (e.g., a certificate) that can be used to authenticate the cardholder. One or more data object credentials may be stored on the same physical memory device (e.g., a PIV Card).
Credential Validation	The process of determining if a credential is *valid*, i.e., it was legitimately issued, its activation date has been reached, it has not expired, it has not been tampered with, and it has not been revoked, suspended, or revoked by the issuing authority.
Digital Signature	A data object produced by a digital signature method, such as Rivest, Shamir, Aldeman (RSA) or the Elliptic Curve Digital Signature Algorithm (ECDSA), that when verified provides strong evidence of the origin and integrity of the signed data object.
Federal Agency Smart Credential Number (FASC-N)	As required by [FIPS201], the FASC-N is one of the primary identifiers on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in [TIG SCEPACS], and included in several data objects on a PIV Card.
FASC-N Identifier	The FASC-N shall be in accordance with [TIG SCEPACS]. A subset of FASC-N, a FASC-N Identifier, is a unique identifier as described in [TIG SCEPACS]. Section 2.1, 10th paragraph of [TIG SCEPACS] states "For full interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (i.e., a combination

	of an Agency Code, System Code, and Credential Number) when matching FASC-N based credentials to enrolled card holders." Also, Section 6.6, 3rd paragraph of [TIG SCEPACS] states, "The combination of an Agency Code, System Code, and Credential Number is a fully qualified number that is uniquely assigned to a single individual." The Agency Code is assigned to each Department or Agency by Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations* [SP800-87]. The subordinate System Code and Credential Number value assignment is subject to Department or Agency policy, provided that the FASC-N Identifier (i.e., the concatenated Agency Code, System Code, and Credential Number) is unique for each card.
Head End System (or 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.
Identifier (or Unique Identifier)	In this publication, a data object, assigned by an authority, that unambiguously identifies a person within a defined community. For example, a driver license number identifies a licensed driver within a state. The authority registers people and guarantees assignment of each identifier to a unique person.
Identity Credential	A credential that contains one or more identifiers for its subject, a person. In this publication, an identity credential is designed to verify the identity of its subject through authentication mechanisms, via an electronically mechanism (see PKI-CAK, PKI-AUTH, BIO, BIO-A, etc.) or a manual mechanism (see VIS).
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.
Interoperability	In this publication, the quality of allowing any government facility or information system to verify a cardholder's identity using the credentials on the PIV Card, regardless of the PIV Card Issuer (PCI).
Issuance (or Credential	The process by which an issuing authority obtains and verifies information about a person, assigns one or more unique identifiers

Issuance)	to the person, prepares information to be placed in or on a credential, produces a physical or data object credential, and delivers the finished credential to its subject. In the case of PIV Cards, issuance is performed only by accredited PCIs.
Issuer	The organization that is issuing the PIV Card to an applicant.
Multi-Factor Authentication	Authentication based on more than one factor. In some contexts, each factor is a different authenticator. In other contexts, each factor is one of "something you know, something you have, something you are" (i.e., memorized fact, token, or biometric) and thus the number of factors is 1, 2, or 3.
OCC-AUTH	A two-factor authentication mechanism that uses secure messaging and on-card comparison of cardholder fingerprint(s).
Online Certificate Status Protocol (OCSP)	An online protocol used to determine the status of a public key certificate. See [RFC2560]
PACS Registration	The process of authenticating, validating, and verifying information about the PIV cardholder prior to entering the information into a PACS server. The information added during registration is then utilized to perform authentication and authorization of an individual at an access point.
Path Validation (or Trust Path Validation)	The process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. Successful path validation provides strong evidence that the information in the target certificate is trustworthy.
Personal Identification Number (PIN)	A short numeric password (6 to 8 digits) used as an authenticator by the PIV Card to authenticate the cardholder.
Personal Identity Verification (PIV) Card	A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
PIV Implementation Maturity Model (PIMM)	A model that can be used to measure the progress of a facility or an agency towards accepting PIV Cards.

PIV System	A system comprised of components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical access environments.
Physical Access Control System (PACS)	An electronic system that controls the ability of people to enter a protected area, by means of authentication and authorization at access control points.
PKI	A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification.
PKI-AUTH	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV Authentication certificate and key.
PKI-CAK	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card Authentication certificate and key.
Private Key	A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.
Public Key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.
Reader	A device that interfaces with a PIV Card and a controller to execute or support execution of one or more PIV authentication mechanisms.
Relying Party	In this publication, an entity, such as a PACS, that depends upon the trust model of the PIV System to correctly produce the results of authentication, i.e., the identity of the cardholder.
Revocation	The process by which an issuing authority renders an issued credential useless. For example, a certification authority may revoke certificates it issues. Typically, a certificate is revoked if its corresponding private key is known to be, or suspected to be, compromised.
Secret Key	A key used by a symmetric key algorithm to encrypt, decrypt, sign, or verify information. In a symmetric key infrastructure (SKI), the sender and receiver of encrypted information must

	share the same secret key.
Secure Messaging	A protocol by which a PIV Card Application is authenticated to the relying system. Secure Messaging is used to provide confidentiality and integrity protection for the card commands that are sent to the card as for the responses from the PIV Card.
Skimming	Surreptitiously obtaining data from a contactless smart card, using a hidden reader that powers, commands, and reads from the card within the maximum read distance (reported as about 25 cm with [ISO/IEC 14443] smart cards like the PIV Card). [SKIMMER]
Sniffing	Surreptitiously obtaining data from a contactless smart card, using a hidden reader that receives RF signals from a legitimate reader and smart card when they perform a transaction. Sniffing is a form of electronic eavesdropping. Sniffing is possible at greater distances than skimming.
Social Engineering	A process or technique, similar to a confidence game, used to obtain information from a person without raising suspicion.
SYM-CAK	The SYM-CAK is an authentication mechanism based on the optional symmetric card authentication key. As the name implies, the purpose of the SYM-CAK authentication mechanism is to authenticate the card and thereby the cardholder.
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Trust Anchor	A named entity producing digital signatures, and a corresponding certificate that a relying party has decided to trust, i.e., if a digital signature is verified using the public key within the certificate, the signature is trusted to have been made by the entity named in the certificate.
Validation	In this publication, the process of determining that an identity credential was legitimately issued and is still valid, i.e., has not expired or been revoked.
Verification	The process of determining if an assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer.
VIS	A [FIPS201] authentication mechanism in which the visual identity verification of a PIV Card is done by a human guard.
Virtual Contact	An interface established over the contactless interface after the

Interface	presentation of the pairing code to the PIV Card using secure messaging. All non-card-management operations that are allowed over contact interface may be carried out over the VCI.
Wiegand	With regard to deployed PACS, a one-way communication protocol consisting of a formatted bit string used from the access reader to the controller. It can be used with any media, including proximity, bar code, magnetic stripe, and smart cards.

2263

Appendix G—Abbreviations and Acronyms

ACL	Access Control List
BIO	Authentication Using Off-Card Biometric Comparison
BIO-A	Attended Authentication Using Off-Card Biometric Comparison
BIO(-A)	A short-hand to represent both BIO and BIO-A authentication mechanism
CHUID	Cardholder Unique Identifier
CRL	Certificate Revocation List
DUNS	Data Universal Numbering System
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FSL	Facility Security Level
GSA	General Services Administration
GUID	Global Unique Identification Number
HSPD	Homeland Security Presidential Directive
ID	Identification
IEC	International Electrotechnical Commission
ISC	Interagency Security Committee
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LB	Lower Bound
NIST	National Institute of Standards and Technology
OCC	On-Card Biometric Comparison
OCC-AUTH	Authentication Using On-Card Biometric Comparison
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PACS	Physical Access Control System
PCI	PIV Card Issuer
PIMM	PIV Implementation Maturity Model
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI-AUTH	Authentication with the PIV Authentication Certificate Credential
PKI-CAK	Authentication with the Card Authentication Certificate Credential
POST	Power-up self-test
RF	Radio Frequency
RSA	Rivest, Shamir, Aldeman
SP	Special Publication

SYM-CAK Authentication with the Symmetric Card Authentication Key

UB Upper Bound

UUID Universally Unique Identifier

VCI Virtual Contact Interface

VIS Authentication using PIV Visual Credentials