
NIST Special Publication 800-116
DRAFT

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

NIST

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

**William MacGregor
Ketan Mehta
David Cooper
Karen Scarfone**

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8930

March 2008



U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Dr. James Turner, Acting Director

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 non-national security-related information in Federal information systems. This 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.

**National Institute of Standards and Technology Special Publication 800-116, 55 pages
(March 2008)**

Acknowledgements

The authors, David Cooper, William MacGregor, and Karen Scarfone of the National Institute of Standards and Technology (NIST) and Ketan Mehta of Mehta, Inc., wish to thank their colleagues who reviewed drafts of this document and contributed to its development. We thank Tony Cieri and Ron Martin for substantial written contributions to the document. The authors gratefully acknowledge and appreciate the support received from the Interagency Security Committee, Department of Justice (DOJ), General Services Administration (GSA), Department of Homeland Security (DHS), Department of Defense (DoD), Social Security Administration (SSA), and Department of Treasury in developing this document. Special thanks to our expert collaborators who participated in weekly conference calls and provided comments on many versions of the document:

- + Tim Baldrige
- + Joe Broghamer
- + Mike Defrancisco
- + Hildegard Ferraiolo
- + Scott Glaser
- + Christopher Hernandez
- + Gwainevere Hess
- + Everett Hilliard
- + Nolin Huddleston
- + Lemar Jones
- + C. Larson
- + Edward Layo
- + Diana Londergan
- + Ron Martin
- + Eric Mitchell
- + Steve Mitchell
- + Benjamin Overbey
- + Ron Ross
- + Austin Smith
- + Carlton Stevenson
- + David Vanderweele
- + Tom Whittle
- + Craig Zeigler

Table of Contents

1. Executive Summary	1
2. Introduction	3
2.1 Authority	3
2.2 Background	3
2.3 Purpose and Scope	4
2.4 Audience	5
3. Terminology	6
4. Threat Environment	10
4.1 Identifier Collisions	10
4.2 Terminated PIV Cards	11
4.3 Visual Counterfeiting	11
4.4 Skimming	11
4.5 Sniffing	12
4.6 Social Engineering	12
4.7 Electronic Cloning	12
4.8 Electronic Counterfeiting	12
4.9 Other Threats	13
5. Limitations of Legacy Physical Access Control Systems	14
5.1 Cardholder Identification	14
5.2 Door Reader Interface	14
5.3 Authentication Capability	14
5.4 Legacy Wiring	15
5.5 Software Upgrades	15
5.6 Legacy and PIV System Differences	15
6. The PIV Vision	17
6.1 Interoperability	17
6.2 Qualities of the Complete Implementation	18
6.3 Benefits of the Complete Implementation	19
6.4 Infrastructure Requirements	20
7. Authentication and Assurance	21
7.1 PACS Authentication Mechanisms	21

7.1.1	Legacy Proximity or Magnetic Stripe Authentication	22
7.1.2	Visual (VIS) Authentication.....	22
7.1.3	CHUID Authentication	22
7.1.4	Card Authentication Key (CAK) Authentication	22
7.1.5	PIV Authentication Key (PKI) Authentication.....	23
7.1.6	BIO Authentication	23
7.1.7	BIO-A Authentication.....	23
7.2	Multi-Factor Authentication	23
7.3	Selection of Authentication Mechanisms	23
7.4	PACS Enrollment	25
7.5	Credential Validation and Path Validation.....	26
7.6	Lost PIV Card or Suspicion of Fraudulent Use	27
8.	PACS Use Cases.....	28
8.1	Single-Tenant Facility	28
8.2	Multi-Tenant Facility	29
8.3	Mixed-Multi-Tenant Facility	30
8.4	Single-Tenant Campus	30
8.4.1	Level I or II Campus Facility	31
8.4.2	Level III Campus Facility	31
8.4.3	Level IV or V Campus Facility	32
8.5	Multi-Tenant Campus.....	33
8.6	Role-Based Authentication	33
8.7	Temporary Badges	33
9.	Migration Strategy	35
9.1	Project Planning.....	35
9.2	Risk Assessment	35
9.3	Business and Functional Requirements	36
9.4	Develop Migration Plan.....	36
9.5	Migration Strategy & Tactics	36
9.6	PIV Implementation Maturity Model (PIMM)	37
10.	Future Topics	39
10.1	Generalized Credential Identifier	39
10.2	Secure Biometric Match-On-Card.....	39

List of Figures

Figure 7-1: Perimeters and Authentication Mechanisms	2
Figure 7-1: Perimeters and Authentication Mechanisms	24
Figure 8-1: Single-Tenant Facility	29
Figure 8-2: Multi-Tenant Facility	30
Figure 8-3: Level II Campus Facility	31
Figure 8-4: Level III Campus Facility	32
Figure 8-5: Level IV or V Campus Facility	32
Figure 9-1: Migration Strategy	35

List of Tables

Table 7-1. Expanded PACS Assurance Levels	21
---	----

1. Executive Summary

The physical access control systems (PACS) deployed in most Federal buildings are facility-centric rather than enterprise-centric and are designed around proprietary PACS architectures. Therefore, the PACS as they are installed today are not interoperable. The technologies used in these systems may offer little or no authentication assurance. In addition to the lack of interoperability, legacy PACS technology presents the following challenges:

- + Scalability. Even when two sites use compatible card technology, they assign site-specific identifiers to cards. Without government-wide coordination of identifiers, the same identifier could be used on multiple cards at different sites.
- + 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.
- + 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 with access to multiple sites.
- + Efficiency. Use of personal identification numbers (PIN), Public Key Infrastructure (PKI), and biometrics with legacy PACS is 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.

Homeland Security Presidential Directive 12 (HSPD-12) sets a clear goal to improve PACS through the use of government-wide standards. Federal Information Processing Standard (FIPS) 201 defines characteristics of the identity credential that can be used interoperably 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 FIPS 201 authentication mechanisms. FIPS 201 defines authentication mechanisms at three E-Authentication assurance levels (SOME, HIGH, and VERY HIGH), and standardizes optional credential elements that extend trust in the PIV System to functions beyond subject authentication. A gap remains, however, between the concepts of impact and assurance levels. To close this gap, this document:

- + Discusses the different PIV Card authentication capabilities so that the Facility impact assessment can be aligned with the appropriate FIPS 201 authentication assurance levels.
- + Introduces the concept of Controlled, Limited, Exclusion areas to bridge the gap between PACS impact assessments and authentication assurance levels.
- + 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 access points do not all require the same level of security within a facility, the authentication assurance levels do not have one-to-one mappings with the Facility Security Levels. A given facility may need multiple authentication mechanisms. Therefore, the designation of Controlled, Limited, Exclusion areas, detailed in Section 7.3, is applied to the facility. A facility may have multiple perimeters requiring different authentication assurance levels. This document recommends FIPS 201 authentication mechanisms to Controlled, Limited, Exclusion perimeters established around assets or resources being protected. When authentication mechanisms are implemented in the manner shown in the following figure, each perimeter adds to the security context of granted access, with cumulative effect as an individual moves inward.

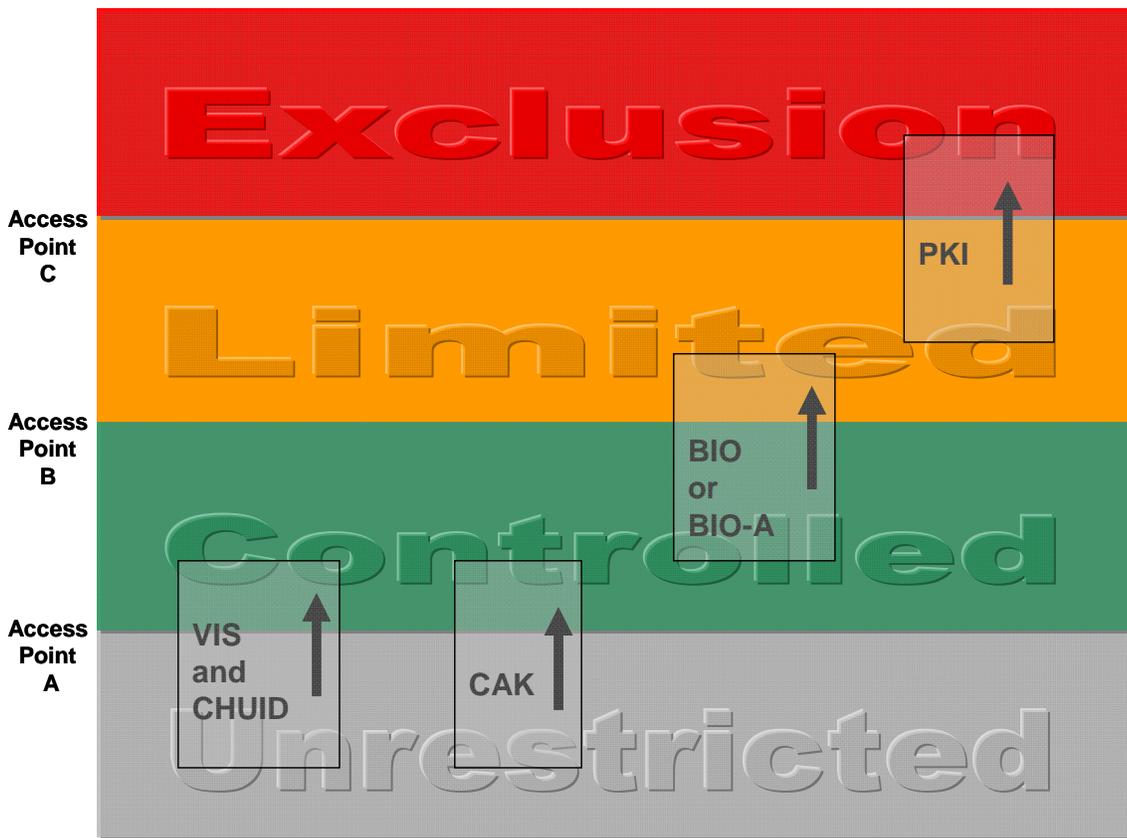


Figure 7-1: Perimeters and Authentication Mechanisms

Typically, proof of affiliation is 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 stronger authentication of the card and/or the cardholder, and authorization of a limited group). Access to Exclusion areas may be gained by individuals whose identity is substantiated by multiple factors of authentication, and who are individually authorized for access. While such guidelines are applicable in many circumstances, a facility physical security policy should specify the site-specific protection model and the requirements for authentication in physical access control.

A risk-based migration strategy should be planned and implemented to achieve PIV conformance. This document presents a model recommendation that allows agency to achieve PIV conformance incrementally. 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 Area.
- + Maturity Level 3—Access to Exclusion Areas by PIV or exception only.
- + Maturity Level 4—Access to Limited Areas by PIV or exception only.
- + Maturity Level 5—Access to Controlled Areas by PIV or exception only.

2. Introduction

2.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict 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.

2.2 Background

Homeland Security Presidential Directive 12 (HSPD-12, [HSPD-12]) mandates the establishment of a government-wide standard for identity credential to improve physical security in federally controlled facilities¹. To that end, HSPD-12 requires all government employees and contractors be issued a new identity credential based on the Federal Information Processing Standard 201 (FIPS 201, [FIPS 201]) on Personal Identity Verification (PIV). Following FIPS 201, this credential is referred to herein as a PIV Card². The Office of Management and Budget (OMB) Memorandum [M-08-01] requires that the credential issuance be accomplished by October 27, 2008 (or by the date specified in the implementation plan mutually agreed-upon by the agency and OMB). Once PIV Cards have been issued to a substantial fraction of employees and contractors, agencies can begin to maximize the use and benefits of the credential.

HSPD-12 explicitly requires the use of PIV Cards “in gaining physical access to federally controlled facilities and logical access to federally controlled information systems.” The PIV System was designed to integrate with electronic physical access control systems (PACS). 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 FIPS 201 standards suite defines the electronic authentication mechanisms as transactions between a PIV Card and a PACS reader. FIPS 201 does not, however, elaborate on the uses and benefits of the credential. This document provides guidelines on the uses of PIV credentials with PACS.

The PACS technology deployed in most Federal buildings is facility-centric rather than enterprise-centric and is designed around a proprietary PACS architecture. The PACS currently in use are not interoperable, are largely dependent on bar code, magnetic stripe, and proximity technologies, are not highly secured, and are not implemented at an enterprise level. In other words, an identity credential issued by one PACS may not have the

¹ Federally controlled facilities as defined in Section 1D of OMB Memorandum M-05-24.
<http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf>

² Federal agencies may refer to PIV Cards by other names, for example, “identity badges” or “access cards”. In this document, all such credentials issued by an accredited PIV issuer are called PIV Cards.

capability to be used by another. To enhance security and improve efficiency through the application of best practices, it is essential to develop an efficient and cost-effective strategy to migrate PACS from proprietary and facility-centric approaches to standardized and interoperable methods as defined in the FIPS 201 standard.

Full compliance with HSPD-12, and the use of FIPS 201 authentication mechanisms for access to Federal facilities and systems as required by HSPD-12, should be the principal goal 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:

- + The use of "multi-technology" readers, enabling a transition to the FIPS 201 standard over time by allowing proprietary identity cards and PIV credentials to work side-by-side.
- + Retrofit or upgrade of the existing PACS to use new credentials.
- + Coexistence of PIV-enabled and existing PACS in leased, multi-tenant facilities.

Note that when multi-technology readers, or PIV-enabled and existing PACS, are used to facilitate the transition, legacy ID cards such as magnetic stripe and proximity cards will authenticate at the LITTLE OR NO confidence assurance level, while PIV Cards will authenticate at the SOME, HIGH, or VERY HIGH confidence assurance level, depending on the authentication mechanism (see Section 7).

Recommendation: PACS technology is undergoing rapid evolution as it incorporates powerful and inexpensive sensor, computing, and networking technologies. These trends will create many opportunities for enhanced capabilities, lower cost, and comprehensive system integration. Officials responsible for policies and operation of PACS should remain alert for new national, international, and industry standards, as well as new products, to maximize mission effectiveness.

2.3 Purpose and Scope

The purpose of this document is to describe a strategy allowing agencies to PIV-enable their PACS, and migrate to standards-based identity credentials and authentication mechanisms with government-wide interoperability. Specifically, the document presents a strategy for migrating selected authentication use cases from existing PACS use cases to endpoint PIV Card use cases. 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 authentication capabilities so that the Facility Security Level assessment can be aligned with the appropriate FIPS 201 authentication assurance levels
- + 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 facility perimeters. This document does not address non-PIV mechanisms used to authenticate individuals.

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. PACS access controls are intended to be unavoidable. Section 508 should be considered early during projects that integrate the PIV System with PACS. Section 508 should be considered as it applies to enrollment software, smart card and biometric readers, monitoring systems, and access control point sensors and actuators. Note that FIPS 201,

Section 4.4.1, states that an alternative to BIO or BIO-A should be used if one or more fingers cannot be enrolled. Further information can be found at [SECTION508] and in [FIPS 201].

Many other aspects of physical access control are outside the scope of this report. Authorization (i.e., granting permission within a PACS system 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, 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 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 mitigate these risks before applying the measures.

The evaluation of specific PACS architectures or implementations is also outside the scope of this report, as is the standardization of PACS. This document does, however, make recommendations on shared infrastructure, interfaces, and procedures that will contribute to personal identity verification by 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: Agencies should utilize the higher authentication assurance offered by the PIV Card to counter physical threats to Federal government facilities resulting from misidentification. 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.

2.4 Audience

This document is intended for the government officials responsible for implementing HSPD-12. This document will also aid government executives (i.e., decision makers) to evaluate business cases and develop strategies for their departments or agencies. Information in this document is also useful to the government contractors and security industry vendors implementing HSPD-12-related systems, products, and services.

3. Terminology

The following terms are used throughout this document.

Access Control: A function or a system that restricts access to authorized persons only.

Access Control List: A list of (identifier, permissions) pairs associated with a resource or 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 Signature: A data object produced by a digital signature method, such as RSA or Elliptic Curve Digital Signature Algorithm (ECDSA), that when verified, provides strong evidence of the origin and integrity of the signed data object.

Assurance Level (or E-Authentication Assurance Level): A measure of trust or confidence in an authentication method defined in OMB Memorandum M-04-04 and NIST Special Publication (SP) 800-63, in terms of four levels:

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

Authentication: A process that establishes the identity of a person or computational process, often as a prerequisite to allowing access to physical or logical (i.e., information) resources. In this publication, authentication often means the performance of a FIPS 201 authentication mechanism.

Authentication Mechanism: In reference to FIPS 201, a method of authentication defined in Section 6 of that document or one of its normative references, i.e., one of VIS, CHUID, CAK, PKI, BIO, or BIO-A.

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 fingerprints are authenticators.

Biometric: An authenticator produced from measurable qualities of a living person.

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 Authentication Key (CAK): A FIPS 201 authentication mechanism (or the PIV Card key of the same name) that is implemented by an asymmetric or symmetric key challenge/response protocol. The CAK is an optional mechanism defined in NIST SP 800-73.

Cardholder Unique Identifier (CHUID): A FIPS 201 authentication mechanism (or the PIV Card data object of the same name) that is implemented by transmission of the CHUID data object from the PIV Card to a relying party.

Certificate (also, PKI Certificate): A data object containing a subject identifier and a PKI 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.

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 ISO/IEC 7816-3.

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 that communicates with multiple readers, actuators, and the Head End System. The readers provide cardholder information to the Controller, which it uses to make access control decisions and send commands to actuators. The Controller communicates with the Head End System to receive changes in access permissions, and to send audit records and other log information.

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 may be a physical artifact (e.g., a **PIV Card**) or a data object (e.g., a **PKI certificate**). One or more data object credentials may be stored on the same physical memory device (e.g., a smart 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, and it has not been terminated, suspended, or revoked by the issuing authority.

Federal Agency Smart Credential Number (FASC-N): As required by FIPS 201, the primary identifier on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, defined in FIPS 201 and NIST SP 800-73, and included in several data objects on a PIV Card.

Federal Agency Smart Credential Number (FASC-N) Identifier: The result of the concatenation of the System Code, Agency Code, and Credential Number from the FASC-N. The FASC-N identifier is the minimal length identifier that uniquely identifies a PIV Card; it is 14 digits when represented in decimal and 37 bits when represented in binary.

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 with the latest changes.

Identifier (or Unique Identifier): In this publication, a data object, assigned by an authority, that uniquely 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**, either manually (see **VIS**) or electronically (see **CHUID, CAK, PKI, BIO, and BIO-A**).

Infrastructure: Distributed substructure of a large-scale organization that facilitates related functions or operations, e.g., telecommunications infrastructure. With regard to PACS, components including 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.

Issuance (or Credential Issuance): The process by which an issuing authority obtains and verifies information about a person, assigns one or more unique identifiers 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 PIV Card Issuers (PCI).

Logical Access Control System (LACS): An electronic system that controls the ability of principals (i.e., people and processes with identities known to the LACS) to perform operations on objects within the boundary of a protected information system.

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.

Path Validation (or Trust Path Validation): The process of determining that a chain of asymmetric signatures, beginning with a signed object and continuing through the sequence of signing certificates to a trust anchor certificate, is complete and all certificates are valid. Successful path validation provides strong evidence that an asymmetric signature is trustworthy.

Personal Identification Number (PIN): Typically, a short numeric password (4 to 8 digits) used as an authenticator with a bank card, ID card, or other personal security device.

Personal Identity Verification (PIV) Card: The identity credential mandated by HSPD-12 and defined by FIPS 201. A PIV Card is a smart card with contact and contactless communication capability, and ten defined Data Objects for Interoperability, five mandatory and five optional.

Physical Access Control System (PACS): An electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points.

PACS Enrollment: The process of adding information about the cardholder into the PACS server. The information added during enrollment is then utilized to perform authentication and authorization of an individual at an access point.

PIV System: It is a system composed 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 and logical access environments.

Private Key: One key of a public key cryptography key pair, the other being the **Public Key**. What a private key encrypts, only the matching public key can decrypt, and vice versa.

Public Key: One key of a public key cryptography key pair, the other being the **Private Key**. Given only the public key, it is computationally infeasible to derive the matching private key.

Public Key Infrastructure (PKI): A service infrastructure implementing a trust model for transactions using private keys and public key certificates, based on the concepts of Public Key Encryption (PKE) and Certification Authorities (CA).

Reader: A device that reads an ID card and passes the ‘identifying information’ to the Controller, often using the **Wiegand** protocol, magnetic stripe, contactless (13.56 MHz), or proximity (125 kHz) technologies. Multi-technology card readers are commercially available.

Relying Party: In this publication, an entity 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 PKI Certification Authority may revoke certificates it issues. Typically, a PKI 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.

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).

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.

Termination: In this publication, the action of an identity credential issuer that causes the credential to become invalid.

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 terminated.

Verification: The process of determining if a security assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer.

Wiegand: With regard to legacy PACS, a one-way communication protocol used from the access reader to the Controller. A security industry standard, it is similar to RS-232, RS-485, and TTL. It can be used with any media, including proximity, bar code, magnetic stripe, and smart cards.

4. Threat Environment

The PIV System is built on a foundation of security assurance methodologies, but no practical system can guarantee perfect security. This section discusses known technical threats to PIV authentication mechanisms, especially the CHUID authentication mechanism. Methods of attack are described in general terms. This section should not be considered complete. 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 asymmetric signatures (“digital signatures”). Overall trust in the authentication transaction is also dependent on correct operation of the PIV Card, the PIV Card reader, the Controllers, 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 PIV System or PACS elements, with varying difficulty and potential impact.

The factors critical to sustained trust in PIV authentication 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 trusted operation of other system elements in the PIV System and the PACS.

To perform an electronic authentication transaction, the PIV cardholder presents their card to a PIV Card reader. 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 are easily carried out. 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, visual counterfeiting, skimming, sniffing, social engineering, electronic cloning, and electronic counterfeiting. These methods of attack, as well as others, are discussed below.

4.1 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 create unique identifiers during the card issuance process. The presence of a unique identifier 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 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 identifier, the concatenated Agency Code, System Code, and Credential Number in the FASC-N, for the purposes of physical access control decisions. To prevent collisions, this triple, or equivalently the entire FASC-N, should always be used as the PIV Card unique identifier for purposes of comparison against Access Control List entries. See Appendix B for further details.

4.2 Terminated PIV Cards

A terminated PIV Card could continue to open doors with the CHUID authentication mechanism long after the card has been terminated. As described in FIPS 201, the check for termination should be performed by a status check, using either the Online Certificate Status Protocol (OCSP) or certificate revocation lists (CRL), on a PIV authentication certificate³. Credential validation is required by FIPS 201 for the PKI authentication mechanism, but it is not required, nor described, for the CHUID authentication mechanism. If a PIV Card is lost, reported, and terminated by the issuer, PACS relying on CHUID authentication 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 terminated PIV Card will remain “valid” until the cache is refreshed. The process for PACS de-authorization is not required or defined by FIPS 201, raising the possibility that on-line credential validation will not be implemented, or not effectively implemented, where the CHUID authentication mechanism is employed.

The PIV Card mitigates the risk of use of a misappropriated PIV Card through the process of on-line credential validation. FIPS 201 Section 5.4.5 equates on-line PIV credential validation to path validation of a PIV authentication certificate. In the CHUID authentication mechanism, only the CHUID data object is read from the PIV Card, and a reader cannot check the status of an authentication certificate on the basis of the CHUID alone. Implementation methods that can further reduce this risk are not standardized as interoperable services in the PIV System; see Sections 7.4 and 7.5.

4.3 Visual Counterfeiting

PIV Cards are used in the VIS authentication mechanism that requires visual verification of the PIV Card 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 smart card 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. ID cards may receive only cursory examination when used as “flash passes”, however.

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, smart card stock, and smart card printers, electronic verification is strongly recommended, either in place of the VIS authentication mechanism, or in combination with it.

4.4 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, which includes the CHUID⁴ and the certificates.

The PIV Card mitigates the risk of skimming by access rules that prevent the release of biometric and other data over the contactless interface, and by minimizing content in the free-read data objects. Additional protection can be achieved by shielding techniques that positively deactivate a PIV Card when not in use. The electromagnetically opaque sleeve mentioned in FIPS 201-1 Section 2.4 is one such technique.

³ A PIV authentication certificate is either the PIV Authentication Key certificate, or the optional Card Authentication Key certificate, if present.

⁴ CHUID is one of the data elements of PIV credentials that uniquely identifies the PIV cardholder. CHUID stands for Cardholder Unique Identifier. See the latest version of NIST SP 800-73 for a complete definition

4.5 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 RF communications. A sniffer is a 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.

4.6 Social Engineering

If an attacker persuaded the cardholder to give them possession of the PIV Card, the attacker could quickly insert the card into a contact reader and copy all of the information available as free-read (the CHUID, the security object, the Card Capability Container, and the certificates) over the contact interface. 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 their PIV Card and enter their 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 readable PIV data objects, including the CHUID.

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. 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.

4.7 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 attack vectors 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 CHUID-based authentication, but is not able to create a clone that would succeed in PKI or CAK authentication mechanisms.

The PIV Card mitigates the risk of electronic cloning by providing the PKI and CAK alternative mechanisms. It is strongly recommended that agencies use cryptographic challenge/response methods instead of the CHUID authentication mechanism (see the Recommendation in Section 4.9).

4.8 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 an asymmetric signature field. Electronic counterfeiting will be extremely difficult if CHUID signature verification is

done, although signature verification is not required by FIPS 201. Moreover, since many counterfeit CHUIDs may be presented while an attacker probes for a valid counterfeit CHUID, the PACS should employ methods to detect, alarm, and block repeated unsuccessful CHUID presentations.

4.9 Other Threats

The PIV System and PACS 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: This section emphasizes the technical risks that remain with the CHUID authentication mechanism. If the CHUID authentication mechanism were implemented without restriction, operational risk would increase as the value of targets and the availability of cloning and counterfeiting tools increase. NIST therefore recommends that the CHUID authentication mechanism be implemented in only two situations: 1) access control points separating two areas at the same impact level, either Controlled or Limited; and 2) combined with the VIS authentication mechanism at access points between Unrestricted and Controlled areas. See Section 7 for further detail. NIST further recommends that the asymmetric CAK authentication mechanism be used instead of the CHUID authentication mechanism to the greatest extent practical.

5. Limitations of Legacy Physical Access Control Systems

FIPS 201 imposes specific requirements for the PIV card interface and reader/controller/PACS server processing to improve identity authentication. Technically, some of these requirements will present 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 FIPS 201 requirements differ from the capabilities of existing legacy systems.

5.1 Cardholder Identification

Legacy PACS deployed in Federal government facilities use legacy cards with data formats that are often proprietary to the specific enterprise. Most of the installed 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 systems but they are not necessarily interoperable.

A legacy 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. FIPS 201 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 to interface with and use the capabilities of the PIV Card, which serves to verify identity.

5.2 Door Reader Interface

Legacy PACS readers come in varying configurations and offer multiple interface options for the card and the Controller. FIPS 201 standardizes the use of the ISO/IEC 14443 contactless interface for the 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 FIPS 201 Evaluation Program (<http://fips201ep.cio.gov/>), which defines tests and maintains a list of validated products. Not all existing PACS use this interface, so some agencies may have to plan to migrate from their existing environment to the ISO/IEC 14443 conformant interface. Alternatively, an agency may choose to migrate to the contact interface based on ISO/IEC 7816.

The interface from the Door Reader to the Controller also comes in different configurations. FIPS 201 does not specify which protocols can be used for this interface, provided the necessary data can be communicated to the Controller. Typical legacy implementations support transmitting a small amount of data (on the order of 10 to 15 bytes), but FIPS 201 defines data elements which are much larger. Therefore, depending on the agency's implementation strategy, an upgrade to the Door Reader to Controller interface may also be required. Note that any change to this interface may also necessitate changes to the physical wiring and cabling infrastructures.

5.3 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 its use is limited to the local site. FIPS 201 provides interoperability requirements for a new generation of identity management technology for building access. FIPS 201 and its supporting special publications define the credential data model and the card-to-reader interface, and also provide requirements for implementing the use of digital certificates in building PACS, much as they are used in secure information systems.

FIPS 201 added a standardized contactless and contact interface, biometric fingerprint, and cryptography to the credential that could be used to attain a higher level of identity authentication assurance. The contactless interface and the capability to perform bi-directional data communication are two features that are fundamental to the deployment of secure building access. Adding cryptography to the credentials permits agencies to

validate the data objects on the card and authenticate the cardholder. Adding credential expiration and on-line credential validation requirements also strengthens access control decisions. At the same time, FIPS 201 provided the opportunity to migrate building access systems from LITTLE OR NO confidence assurance levels to VERY HIGH confidence assurance levels. Existing PACS need to be upgraded to take advantage of these features and functions, in coordination with the following guidelines and authorities:

- + FIPS 201 assurance levels
- + Department of Justice Vulnerability Assessment Report of Federal Facilities
- + OMB M-04-04, E-Authentication Guidance for Federal Agencies.

FIPS 201 redefines the requirements for building access in a fundamental way: instead of each facility issuing an access card solely for that facility's defined 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 inter-agency interoperability and the credential has been issued to the user as part of the FIPS 201 identity management process.

5.4 Legacy Wiring

Selecting a particular reader type and its interface with the Controller requires careful attention to legacy wiring. Existing wiring should be assessed for its ability to meet the requirements of new readers and Controllers. The existing wiring may be a limiting factor due to its age and original specifications. Many recently installed systems use CAT-5 cabling, which is 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.

5.5 Software Upgrades

Vendors may be able to upgrade their existing PACS software to minimize the hardware changes needed for an existing 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 insure that the software upgrade will have no adverse effect on the PACS system.

5.6 Legacy and PIV System Differences

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

- + 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 legacy tokens can be copied easily.
- + Even when two sites use compatible card technology, they assign site-specific identifiers to cards. 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. Legacy PACS typically 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

⁵ to meet their user base requirements.

- + Legacy PACS control expiration of credentials through an expiration date stored in a site database. 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 database for the legacy PACS.
- + Use of PINs, PKI, and biometrics with legacy PACS is 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 the requirements of other sites.

FIPS 201-conformant PACS eliminate or substantially reduce each of these limitations, relative to legacy PACS installations.

⁵ Corporate 1000®: The Corporate 1000 Program allows the manufacturer to provide end-user customers with a 35-bit card format that can provide the end-user with just over 1,000,000 individual card numbers within the assigned format.

6. 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 2, “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 department and agencies to improve identification and authentication of Federal employees and contractors requiring access to Federally controlled facilities through the widespread application of FIPS 201. The standard defines the characteristics of the Personal Identity Verification (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 Physical Access Control Systems (PACS) managed by the United States Government.

This section focuses on the benefits of electronic verification and direct integration with an electronic PACS. The visual (VIS) FIPS 201 authentication mechanism, which must be verified manually, is applicable to physical access control, as described in other sections of this publication. The FIPS 201 authentication mechanisms that can be performed electronically are CHUID, PKI, BIO, and BIO-A. NIST Special Publication 800-73-2, included by reference in FIPS 201, defines an additional, optional authentication mechanism, CAK.

6.1 Interoperability

In this publication, the term interoperability means the ability to use any PIV Card with any application performing one or more FIPS 201 authentication mechanisms. The data objects and keys placed on a PIV Card during issuance use specific cryptographic algorithms selected from the acceptable algorithms in NIST SP 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* [SP800-78]. A PACS application can interrogate the card to learn which algorithms are used. To attain full interoperability, a relying PACS application will support all acceptable algorithms, key lengths, and key material that could be presented, either by a PIV Card or by the PIV infrastructure, and a PIV Card will contain the asymmetric CAK and associated certificate.

The interoperability goal of the 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, in the form of a FASC-N identifier, to the relying party.

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

- + If the PKI authentication mechanism is performed by a PACS application, the PACS should support all of the asymmetric algorithms possible for the PIV Authentication Key as functionally required, as defined in Table 3-1 of [SP800-78], i.e., RSA 1024 (through 31 December 2013), RSA 2048, and ECDSA P-256, and the PACS should accept all valid PIV authentication certificates and require PIN entry.
- + If the CAK authentication mechanism is performed by the PACS, the accepted algorithms will be the same, but the PACS will accept only Card Authentication Key certificates and not require PIN entry.
- + If CHUID authentication with signature verification is performed, the PACS should support all of the signature algorithms and key size requirements as defined in Table 3-3 of [SP800-78]. If only CHUID authentication without signature verification of the CHUID is performed, no cryptographic operations are performed, and no cryptographic requirement is placed on the PACS.

- + PINs required for PIV authentication mechanisms are strings of eight or fewer decimal digits. For PKI, BIO, and BIO-A authentication mechanisms, a PIN entry device must acquire PINs from the cardholder and present them to the PIV Card to activate the card.

The PIV Implementation Maturity Model (PIMM) presented in Section 9 can be used to measure progress towards the interoperability goal. When PIV implementation is complete, all installed PACS readers will be approved products on the GSA HSPD-12 Evaluation Program Approved Products List, and each will be capable of one or more PIV authentication. At this time, any PIV Card will be able to perform any authentication mechanism it has been issued to perform at any PACS reader.

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, to the reader. A cardholder must authenticate *and be authorized* to be granted access. Authorization policies and mechanisms are outside the scope of the FIPS 201 standard.

Recommendation: To obtain full benefit from the PIV interoperability model, HSPD-12 Project Managers should understand the requirements for support of multiple cryptographic algorithms and ensure that relying systems have, or can be upgraded to have, capability to use all cryptographic algorithms that apply to the authentication mechanism(s) performed. Departments and agencies should procure and deploy only HSPD-12 products on the GSA HSPD-12 Evaluation Program Approved Products List, and can use the PIMM presented in Section 9 to measure progress.

6.2 Qualities of the Complete Implementation

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

1. Only PIV Card authentication mechanisms are used wherever they are applicable, in accordance with HSPD-12 and FIPS 201.
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.
4. All access control decisions are made by comparing an initial string of the FASC-N that includes Agency Code, System Code, and Credential Number against the Access Control List entries. See Appendix B for details and examples.
5. PIV authentication mechanisms are applied at impact-appropriate authentication levels.
6. Cryptographic and biometric authentications are applied widely in moderate- and high-impact use cases.
7. Agencies exhibit reciprocal trust in the process assurance of PIV issuers.
8. Major applications, and most new applications, accept PIV Cards as proof of identity for user registration/provisioning, user authentication, or both.

All of these qualities apply to both PACS and logical access control systems (LACS), although the authentication mechanisms will differ across applications.

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 Management Act (FISMA) [FISMA] mandated 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). FIPS 201 follows this methodology by implementing authentication mechanisms at three E-Authentication confidence levels (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, and Exclusion boundaries for appropriately protecting facility assets or resources.

Interoperability of PIV Cards and FIPS 201 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 PIV issuers 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 FIPS 201, and supported by the Certification and Accreditation (C&A) process methodology described in NIST SP 800-79. Trust is built when the technical standard is thorough, unambiguous, and grounded in practical requirements; when the conformance and audit processes are documented, trained, and uniformly practiced; and when positive PIV System audit results are available to the community of relying parties.

Recommendation: 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 eight 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.

6.3 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 a standardized, audited process, which will exceed the best practice level for low- and moderate-impact applications today, and equal best practice reached for high-impact applications. Authentication assurance will be improved.
- + 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 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 and tightly coupled 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 on-line 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 (one, two, or 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.⁶ In the complete PIV System, the marginal cost for biometric enrollment to the application owner, relative to other authentication mechanisms, is near zero, enabling many more applications to gain the benefits of biometric authentication.

Recommendation: 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 enrollments that are performed automatically by provisioning from the PIV issuance system.

6.4 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 can be achieved by PACS, and should therefore be supported by PACS upgrades and new PACS procurements:

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: 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 among PACS system elements (e.g., replacing Wiegand-style signaling with TCP/IP networking).

⁶ [FIPS 201] Section 4.4.1 states that “In cases where there is difficulty in collecting even a single fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.”

7. Authentication and Assurance

FIPS 201 defines identity authentication mechanisms and assigns assurance levels for each mechanism. In the context of this document, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV Card. The degree of confidence achieved in the cardholder’s identity is referred to as the authentication assurance level. The four E-Authentication assurance levels are⁷:

- + Level 1: LITTLE OR NO confidence
- + Level 2: SOME confidence
- + Level 3: HIGH confidence
- + Level 4: VERY HIGH confidence

FIPS 201 uses only E-Authentication assurance levels 2, 3, and 4.

Once an agency determines the assurance level required for its PACS application, the appropriate authentication mechanisms can be implemented. The authentication mechanisms in FIPS 201 are not an exhaustive list of all possibilities, so this section provides additional options for agencies. This section includes discussion of each authentication mechanism and assigns an appropriate assurance level.

7.1 PACS Authentication Mechanisms

FIPS 201 defines a set of authentication mechanisms for PACS applications. These mechanisms are derived from mandatory PIV Card elements. These mechanisms range from the most basic visual inspection of PIV Cards to fully automated electronic authentication. Additional mechanisms can also be derived from optional PIV Card elements. An expanded view of assurance levels is provided in considering the variety of attended and unattended PACS authentication mechanisms that are possible as the PIV Card is integrated into the systems. The expanded view takes into consideration the PACS operational environment of the Controlled, Limited, and Exclusion areas. The expanded view also gives particular focus and allowance to assurance levels defined as LITTLE OR NO confidence. Table 7-1⁸ provides the association between the PACS-Identity Authentication Assurance Levels and authentication mechanisms.

Table 7-1. Expanded PACS Assurance Levels

PACS-Identity Authentication Assurance Level	Applicable Authentication Mechanism
LITTLE OR NO confidence	Legacy Proximity, Magnetic Stripe
SOME confidence	VIS, CHUID, CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI

⁷ Levels 1, 2, 3, and 4 refer to levels in OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies,” dated December 16, 2003.

⁸ An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level. Each authentication mechanism described in the table can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the department or agency’s network infrastructure.

7.1.1 Legacy Proximity or Magnetic Stripe Authentication

Legacy proximity and magnetic stripe authentication are not PIV authentication mechanisms, but when used in conjunction with PIV mechanisms, there is a strong potential for “collisions”. Proximity and magnetic stripe card technology read a number from a card and send it to the Controller. The Controller compares this number against its database to make the access control decision. If a legacy system does not include an agency code in the numbers compared, an out-of-agency cardholder may be mistakenly accepted as an authorized site user. Refer to Appendix B for additional details. Moreover, proximity and magnetic stripe cards are easily counterfeited.

7.1.2 Visual (VIS) Authentication

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 training, skill, and diligence of the guard (to match the face in spite of changes in beard, mustache, hair coloring, eye glasses, etc.)—counterfeit IDs and banknotes pass visual inspections every day. 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 feature(s).

7.1.3 CHUID Authentication

The CHUID, as defined in FIPS 201, is one of the data objects on PIV credentials. The CHUID includes a Federal Agency Smart Credential-Number (FASC-N) data element that uniquely identifies 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.

The CHUID is completely standardized by FIPS 201; therefore, a CHUID data object can be counterfeited easily with the exception of the issuer signature. A counterfeit CHUID would not possess a valid issuer signature. The CHUID is a free read object on the PIV Card; therefore, it can be read or cloned easily. Because of the risk of CHUID counterfeiting or cloning, the CHUID authentication mechanism, used in isolation, provides a confidence level that is comparable to proximity cards in widespread use today. However, if the CHUID signature validation is performed, the PACS can be sure the CHUID came from a valid issuer. In addition to integrity, standardization of the CHUID authentication mechanism also provides government-wide interoperability.

7.1.4 Card Authentication Key (CAK) Authentication

The CAK is an optional key that may be present on any PIV Card. As the name implies, the purpose of a CAK authentication mechanism is to authenticate the card and therefore its possessor. This may also be viewed as one-factor authentication of the cardholder, since the person in possession of the card may successfully authenticate.

The CAK is unique among the PIV keys in several respects: 1) the CAK may be used on the contactless or contact interface for challenge/response authentication; 2) the use of the CAK does not require PIN entry; and 3) the CAK on a specific card may use any of the symmetric or asymmetric encryption algorithms permitted for this key by NIST SP 800-78-1. Points (1) and (2) were intended to allow the CAK to be used for one-factor authentication to PACS readers. CAK authentication mechanism examples are given in SP 800-73-2, Part 1, Appendix B.

Due to the optionality and variability described, unrestricted CAK authentication will not scale to an interoperable authentication mechanism across agencies. For this reason, NIST recommends that the asymmetric CAK be encouraged as the interoperable, single-factor PIV authentication mechanism.

7.1.5 PIV Authentication Key (PKI) Authentication

PACS may be designed to perform PKI-based authentication using PIV Authentication Key (PKI). Use of the PKI provides two-factor⁹ authentication, since the cardholder must enter a PIN to unlock the card in order to successfully authenticate.

When using PKI authentication, a PACS requires the ability to determine or check the validity of certificates at the time an individual presents his or her card to a card reader. This may be done on-line in real-time, or it may be implemented by pre-validating the certificates and caching the results. Section 7.4 specifies procedures for performing PKI-based authentication under the assumption that only individuals who are pre-enrolled will be granted access.¹⁰ Section 7.5 further describes the caching status proxy.

7.1.6 BIO Authentication

PACS may be designed to perform biometric authentication using the fingerprint information stored on the PIV Card. The biometric on the PIV Card is signed by the issuer, so the authenticity of the biometrics can be checked by the PACS. The biometric on a PIV Card is PIN-protected, so the cardholder must be present to release the biometric information. Verification of the signature on the biometric data object, and matching of the reference biometric template with the sample biometric template, are performed by the biometric reader.

Recommendation: A biometric reader should *always* verify the asymmetric signature, and do path validation, before performing a match. Otherwise, the result of the match should not be trusted.

7.1.7 BIO-A Authentication

This 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.

7.2 Multi-Factor Authentication

The VIS, CHUID, and CAK authentication mechanisms provide one-factor authentication, which is the possession of a PIV Card. VIS provides weak one-factor authentication since the card validation is subjective. CHUID also provides weak one-factor authentication since it could be cloned or counterfeited (in absence of signature validation) easily. The PKI authentication mechanism provides two-factor authentication since it requires possession of the PIV Card and knowledge of the PIN. The BIO and BIO-A mechanisms provide multi-factor authentication (under the assumption that a copy of the biometric has not been obtained by an attacker, and copied onto a counterfeit card; this attack can be prevented by combining PKI and BIO). The BIO and BIO-A mechanisms require a PIV Card, knowledge of a PIN, and live fingerprint. The next section describes the use of multi-factor authentication in the PACS environment.

7.3 Selection of Authentication Mechanisms

There is no simple one-to-one mapping between the Facility Security Level (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 have no high-value assets. 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 perimeters established around assets or resources. Following [PHYSEC], this report assumes that most facilities

⁹ Two-factor authentication is a system wherein two different methods are used to authenticate. An example of two factor authentication is a verification of something you have and something you know. Using two factors as opposed to one delivers a higher level of authentication assurance.

¹⁰ Pre-enrolling a certificate is not the same as pre-authorizing the identity for access. Pre-enrolling means only that a valid identity is known to the PACS. Authorization decisions for known identities are made separately.

can identify and categorize PACS perimeters as protecting Controlled, Limited, or Exclusion areas, corresponding generally to LOW, MODERATE, and HIGH impact assets or resources.

Figure 7-1 illustrates the application of the authentication mechanisms in FIPS 201 to the individual areas.

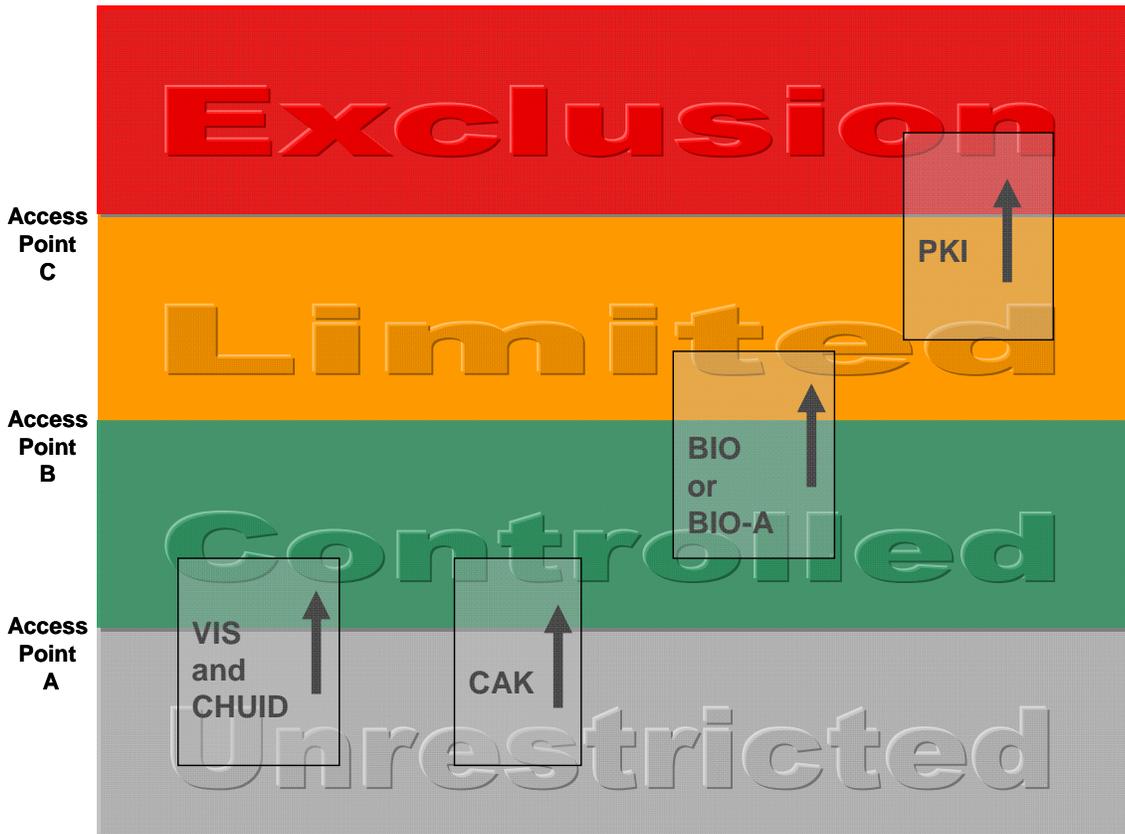


Figure 7-1: Perimeters and Authentication Mechanisms

Figure 7-1 shows the FIPS 201 authentication mechanisms applied to perimeter crossings between areas of different impact levels. The figure should be interpreted with the following notes:

1. “VIS and CHUID” means a combined authentication mechanism, in every instance performing visual inspection of the PIV Card and CHUID authentication, at the same access point.
2. Authentication mechanisms at one level in Figure 7-1 may be used at lower levels, but not the reverse. Thus, any of the mechanisms shown in Figure 7-1 are possible at Access Point A; BIO, BIO-A, and PKI are possible at Access Point B; only PKI is possible at Access Point C.
3. In a particular facility, the authentication mechanisms applied at enclosing perimeters of different impact levels should be distinct. For example, if PKI is applied to enter an Exclusion area, it should not be applied to enter the enclosing Limited or Controlled areas, and if BIO or BIO-A is applied to enter a Controlled area, it should not be applied to enter an enclosed Limited area.
4. 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 access points should combine BIO or BIO-A with PKI. The term “combine” means that both authentication mechanisms must successfully authenticate the presenting person, at the same access point, before access is permitted.
5. 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 7-1, as well as the CHUID authentication mechanism without VIS.

6. Within an Exclusion area, an access point to an adjacent area at the same impact level may employ CAK, BIO, BIO-A, or PKI.
7. In most cases, Figure 7-1 and these notes allow some flexibility in the selection of specific authentication mechanisms. A decision should be made based on the local security policy and operational considerations.

Note (1) ensures that the CHUID mechanism is combined with VIS where impact level escalation occurs, mitigating the risks described in Section 4.

Notes (2) and (3) ensure that assurance level ordering is preserved, with higher authentication assurance mechanisms employed at higher impact levels.

Notes (3) and (4) 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 (5) and (6) add some flexibility in the case of discretionary access control among areas at the same impact level.

The authentication methods in Figure 7-1 apply at all Threat Condition levels. At Threat Condition Orange or Yellow, the facility should employ only the Exclusion entry methods (PKI and BIO or BIO-A) at all perimeters. At Threat Condition Blue or Green, the facility should employ the entry methods at each perimeter as shown.¹¹

When the Threat Condition level increases, some access points may be closed. Access points that remain open should be capable of the required authentication mechanisms at the elevated Threat Condition level.

7.4 PACS Enrollment

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 Card holders, or all PIV Card holders sponsored by a specific agency or bureau (see Appendix B). If authorization is granted to specific individuals, information about the cardholder (specifically, at least their FASC-N) must be added to the PACS Server's authorization database.

If on-line credential validation is performed by the PACS at the time of each authentication (see Section 7.5), the PACS could store no 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, SOME confidence authentication is sufficient, the CAK certificate may be used. Where at least two-factor, HIGH or VERY HIGH confidence authentication is required, the PIV Authentication Key certificate should be used. Enrollment using a caching status proxy should collect and store information required for all FIPS 201 authentication mechanisms needed in the event of increased Threat Condition level.

Recommendation: When a card is terminated, the PIV card issuer must revoke all valid authentication certificates for the PIV Card. The authentication certificates include the PIV Authentication Key certificate and the Card Authentication Key certificate (if present).

When the individual is enrolled using a caching status proxy, the enrollment station obtains the PIV Authentication or asymmetric Card Authentication Key certificate from the PIV card, validates the certificate, checks the certificate revocation, and sends a challenge to the card to verify that the card 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).

¹¹ Note that at High Threat Conditions the security officials should consider closing down the perimeter if appropriate authentication assurance mechanism is not available.

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 re-validate all of the certificates in its database and rescind the access privileges of any individual whose certificate has expired or has been revoked. Re-validation should be performed by the caching status proxy at least once per day.

When an individual presents his or her PIV card to a door reader, the door reader obtains the authentication certificate from the card, sends a challenge to the card, and then uses the public key in the certificate to verify the response to the challenge.

Recommendation: The CHUID may be collected at enrollment, but it should be treated as if it were a password for purposes of retention, i.e., hashed, the hash stored, and the CHUID deleted. A stored CHUID presents risks similar to a stored password; it can be copied and used to gain access. Data elements may be extracted from the CHUID and retained (e.g., the FASC-N, Data Universal Numbering System [DUNS] Number, and Global Unique Identifier [GUID]), and a retained hash is sufficient to enable verification. *NIST strongly recommends against the storage of complete CHUIDs in relying systems.*

Recommendation: PKI and asymmetric CAK authentication mechanisms should be implemented by a PACS reader capable of full certificate path validation, either on-line or using a caching status proxy. If a caching status proxy is used, the certificates should be captured when the PIV card is enrolled to the PACS.

7.5 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 terminated. On-line credential validation is extremely valuable to relying parties because it retrieves the most up-to-date credential status, and can block fraudulent use of a PIV card that has been terminated as lost or stolen. Credential validation is required by the PKI authentication mechanism, and can be implemented for BIO, BIO-A, CAK, and CHUID authentication mechanisms.

FIPS 201 Section 5.4.5 states “The presence of a valid, unexpired, and unrevoked PIV authentication certificate on a card is proof that the card was issued and is not revoked.” FIPS 201 Section 6.2 further says “The status of the PIV authentication certificate is directly tied to the status of all other credential elements held by the card.” These statements imply that PIV credential validation may be done by performing path validation (see below) on the PIV Authentication Key certificate or Card Authentication Key certificate.

Since the expiration date of a PIV Card is contained in the CHUID, a relying party can determine if a PIV Card has expired by reading the CHUID, verifying the CHUID’s signature, then extracting and comparing the expiration date with the current date received from a trusted source.

On-line, on-demand credential validation may not always be practical, due to absence of network connectivity to the PIV card issuer, or inadequate response time. In these circumstances, it may be possible for PIV Cards of interest to be registered with a caching status proxy. The caching status proxy can poll the status of all registered cards periodically, and cache 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: On-line credential validation should be implemented for all of the FIPS 201 authentication mechanisms whenever possible. It is especially important when the one factor, non-biometric mechanisms (CHUID, CAK) are used, because they could be exploited by simple possession of a misappropriated PIV Card. Caching techniques can be used to implement credential validation when on-line, on-demand credential validation is not possible. It is also recommended that the cached data be protected against tampering.

Data objects read from a smart card by a reader should not be fully trusted as authentic (i.e., produced by a PIV Card issuer) and unmodified until their asymmetric signatures are verified. Most data objects in a PIV card-application have embedded asymmetric signatures (i.e., all certificates, the CHUID, fingerprint template, facial

image, and security object). The Printed Information Buffer must be signed by the Security Object, and the Card Capability Container may be signed by the Security Object.

Path validation (or *trust path validation*) is the process of determining that a chain of signatures, beginning with a signed object and continuing through the sequence of signing certificates to a *trust anchor certificate*, verifies completely and all certificates are valid. A trust anchor certificate 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.¹²

The PKI authentication mechanism requires path validation to be performed on the PKI Authentication Key certificate. The BIO, BIO-A, CHUID, and CAK authentication mechanisms do not require path validation to be performed, however. 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 rogue Certificate Authority. BIO authentication would succeed with this counterfeit PIV Card, and the forgery would not be detected.

Because credential validation is a special case of path validation, both services can be economically implemented by a single PACS service component.

Recommendation: Path validation should be performed on all signed data objects required by the authentication mechanism in use. Path validation should employ on-line credential validation where possible, or cached certificate status where on-line certificate validation is not possible.

7.6 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 will determine if further investigation is warranted and if the PIV Card issuer should be asked to terminate the PIV Card. In the event of PIV Card termination, the PIV Card issuer will request the Certification Authority to revoke the PIV Authentication Key certificate and the Card Authentication Key certificate (if present on the PIV Card).

¹² If a data object is not used in the authentication mechanism being performed, path validation need not be performed on the data object's asymmetric signature for the authentication result to be fully trusted.

8. PACS Use Cases

HSPD-12 requires that the 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. The PIV credentials, as defined in FIPS 201, offer a range of security which is discussed in Section 7. 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 building 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 Determination¹³ to derive the security level required 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 asset 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 which 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 its 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”.

8.1 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 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, MEDIUM, or HIGH value assets to protect. Facilities evaluated at FSL I or II may not implement PACS and may continue without PACS. Facilities

¹³ FSL determination is criteria for categorizing federal office facilities into five security levels with the number of federal employees housed and the size of the facility being prominent criteria.

evaluated at FSL III or above should implement PACS. These facilities may have general access area 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 8-1 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 Controlled, Limited, or Exclusion area and the appropriate authentication mechanisms should be selected from Figure 7-1.

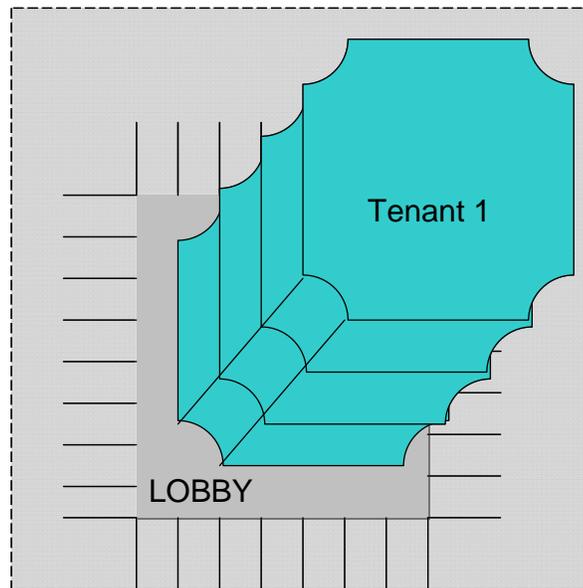


Figure 8-1: Single-Tenant Facility

8.2 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 (aka, 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.

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 Controlled area authentication mechanism, but the individual agency should implement Exclusion area authentication mechanism for access to their 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 their own Controlled, Limited, and Exclusion areas and employ appropriate FIPS 201 authentication mechanisms as in Figure 7-1. 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 8-2 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.

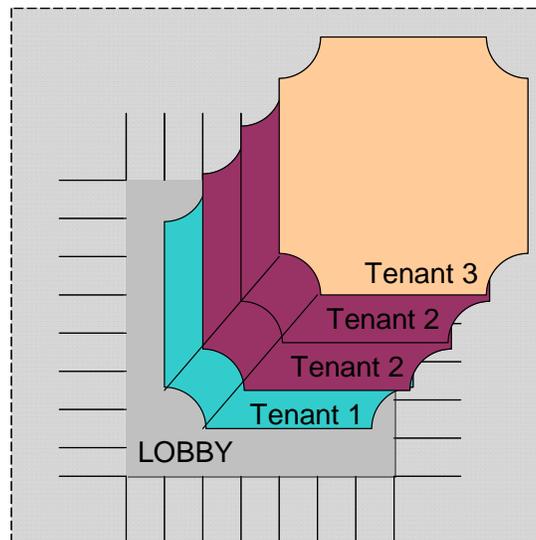


Figure 8-2: Multi-Tenant Facility

8.3 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. 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, and Exclusion areas and then evaluate if the facility PACS will accommodate their security needs. Each Federal government tenant should ensure an appropriate PIV authentication mechanism from Table 7-1 is implemented for its designated areas. If the facility PACS cannot, they 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 9.

8.4 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 employee, 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 the campus visitors, while some may be specialized spaces such as a high security-lab or chemical storage 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, and 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, and 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. Other authentication mechanisms, such as PIN-to-PACS or iris scan, may be considered but are outside the scope of this document.

8.4.1 Level I or II Campus Facility

Figure 8-3 depicts a security posture of a Level I or II Campus Facility. It includes one or more Controlled areas which are available to authorized personnel. Since a Level 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 area would be an appropriate countermeasure for security at this facility. VIS and CHUID together or CAK are the two recommended authentication mechanisms in this environment. Note that these authentication mechanisms validate something you have (one-factor authentication).

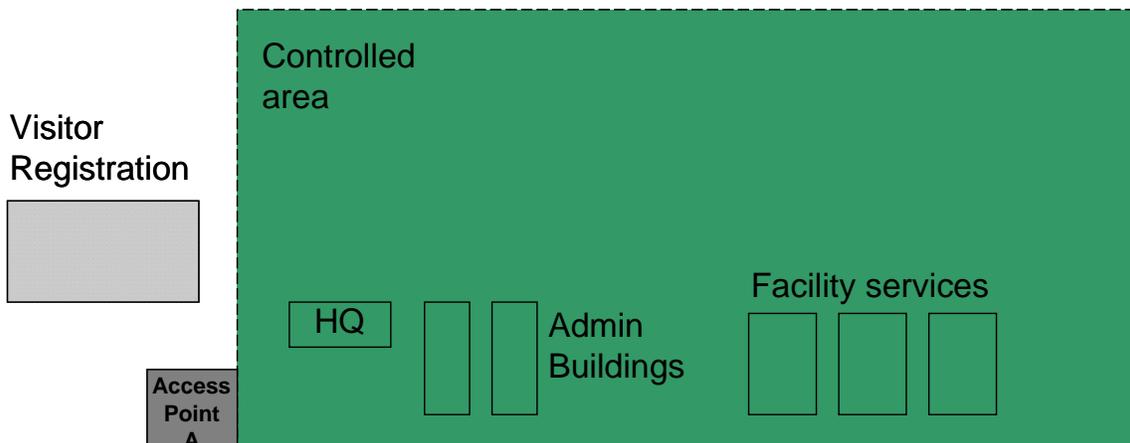


Figure 8-3: Level II Campus Facility

8.4.2 Level III Campus Facility

Figure 8-4 depicts a security posture of a Level III Campus Facility. It includes one or more Controlled areas as well as Limited areas which are restricted to specific group of individuals. Since a Level 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, BIO-A, or PKI authentication mechanisms would be an appropriate countermeasure for the Limited area. Note that these authentication mechanisms validate something you are or something you know (another factor in authentication).

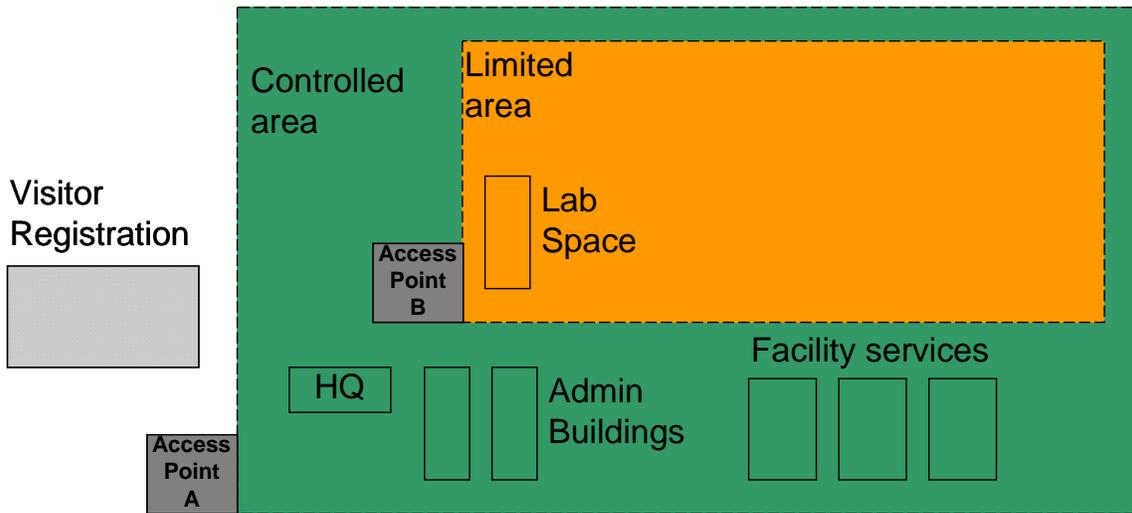


Figure 8-4: Level III Campus Facility

8.4.3 Level IV or V Campus Facility

Figure 8-5 depicts a security posture of a Level IV or V Campus Facility. It includes one or more Controlled areas, Limited areas, and Exclusion areas which are restricted to specific group of individuals.

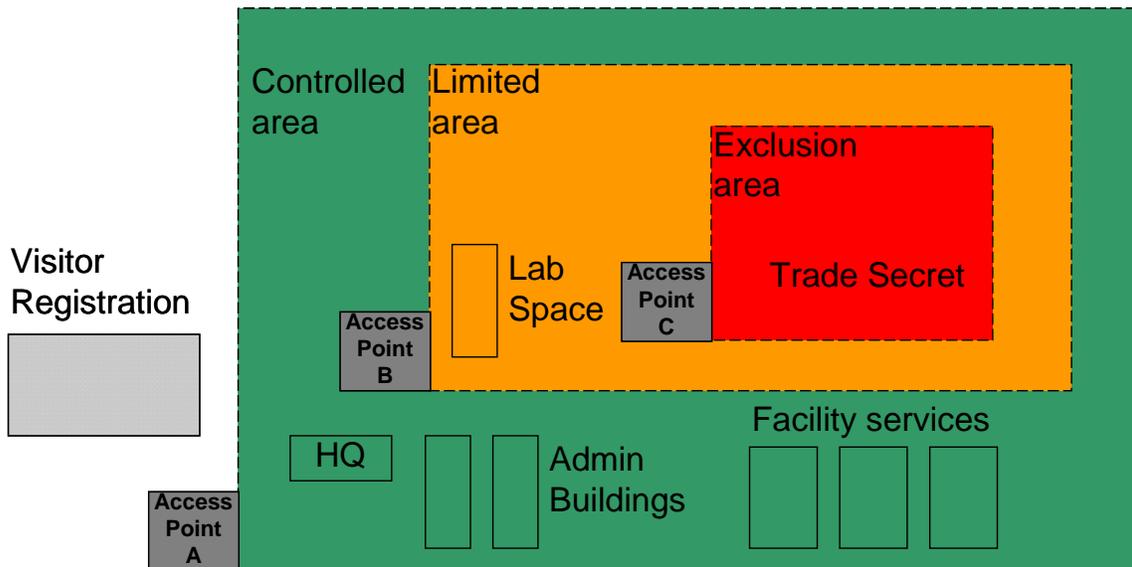


Figure 8-5: Level IV or V Campus Facility

Although there is not a simple one-to-one mapping between FSLs and PACS Identity Authentication Assurance Levels at access control points, generally higher-risk areas will need stronger identity assurance. Since a Level 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 area. Note that the entire facility does not need the highest level of confidence in the identity of the cardholder. For access to the Exclusion area, three-factor authentication should be achieved. This is done by nesting perimeters such that cumulative effect of authentication is realized. As shown in Figure 7-1, cardholder is authenticated using BIO or BIO-A authentication mechanism to enter

Limited area and is authenticated again using PKI authentication mechanism to enter Exclusion area. Note that these authentication mechanisms provide for multi-factor authentication.

8.5 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 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 FIPS 201 authentication assurance levels required for access to its space (see Figure 7-1). 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 7-1 are implemented for its determined areas.

8.6 Role-Based Authentication

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 access control decisions by evaluating the information on a presented PIV card against a set of access control policy 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 authentication, group permissions will usually be derived from off-card information.

Recommendation: 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. Currently, the only practical exceptions are broad discriminators (e.g., based on agency or bureau). In the future, standardized role information may be available on-card, especially for Emergency Response Officials or Continuity of Operations (COOP) procedures.

8.7 Temporary Badges

HSPD-12 mandated the issuance of electronic identity credentials to Federal employees and contractors. OMB Memorandum M-05-24 clarified the eligibility requirements for PIV Cards to temporary Federal employees and contractors, by requiring PIV Card issuance to all Federal employees and contractors who require access to Federal facilities or information systems for six months or longer. Agencies are permitted to issue non-PIV Cards to individuals with access of 6 months or less. Ineligible personnel (i.e., visitors who are neither Federal employees nor contractors), temporary personnel requiring access less than 6 months, eligible personnel who, as a matter of agency policy, are not issued PIV Cards, and PIV cardholders who have forgotten their cards comprise the people who could receive temporary badges. 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 OMB 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 HSPD-12 readers and authentication mechanisms (especially CHUID and CAK for physical access).
- + The assignment of FASC-N unique identifiers to temporary badges, to foster interoperability with HSPD-12 readers.
- + The suitability of contactless-only temporary badges, for physical but not logical access.
- + The performance, cost, and security tradeoffs between disposable and reusable temporary badges.
- + The importance of VIS authentication mechanisms with temporary badges.

Many approaches to temporary badges are possible. A two-tier approach could become commonplace. A paper-based tier would provide disposable paper badges, with or without printed ID photos. A smart-card tier would issue a reusable card with greater functionality, possibly using PIV Card stock, with capability for physical and logical access, interoperability with HSPD-12 readers and use cases, for periods of weeks to six months.

9. 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.

9.1 Project Planning

Planning for a migration to PIV PACS should be viewed as an opportunity to modernize legacy PACS. Given the threat environment, as described in Section 4, migrating to PIV PACS enhances security, fosters trust among agencies, and creates cost efficiencies. This section provides a strategy for developing migration plans, as shown in Figure 9-1.

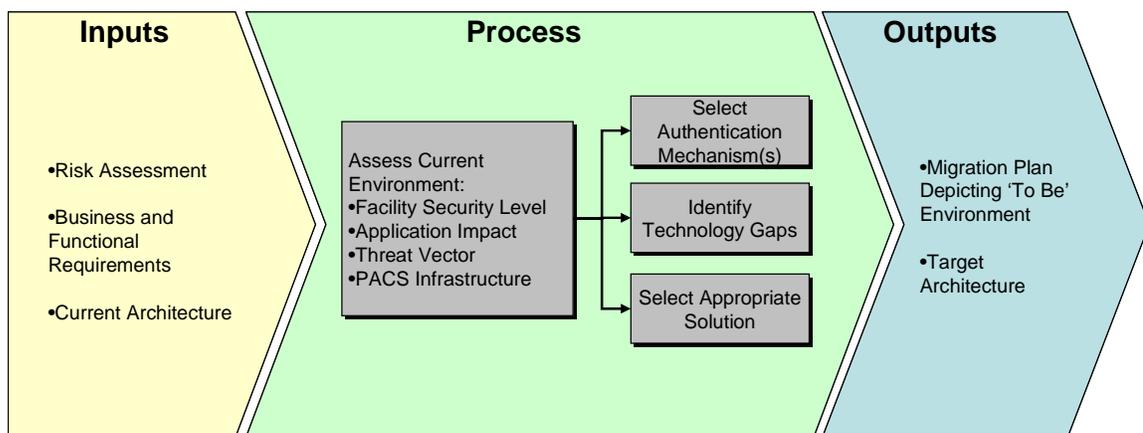


Figure 9-1: Migration Strategy

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.

9.2 Risk Assessment

Vulnerability analyses and 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 4 provides threat 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 following threats:

1. Counterfeiting
2. Skimming
3. Sniffing

4. Social engineering
5. Cloning.

9.3 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. The result is today's PACS environment, which is site-specific and hardly interoperable with other agency implementations. HSPD-12 adds two requirements to these implementations, namely enhanced security and interoperability. Interoperability means that 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 6 provides characteristics of a future 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.

9.4 Develop Migration Plan

Developing a migration plan requires a vision for PIV-enabled PACS operations. Specifically, a new business process needs to be charted 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 information technology (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 (CPIC) process to acquire, use, maintain and dispose of information technology. In particular, the Clinger-Cohen Act (CCA) 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 7 of this document. Once authentication mechanism(s) 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 8 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 6.2. For this, guidance is provided in the following section to enable agencies to progress in stages.

9.5 Migration Strategy & Tactics

Continuity of operations planning is essential to the success of a migration from legacy PACS to HSPD-12-compliant operation. 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.

- + 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.
- + Budget the project carefully. A complete PACS system replacement may look better than an upgrade if the budget and business case are well-constructed.
- + 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.
- + Develop a relationship with a senior partner. A “senior partner” should be farther along in implementation, or have deeper expertise, than your organization.
- + 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 have a plug-in for contact card readers. The agency may have a choice to add contact readers without replacing the reader infrastructure.
- + Use the extra bandwidth to support remote monitoring and diagnosis, off-loading of service elements, PKI credential validation, cryptographic key management, and so on.
- + Initially, buy multifunction readers that read legacy and PIV Cards and can perform all PIV electronic use cases—they can be used anywhere. The agency should design to the highest authentication assurance level that it thinks it may require in the future. Multifunction readers can also implement authentication mechanism agility required by changing Threat Conditions.
- + As experience and the number of deployed readers grow, select more restricted and cost-effective readers implementing just the required authentication mechanisms.
- + Avoid long-term, side-by-side operation of legacy and PIV technologies. Once PIV Cards have been issued to half the users, cut costs by aggressive completion of the migration.

9.6 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 PIV Implementation Maturity Model (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 7-1. An actual facility may map its perimeters onto one, two, or all three of these. Some facilities may have more than three enclosing perimeters, in which case two or more may be mapped onto a repetition of Controlled, Limited, or Exclusion, as necessary. Generally, the authentication mechanisms should be different at each of the enclosing perimeters. Each perimeter therefore adds to the security context of a granted access, with cumulative effect as an individual moves inward.

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. 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). Access to Exclusion areas may be gained by individual authorization only.

With this background, the following PIMM maturity levels begin by achieving some capability and experience with PIV-based PACS:

- + Maturity Level 1—Ad Hoc PIV Verification. A site has the ability to authenticate PIV Cards by performing required authentication mechanism(s) on an ad hoc, on-demand basis. For example, card and cardholder authentication is achieved with a handheld terminal or a specific PC, for special or occasional uses.
- + 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 legacy PACS credentials. A visitor registration procedure exists to accept PIV Cards and if necessary convert PIV authentication to a temporary legacy PACS credential.
- + 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 VIP visitors, for example. At Level 3, legacy PACS or badges are not acceptable for authentication to exclusion areas.
- + Maturity Level 4—Access to 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, legacy PACS or badges are not acceptable for authentication to Limited areas. BIO, BIO-A, or PKI are acceptable authentication mechanisms in Limited Areas for authorized PIV cardholders.
- + Maturity Level 5—Access to 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, legacy PACS or badges are not acceptable for authentication to Controlled 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-based authentication mechanisms. This capability may exist in parallel with legacy PACS, and after the Maturity 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 legacy 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 Maturity 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 appropriate¹⁴.

Maturity levels are progressive: for example, Maturity Level 1 must be achieved before Maturity Level 2 can be achieved. 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.

¹⁴ Note that some use of methods other than FIPS 201 authentication mechanisms will continue because not everyone is eligible or required to have a PIV Card.

10. Future Topics

This section describes advances in FIPS 201 and its associated document suite, and in the architecture and implementation of the PIV infrastructure, that are recommended to realize the full potential of the PIV System applied to PACS authentication.

10.1 Generalized Credential Identifier

FIPS 201-1 states that the CHUID data object contains the FASC-N data element “which uniquely identifies each card.” The FASC-N actually serves two purposes: 1) identifying a PIV Card (and by correspondence, the cardholder); and 2) binding PIV data objects to the same PIV Card, because the identical FASC-N is contained in the CHUID, the PIV Authentication Key certificate, the Card Authentication Key certificate, the fingerprint biometric record, and the facial image object.

Within the FASC-N, the fundamental card identifier is the (Agency Code, System Code, Credential Number) triple. Uniqueness of the triple is derived from a hierarchical approach to number assignment. The Agency Code field is statically assigned to a department, agency, or bureau through a registration process, and the assigned Agency Code values are listed in NIST SP 800-87. The PIV issuer for the registered department, agency, or bureau can, in turn, assign the System Code and Credential Number.

The FASC-N, as adopted and extended by FIPS 201, meets the objective of HSPD-12 to identify Federal employees and contractors. The success of the FIPS 201 technical standard has led other communities of interest to consider PIV-like identification systems. For some of these communities, the (Agency Code, System Code, Credential Number) triple is not an appropriate solution (because they are not agencies of the Federal government). Also, the data representation of the FASC-N was chosen for compatibility with legacy systems (fixed-length hexadecimal), and may not be optimal for binary identifier values prevalent in commercial systems today.

For these reasons, the CHUID data object also contains the GUID data element for future use. The GUID is a 16-byte, or 128-bit, binary field. It therefore improves on both the length and representation limitations of the FASC-N. Unfortunately, the GUID is only present in the CHUID, and does not serve to bind other data objects together. If the GUID were used to identify a PIV Card, the standard in effect would still require the FASC-N in the other data objects.

These issues lead to a number of questions. If a community outside the Federal government adopts PIV-like technology, what identifier format, registrar, and governance structure should they use? How could larger, binary identifiers be used with PIV-like technology? Could existing, standardized universal identifiers such as the UUID, IPv6 addresses, OpenID identifiers, or Object Identifiers (OIDs) be used in place of the FASC-N, in all of its uses? If non-Federal-government communities adopt identifiers other than the FASC-N, could FIPS 201 be modified to recognize multiple types of identifiers?

Recommendation: Agencies should collaborate to standardize an enhancement or replacement of the FASC-N that accomplishes both credential identification and object binding, and supports an extensible framework for subject identification.

10.2 Secure Biometric Match-On-Card

FIPS 201 defines the biometric authentication mechanisms BIO and BIO-A. According to these definitions, the PIV reference template object is stored on the PIV Card during issuance. When a PIV Card is inserted into a contact biometric reader and the PIN has been entered, the biometric reader can read the reference template object from the PIV Card. The subject presents a finger to a fingerprint scanner on the biometric reader, and the reader acquires a sample template from the scan. The reader then performs the matching algorithm comparing the reference and sample templates, and produces a Yes or No response.

Biometric Match-On-Card (BIO-O) is similar, but performs the match on the PIV Card instead of on the reader. To do this, the sample template must be sent to the reader, but the reference template need not leave the PIV Card. Secure Biometric Match-On-Card combines Biometric Match-On-Card with a secure communication protocol that encrypts the sample template as transmitted into the PIV Card, and signs a Yes or No result returned to the reader.

Secure Biometric Match-On-Card (SBMOC) has important benefits over Match-Off-Card. Communication of sensitive biometric data is always encrypted and can be decrypted only by the PIV Card. The subject's reference template is never released from the PIV Card. The biometric match is performed in the trusted execution environment of the PIV Card. ISO/IEC 7816 secure messaging commands and asymmetric cryptography mean that only the PIV Card can decrypt the biometric data and sign the result. Moreover, the cardholder PIN is not required to perform the transaction. Because of the secure communication protocol and no PIN requirement, SBMOC can be performed safely and faster over a contactless interface. Finally, because the match is performed on the PIV Card, the card knows and can use the result of the match.

NIST recently completed the Secure Biometric Match-On-Card Feasibility Study, as reported in NISTIR 7452 [SBMOC] and the companion MINEX II report [MINEXII]. The results of the SBMOC study show 17 cards successfully implemented the functionality and security requirements of the study, and met the 2.5 second transaction time goal. The MINEX II results indicate that one of the tested cards approached the accuracy of ANSI 378 matching algorithms, thereby exceeding the accuracy requirements of FIPS 201 as defined in SP 800-76-1. Three additional smart cards and Match-On-Card algorithms met some, but not all, of the criteria.

Recommendation: SBMOC should be pursued as a standard FIPS 201 authentication mechanism, especially for PACS. Assuming it is judged to be at least as trustworthy as PIN entry, SBMOC should be allowed to substitute for PIN to activate a PIV Card.

Appendix A—Recommendations

Section 2.2

Recommendation: PACS technology is undergoing rapid evolution as it incorporates powerful and inexpensive sensor, computing, and networking technologies. These trends will create many opportunities for enhanced capabilities, lower cost, and comprehensive system integration. Officials responsible for policies and operation of PACS should remain alert for new national, international, and industry standards, as well as new products, to maximize mission effectiveness.

Section 2.3

Recommendation: Agencies should utilize the higher authentication assurance offered by the PIV Card to counter physical threats to Federal government facilities resulting from misidentification. 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 4.9

Recommendation: This section emphasizes the technical risks that remain with the CHUID authentication mechanism. If the CHUID authentication mechanism were implemented without restriction, operational risk would increase as the value of targets and the availability of cloning and counterfeiting tools increase. NIST therefore recommends that the CHUID authentication mechanism be implemented in only two situations: 1) access control points separating two areas at the same impact level, either Controlled or Limited; and 2) combined with the VIS authentication mechanism at access points between Unrestricted and Controlled areas. See Section 7 for further detail. NIST further recommends that the asymmetric CAK authentication mechanism be used instead of the CHUID authentication mechanism to the greatest extent practical.

Section 6.1

Recommendation: To obtain full benefit from the PIV interoperability model, HSPD-12 Project Managers should understand the requirements for support of multiple cryptographic algorithms, and ensure that relying systems have, or can be upgraded to have, capability to use all cryptographic algorithms that apply to the authentication mechanism(s) performed. Departments and agencies should procure and deploy only HSPD-12 products on the GSA HSPD-12 Evaluation Program Approved Products List, and can use the PIMM presented in Section 9 to measure progress

Section 6.2

Recommendation: 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 eight 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.

Section 6.3

Recommendation: 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 fraction of PACS enrollments that are performed automatically by provisioning from the PIV issuance system.

Section 6.4

Recommendation: 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 among PACS system elements (e.g., replacing Wiegand-style signaling with TCP/IP networking).

Section 7.1.6

Recommendation: A biometric reader should *always* verify the asymmetric signature, and do path validation, before performing a match. Otherwise, the result of the match should not be trusted.

Section 7.4

Recommendation: When a PIV Card is terminated, the PIV Card issuer must revoke all valid authentication certificates for the PIV Card. The authentication certificates include the PIV Authentication Key certificate and the Card Authentication Key certificate (if present).

Recommendation: The CHUID may be collected at enrollment, but it should be treated as if it were a password for purposes of retention, i.e., hashed, the hash stored, and the CHUID deleted. A stored CHUID presents risks similar to a stored password; it can be copied and used to gain access. Data elements may be extracted from the CHUID and retained (e.g., the FASC-N, Data Universal Numbering System [DUNS] Number, and Global Unique Identifier [GUID]), and a retained hash is sufficient to enable verification. *NIST strongly recommends against the storage of complete CHUIDs in relying systems.*

Recommendation: PKI and asymmetric CAK authentication mechanisms should be implemented by a PACS reader capable of full certificate path validation, either on-line or using a caching status proxy. If a caching status proxy is used, the certificates should be captured when the PIV card is enrolled to the PACS.

Section 7.5

Recommendation: On-line credential validation should be implemented for all of the FIPS 201 authentication mechanisms whenever possible. It is especially important when the one factor, non-biometric mechanisms (CHUID, CAK) are used, because they could be exploited by simple possession of a misappropriated PIV Card. Caching techniques can be used to implement credential validation when on-line, on-demand credential validation is not possible. It is also recommended that the cached data be protected against tampering.

Recommendation: Path validation should be performed on all signed data objects required by the authentication mechanism in use. Path validation should employ on-line credential validation where possible, or cached certificate status where on-line certificate validation is not possible.

Section 8.6

Recommendation: 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. Currently, the only practical exceptions are broad discriminators (e.g., based on agency or bureau). In the future, standardized role information may be available on-card, especially for Emergency Response Officials or Continuity of Operations (COOP) procedures.

Section 10.1

Recommendation: Agencies should collaborate to standardize an enhancement or replacement of the FASC-N that accomplishes both credential identification and object binding, and supports an extensible framework for subject identification.

Section 10.2

Recommendation: SBMOC should be pursued as a standard FIPS 201 authentication mechanism, especially for PACS. Assuming it is judged to be at least as trustworthy as PIN entry, SBMOC should be allowed to substitute for PIN to activate a PIV Card.

Appendix B—PIV Uniqueness

All access control decisions are made by comparing an initial string of the FASC-N that includes Agency Code, System Code, and Credential Number against the Access Control List entries. The initial string requirement allows quick checks of large subsets (e.g., all PIV Cards issued to one agency, or to one site in one agency) without introducing dangerous collisions or ambiguities across agencies. In other words, an individual's FASC-N identifier is unique among all cardholders when the initial string of the FASC-N is used for comparison. There will be no collisions since all the cardholders will be assigned a unique number.

This restricts the access control comparison to an initial string of the Agency Code, System Code, and Credential Number, as represented in the FASC-N data element. For example, if the Credential Number is compared, the complete triple (Agency Code, System Code, Credential Number) must be compared. If the System Code is compared, the pair (Agency Code, System Code) must be compared. The Agency Code may be compared alone.

The initial string is defined as a string of binary coded decimal (BCD) digits, beginning with the high-order digit of the Agency Code and ending with the low-order digit of the Credential Number, and the string may contain any number (0 through 14) of BCD digits. Other representations of Agency Code, System Code, and Credential Number, for example binary representation, may be used 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.

B.1 Full FASC-N Comparison

The following table shows a successful match against an ACL pattern consisting of one specific (Agency Code, System Code, Credential Number) triple.

<u>MATCH</u>	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 (Agency Code, System Code, Credential Number) triple.

<u>NO MATCH</u>	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8367	8377
Credential Number	123456	123456

B.2 Partial FASC-N Comparison

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

<u>MATCH</u>	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8391	83xx
Credential Number	654321	xxxxxx

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

<u>NO MATCH</u>	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3628	3728
System Code	8377	83xx
Credential Number	123456	xxxxxx

The following table shows a disallowed pattern that is not an initial string of the (Agency Code, System Code, Credential Number) triple.

<u>DISALLOWED PATTERN</u>	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	37xx
System Code	8377	83xx
Credential Number	123456	xxxxxx

B.3 Isomorphic FASC-N Comparison

The following table shows a successful match against an ACL pattern, with the (Agency Code, System Code, Credential Number) triple and the upper and lower bounds of the ACL pattern represented in hexadecimal. The match succeeds because the presented triple is in the closed interval [LB, UB]. This example is the same as the MATCH example of A.2, with a shift in representation from decimal to hexadecimal.

<u>MATCH</u>	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 (Agency Code, System Code, Credential Number) triple and the upper and lower bounds of the ACL pattern represented in

hexadecimal. The match fails because the presented triple is not in the closed interval [LB, UB]. This example is the same as the NO MATCH example of B.2, with a shift in representation from decimal to hexadecimal.

<u>NO MATCH</u>	PIV Card FASC-N	ACL Pattern LB	ACL Pattern UB
Hexadecimal Value	21010BD3F280	21E9DBE03300	21E9E1D613FF

Appendix C—References

- [FACESTD] INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange.
- [FINGSTD] INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format.
- [FIPS 201] Federal Information Processing Standard 201-1, Change Notice 1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. See <<http://csrc.nist.gov/>>.
- [FISMA] Federal Information Security Management Act of 2002. See <<http://csrc.nist.gov/policies/HR2458-final.pdf>>.
- [GSA Evaluation Program] See <<http://fips201ep.cio.gov/index.php>>.
- [HSPD-12] Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
- [INCITS/M1-040211] ANSI/INCITS M1-040211, Biometric Profile-Interoperability and Data Interchange-Biometrics-Based Verification and Identification of Transportation Workers, ANSI, April 2004. See <http://www.incits.org/tc_home/m1htm/docs/M1040211.pdf>.
- [M-04-04] OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003. See <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.
- [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. See <<http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf>>.
- [M-07-06] OMB Memorandum M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials, January 2007. See <<http://www.whitehouse.gov/omb/memoranda/fy2007/m07-06.pdf>>.
- [MINUSTD] INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange.
- [PHYSEC] Field Manual 3-19.30. *Physical Security*. Headquarters, Department of the Army, United States of America. 8 January 2001.
- [SECTION508] 1998 Amendment to Section 508 of the Rehabilitation Act, 29 U.S.C. ‘ 794d, see <www.section508.gov>.
- [SKIMMER] How to Build a Low-Cost, Extended-Range RFID Skimmer, Ilan Kirschenbaum and Avishai Wool, Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15. Vancouver, B.C., Canada. 8 May 2006.

Appendix D—Abbreviations and Acronyms

ANSI	American National Standards Institute
BCD	Binary Coded Decimal
BIO	Biometrics
BIO-A	Biometrics with Attendant
BIO-O	Biometric Match-On-Card
C&A	Certification and Accreditation
CA	Certification Authority
CAK	Card Authentication Key
CCA	Clinger-Cohen Act
CHUID	Cardholder Unique Identifier
COOP	Continuity of Operations
CPIC	Capital Planning and Investment Control
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DUNS	Data Universal Numbering System
ECDSA	Elliptic Curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKIPA	Federal PKI Policy Authority
FSL	Facility Security Level
GSA	General Services Administration
GUID	Global Unique Identifier
HSPD	Homeland Security Presidential Directive
ID	Identification
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
kHz	Kilohertz
LACS	Logical Access Control System

MHz	Megahertz
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PACS	Physical Access Control System
PC	Personal Computer
PCI	PIV Card Issuer
PIMM	PIV Implementation Maturity Model
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RF	Radio Frequency
SBMOC	Secure Biometric Match-On-Card
SKI	Symmetric Key Infrastructure
SP	Special Publication
SSA	Social Security Administration
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Transistor-Transistor Logic
UL	Underwriters Laboratory
VIP	Very Important Person
VIS	Visual Inspection
VoIP	Voice over Internet Protocol