SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE ACCESS CONTROL COUNCIL GUIDEBOOK

Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems

A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements

Version 1.0

May 2019

A Guidebook to the 2018 Revision of the NIST Guidance SP 800-116 R1 by the Secure Technology Alliance Access Control Council

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

About this Document

This document:

- Is intended to identify the essentials for a successful deployment of a physical access control system (PACS) that complies with Federal Information Processing Standard (FIPS) 201.
- Is intended to provide a streamlined, practical, layman's version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116 R1. Although this guide follows the flow of the original document, some sections have been eliminated and content condensed, including the use of table formats to provide real-life PACS deployment recommendations based on the experience of industry professionals who have deployed Personal Identity Verification (PIV) credentials with PACS.
- Spans applications from a single door to complex multi-door, nested implementations that enable federal agencies to operate as government-wide interoperable enterprises. These guidelines contemplate a risk-based strategy for selecting appropriate PIV authentication mechanisms as expressed within FIPS 201.

SP 800-116 R1 states that many aspects of PACS are out of scope, including authorization (i.e., user access privileges), a critical security function. However, since PACS are typically procured to perform authorization and other security functions, this guide provides a holistic, real-world approach to implementing PACS with PIV. Although PACS are now considered IT systems, guidance cannot ignore that they are nevertheless a physical security system incorporating access control functionality.

Table of Contents

1 Introduction

In June 2018, the National Institute of Standards and Technology (NIST) released a revision of NIST SP 800-116: "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)." The revised document is called NIST SP 800-116 Revision 1: "Guidelines for the Use of PIV Credentials in Facility Access.'' NIST SP 800-116 R1 covers the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within Federal Information Processing Standard (FIPS) 201 and other related documents.

These PIV authentication mechanisms leverage the PIV card data elements contained within secure and hardware-protected data storage areas of the PIV smart card chip. The available authentication mechanisms provide options for the use of the PIV cards at access points to provide progressive levels of security for protecting personnel, resources and assets within facility security boundaries. The authentication mechanisms are managed and controlled by PACS incorporating PIV smart card readers at facility control points that may consist of secure doors, gates, and turnstiles.

NIST SP 800-116 R1 is a guidance document that includes supplemental reference material such as detailed technical concepts, processes, and policies that reference other NIST standards.

Sections 1 through 4 map directly to the associated sections in SP 800-116. Sections 5 and 6 provide supplementary information, helpful for implementation but not addressed in NIST SP 800-116 R1. The appendices also provide supplemental information and, in some cases, an explanation of key aspects addressed in this document.

NIST SP 800-116 R1 can be reviewed in its entirety at: https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final.

1.1 Purpose and Scope

This reference guide is crafted to orient and assist a PACS implementor with many of the key challenges in realizing a state-of-the-art PIV-enabled PACS. NIST SP 800-116 R1 states that the purpose of the special publication is to use risk management to select appropriate PIV authentication mechanisms to manage physical access. The intent of SP 800-116 R1 is stated as follows:

"to facilitate and encourage greater use of PIV Cards, this document:

- *Describes the implementation of PIV-enabled PACS.*
- *Discusses the PIV Card capabilities so that a risk-based assessment can be aligned with the appropriate PIV authentication mechanism.*
- *Outlines an overall strategy for PIV authentication mechanisms with agency facility PACS."*[1]

PIV credential use for accessing buildings is in scope, but non-PIV credentials are out of scope, even if the population requires access to federal facilities.

Many other aspects of physical access control are outside the scope of SP 800-116 R1. Authorization (i.e., granting permission within a PACS for an identified person to pass access control points) is a critical security function, but is out of scope for the PIV system. Other out-of-scope functions include area protection, intrusion detection, egress, monitoring and tracking (other than at access control points),

[1] NIST SP 800-116 Revision 1: "Guidelines for the Use of PIV Credentials in Facility Access," June 2018, https://www.nist.gov/publications/guidelines-use-piv-credentials-facility-access.

and enforcement of access control decisions. It is understood that PACS may also be integrated with surveillance systems, fire alarm systems, evacuation systems and other systems within a facility. This document does not address the integration of PACS with other facility-centric information technology (IT) systems, although it has been written to minimize conflicts during such integration. Therefore, if the integration of the measures outlined in this document creates a life-safety risk, organizations will need to mitigate these risks before applying these measures.

2 Characteristics of PIV Implementation

This section describes the main benefits of a complete PIV implementation, in accordance with SP 800-116 R1.

Figure 1 and Figure 2 show the features, benefits and qualities of a complete PIV implementation.

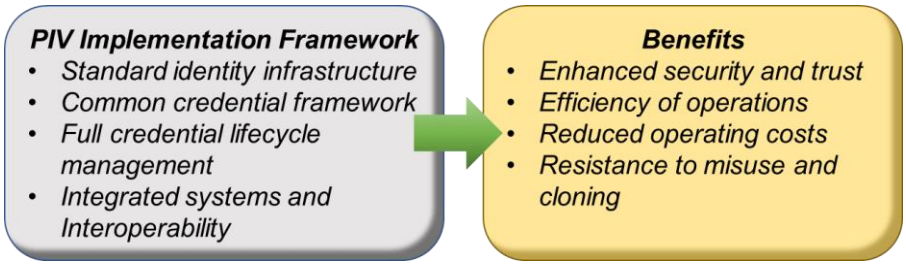

Figure 1. Features and Benefits of a Complete Implementation

The inherent qualities of a complete PIV implementation are:

1. *PIV authentication mechanisms are used wherever applicable*
2. *Electronic authentication is the common practice*
3. *Electronic validation of the PIV Card is done at/near the time of authentication*
4. *All access control decisions are made by comparing the PIV identifier to access control list (ACL) entries*
5. *Cryptographic and biometric authentications are applied widely in low/moderate/ high impact areas*
6. *Agencies exhibit reciprocal trust in the process assurance of PIV card issuers (PCIs)*
7. *New and upgraded PACS accept PIV Cards as proof of identity for user authentication*
8. *Authentication transactions are optimized*

Figure 2. Qualities of a Complete Implementation

2.1 Interoperability Qualities

Interoperability for PIV-based facility access (Figure 3) means the ability of a PACS to use any PIV card issued by any agency to authenticate the cardholder by performing one or more PIV authentication mechanisms. NIST 800-116 R1 further defines the interoperability goal of a PIV-enabled PACS in more detail.

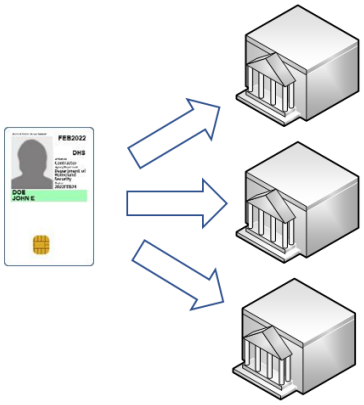

Figure 3. Interoperability

2.2 Infrastructure Requirements

Not every PACS can be adapted to implement the PIV authentication mechanisms end-to-end and achieve the benefits described above. The PACS, its installation and field configuration must be properly selected and designed to realize the benefits and qualities noted in this section. For example, a PACS must be supported by a bi-directional communications infrastructure (Figure 4), as follows:

- *Fast* network or two-way serial communication among PACS readers, controllers/panels, and head-end/back-end PACS components.
- *Fast* network communication for PIV status and validation services.

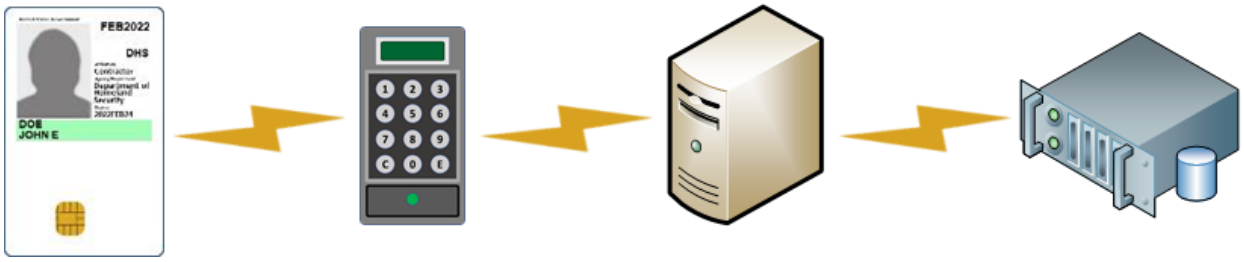

Figure 4. PACS Infrastructure Communications

3 Threat Environment

The PIV system is intended to enhance security and trust in identity credentials, but no practical system can guarantee perfect security. Table 1 uses condensed language from SP 800-116 R1 and includes mitigation techniques with recommendations from the Secure Technology Alliance Access Control Council. The table itemizes some known technical threats to PIV authentication mechanisms and summarizes the techniques that can mitigate the threats.

Table 1. PIV Authentication Technical Threats

Threat	Description	Mitigation Techniques
Identifier Collision	Identifier collision occurs when the processing of multiple credential identifiers results in a common, non-unique identifier value.	PIV-card identifiers (i.e., FASC-N and Card UUID) are unique. Prior to and during physical access and identifier processing, these identifiers must never be truncated, compressed, hashed, or modified such that identifier information is lost or reduced. These restrictions eliminate the possibility of multiple cards appearing to have the same identifier.
Revoked PIV Cards	Revoked PIV cards may potentially still be successfully used for authentication and physical access.	PACS should validate all PIV cards during each physical access event by checking the validity and revocation status of PIV Authentication Certificates and Card Authentication Certificates (CAK) by either accessing authoritative Online Certificate Status Protocol (OCSP) servers or periodically downloading authoritative Certificate Revocation Lists (CRLs).
Visual Counterfeiting	Mimicking the outside appearance of a PIV card, but not the electronic behavior.	With the presence of one or more topographical security features (e.g., optical varying inks, holograms, and watermarks) on the PIV card, a visual counterfeit is unlikely to pass close examination, provided guards are trained to recognize security features.
"Skimming" Idle PIV Cards	A rogue contactless reader with a powerful and sensitive-enough antenna can perform a free read of the PIV card's contactless interface (i.e., CHUID and CAK) at a distance of up to 25 cm/10 in.	Employ shielding techniques (e.g., electronically opaque card sleeve/holder) that positively deactivate the PIV card when not in use.
"Sniffing" Messages between Card and Reader	A sniffer is a passive receiver at a distance that can capture the entire message transaction between a contactless reader and a PIV card.	Employ PIV cards and readers that support secure messaging (as defined in NIST SP 800-73), which provides an encrypted secure channel between the card and reader. While the data may be sniffed, it cannot be decrypted and rendered intelligible to the sniffer.
Social Engineering	Obtaining the PIV card contents through social engineering skills, such as a fraudster convincing someone to give them a PIV card temporarily (while the fraudster secretly skims it), or spoofing a	The PIV card mitigates the risk of social engineering attacks by blocking the release of all private and secret keys. Thus, authentication at the PACS should use private-key challenge mechanisms such as PKI-CAK and PKI-AUTH; i.e., do not rely on CHUID-only authentication at the PACS.

Threat	Description	Mitigation Techniques
	web site that requests PIV card insertion and entering a PIN to allow the site to read the card contents.	
Electronic Cloning	After skimming, sniffing, and/or temporarily gaining possession of a PIV card and obtaining the card's CHUID and CAK through the contactless interface, an attacker could create a cloned card containing the CHUID and CAK of the compromised PIV card.	Employ PKI authentication of the PIV card's CAK (PKI-CAK) at contactless readers during physical access. PKI-CAK authentication relies upon the private key associated with the CAK, which cannot be extracted from the card by any means. Upgrade existing PACS that perform CHUID-only authentication to enable them to perform PKI-CAK for contactless readers and PKI-AUTH for contact readers.
Electronic Counterfeiting	An attacker can counterfeit a card (or emulate one with an electronic device; e.g., smartphone with NFC) with a made-up CHUID that contains a valid identifier that a PACS may have on its access control list.	Employ PKI authentication of the PIV card's digital certificates (i.e., Card Authentication Certificate or PIV Authentication Certificate) at PIV card readers during physical access. Upgrade existing PACS that perform CHUID-only authentication to enable them to perform additional PKI authentication for both contact and contactless readers.
Capture and Replay	An adversary captures/sniffs a message from a PIV card when it is presented to a reader, and replays the message to the reader at a later time to attempt to gain access as an impostor.	Employ PKI authentication of the PIV card's CAK (PKI-CAK) at contactless readers during physical access. Any replay attempts will fail since the adversary will not have the necessary CAK private key to advance through a successful authentication.

4 PIV Authentication Mechanisms in PACS Applications

PIV cards enable a variety of authentication mechanisms that are supported by specific data elements contained in the PIV card's protected memory environment. These data elements and authentication mechanisms are employed at the time of access at entry points (e.g., doors, gates, and turnstiles) controlled by a PACS. Entry points are equipped with PIV card readers that can interact with the PIV card either through the PIV card's contact or contactless interfaces. In addition, card readers at these entry points may be augmented with biometric capture devices such as fingerprint scanners, iris infrared cameras, and/or photographic cameras to support stronger methods of authentication.

Figure 5 provides a consolidated view of the PIV card data elements and the associated contact and contactless authentication mechanisms that may be used at PACS entry points.

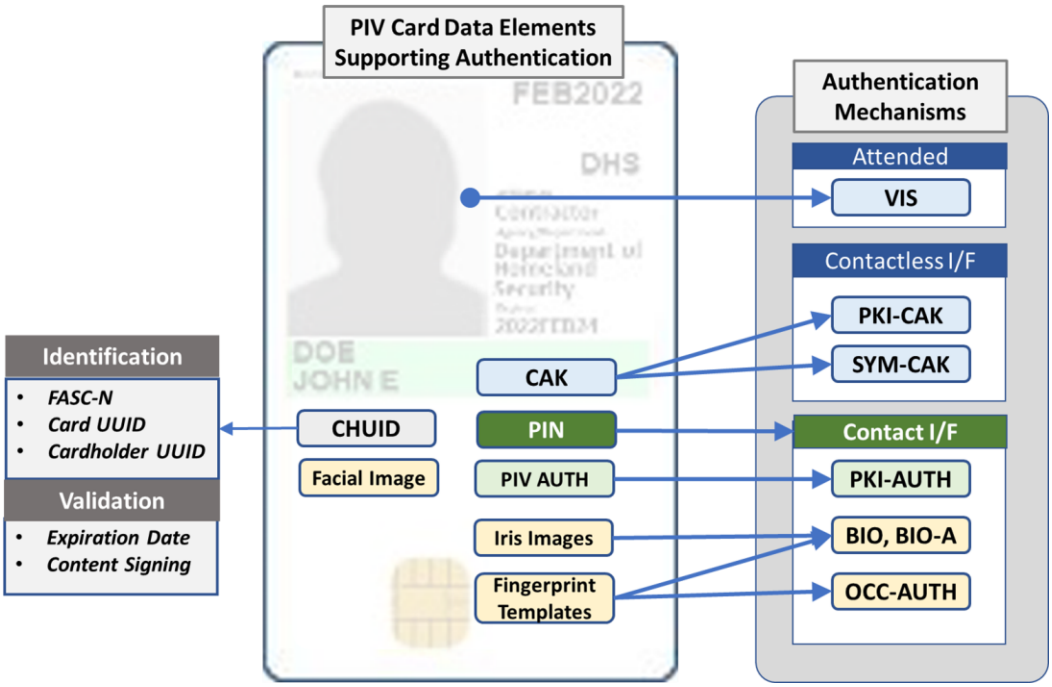

Figure 5. PIV Card Data Objects and Authentication Mechanisms

The content in this guide assumes that the reader has a sufficient understanding of the PIV card data elements and the authentication mechanisms that are supported by PIV cards, as shown in Figure 5.

For reference, Section 9, Appendix A provides an itemized list and description of:

- PIV card data elements
- Authentication mechanisms

4.1 PIV Authentication Mechanisms

Authentication mechanisms consist of techniques and protocols that execute steps to recognize and verify identities against a set of credentials to assure they are authentic. Authentication mechanisms comprise processes that ensure that PIV cards are authentic; i.e., not fraudulent cards or clones of other PIV cards. These mechanisms also provide confidence that the PIV cardholder is the actual owner of the card, and the original individual to whom the card was issued.

Table 8 in Appendix A lists and describes the approved PIV authentication mechanisms.

4.2 Authentication Factors

The PACS application is required to verify the identity of the cardholder presenting a PIV card to a card reader. This is accomplished by performing one or more authentication mechanisms using the PIV card. Successful authentication establishes confidence in the identity of the cardholder. Confidence levels increase with the number of factors used. Factors are referred to as something you HAVE, something you KNOW or something you ARE.

Table 2. Authentication Factors [Source: SP 800-116 R1, Table 4-3, pg.15]

Authentication Factor	What It Means
Something You HAVE	Your PIV card
Something You KNOW	Your PIN
Something You ARE	Your fingerprint, face or iris biometric

The confidence in the cardholder's identity increases with the number of factors used for authentication. If using only one of these, then it is referred to as one-factor authentication; if two of these are used, then two-factor authentication; and if three are used, then three-factor authentication. NIST SP 800-116 R1 Table 4-1 and Table 4-2 provide lists of PIV authentication mechanisms and their authentication factors when used on the contact and contactless interfaces, respectively.

Table 3. PIV Authentication Mechanisms on the Contact Interface [Source: SP 800-116 R1, Table 4-1, pg. 13]

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors
CHUID^{deprecated} + VIS	x			1
BIO			x	1
SYM-CAK	x			1
PKI-CAK	x			1
BIO-A	x		x	2
PKI-AUTH (with PIN)	x	x[2]		2

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

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors
PKI-AUTH (with OCC)	x		x[3]	2
OCC-AUTH	x		x	2
SYM-CAK + BIO(-A)	x	x	x	3
PKI-CAK + BIO(-A)	x	x	x	3

Table 4. PIV Authentication Mechanisms on the Contactless Interface
[Source: SP 800-116 R1, Table 4-2, pg. 14]

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors
CHUID deprecated + VIS	**x**			**1**
SYM-CAK	**x**			**1**
PKI-CAK	**x**			**1**
OCC-AUTH	**x**		**x**	**2**

4.3 Selection of PIV Authentication Factors

A risk-based approach should be used when selecting appropriate PIV authentication mechanisms for physical access to Federal government buildings and facilities, regardless of whether they are leased or government-owned.

The Secure Technology Alliance Access Control Council recommends that authentication mechanisms correspond with the protective areas established around assets or resources. This document adopts the NIST SP800-116 concept of defining progressive levels of required security, from lowest to highest, named "Controlled, Limited, and Exclusion" areas. Areas outside the "Controlled" boundary are considered "Unrestricted," as they are open to all. When crossing boundaries from one area to another, the Secure Technology Alliance Access Control Council makes the following recommendations regarding the required number of factors to use for authentication.

When crossing the boundary from Unrestricted to Controlled (Table 6), one factor is required. The recommendation is to use the "contactless" CAK Authentication mechanism (something you have).

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

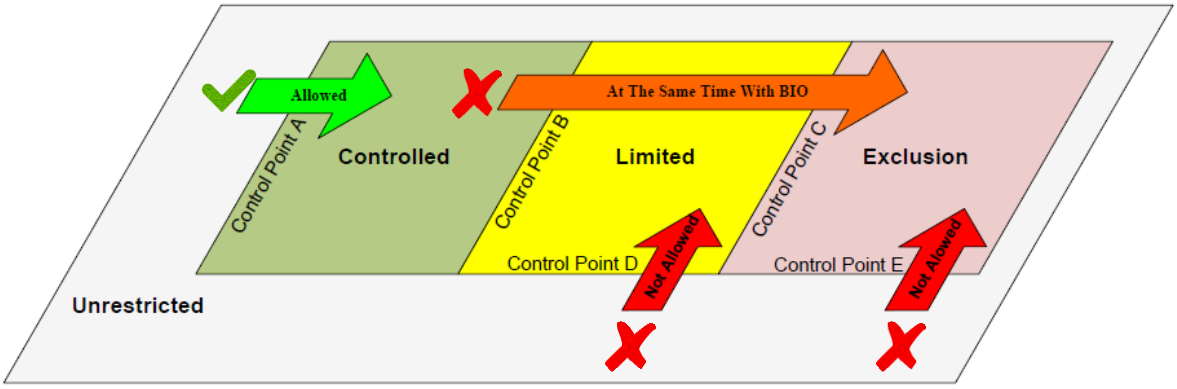

Figure 6. Unrestricted to Controlled – One-Factor Authentication Required
[Source: PIV in E-PACS, pg. 61[4]]

When crossing the boundary from Controlled to Limited (Figure 7), two factors are required. The recommendation is to use the "contact" PKI-AUTH Authentication mechanism (something you have plus something you know).

Because it is two-factor authentication, this pattern is sufficient for moving from an Unrestricted area or into a Controlled or Limited area, or between Controlled and Limited areas.

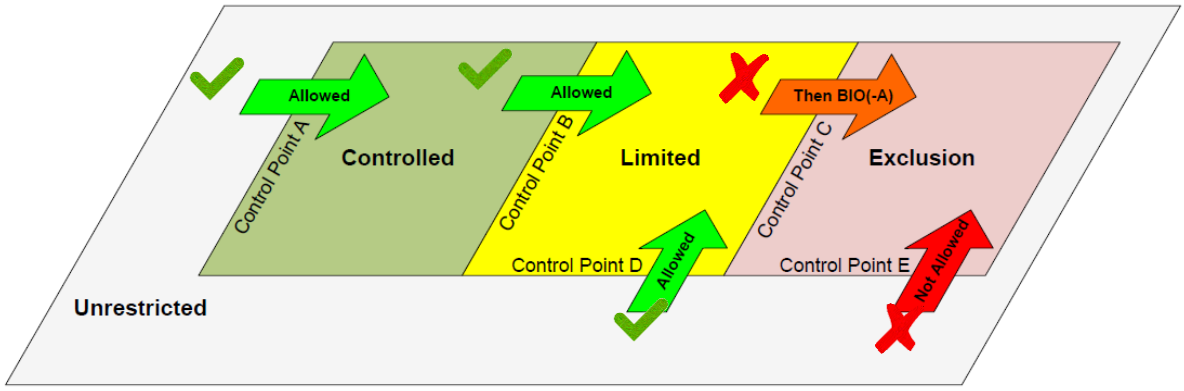

Figure 7. Two-Factor Authentication Required
[Source: PIV in E-PACS, pg. 64]

When crossing the boundary from Limited to Exclusion (Figure 8), three factors are required. The recommendation is to use the "contact" PKI-AUTH + BIO-A authentication mechanism (something you have, plus something you know, plus something you are – actually a combination of two mechanisms).

[4] "Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS)" [PIV in E-PACS], Interagency Security Committee, https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/piv-in-epacs.pdf.

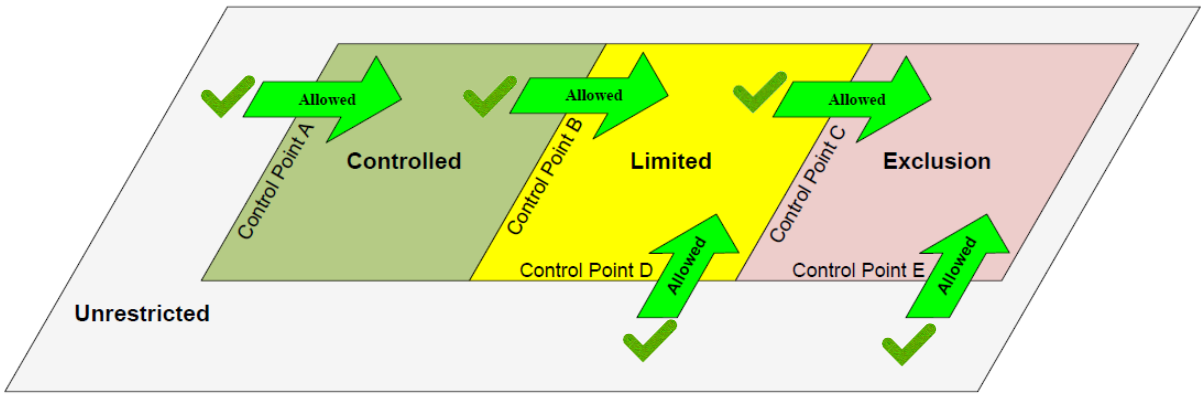

Figure 8. Three-Factor Authentication Required [Source: PIV in E-PACS, pg. 65]

Federal government facilities can be identified and categorized corresponding to LOW (for Controlled), MODERATE (for Limited), and HIGH (for Exclusion) depending on the impact to assets or resources. This white paper recommends that Table 5 be used to determine the minimum number of authentication factors needed to satisfy security requirements of the area.

Table 5. Authentication Factors for Security Areas

Security Areas	Number of Authentication Factors Required	Example Authentication Mechanism	Acronym
Controlled	1 (Something you **HAVE** – your ID card)	Public Key Infrastructure Card Authentication Key	PKI-CAK
Limited	2 (Something you **KNOW** – your PIN)	Public Key Infrastructure - with PIN	PKI-AUTH
Exclusion	3 (Something you **ARE** – your fingerprint, retina, or other biometric)	Public Key Infrastructure - with PIN and biometric	PKI-AUTH + BIO

NOTE: VIS + CHUID, was a previously acceptable authentication factor; however, VIS + CHUID is NOT included in this version of SP 800-116 R1 since both VIS and CHUID provide “LITTLE or NO” confidence in the identity of the cardholder and have been deprecated. Authentication mechanisms other than the CHUID authentication mechanisms must be implemented. Newly-purchased systems must support other authentication mechanisms (e.g., PKI-CAK) rather than the CHUID mechanism.

4.4 Credential Validation

As described in NIST SP800-116 R1, credential validation is the process of determining if a presented identity credential is valid; i.e., was legitimately issued and has not expired or been revoked. Validating credentials by going online to check revocation status is extremely valuable to relying parties, because it retrieves the most up-to-date credential status and blocks access with fraudulent PIV cards that have been lost or stolen. When not practical for a variety of reasons, it may be possible for PIV cards of interest to be registered with a caching status proxy (local storage for later validation). The caching status proxy polls the status of all registered cards periodically and caches the status responses from their issuer(s). The cache status should be updated at least once every 24 hours.

Path validation (or *trust path validation*) is the process of verifying that each certificate of each link of the certificate issuance chain can be trusted or validated successfully along the path between the certificate issuer (e.g., certificate authority) and the certificate being presented to a reader. Full trust in a PIV authentication mechanism requires that path validation succeeds for each PIV data object used by the authentication mechanism.

The latest version of FIPS 201 now requires that path validation be performed for all PIV authentication mechanisms, since authentication mechanisms can be fully trusted only if path validation is performed.

5 PACS Use Cases

The facility security level (FSL) is referenced throughout SP 800-116 R1. At the same time, SP 800-116 states: "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." However, FSL analysis is only to assist in thinking about risk assessment while determining the Controlled, Limited, and Exclusion areas, so an expedient approach is to focus on mapping the FSL and the authentication mechanisms. SP 800-116 R1 examines the following use cases:

- Single-tenant facility
- Federal multi-tenant facility
- Mixed multi-tenant facility
- Single-tenant campus
- Federal multi-tenant campus

Before a credential such as a PIV card may be used in a PACS, the card must be registered in the PACS user database and assigned access privileges (i.e., authorization, which is specifically out of scope for SP 800-116 R1 though essential for a PACS deployment). The registration process will likely vary and is ultimately based on agency policies. For the purpose of this guide, two common registration procedures are covered, local registration and centralized registration.

1. **Local registration**. A few significant system functions enhance trust that the person being registered is presenting a valid, authentic card and that the card is indeed issued to the person who is being registered in the PACS. During local registration, a properly configured PACS will perform two- or three-factor authentication to ensure the right person is presenting the card. Second, the PACS will check the validity status of each certificate authority (CA) in the path from the issuer of the presented card to the approved trust anchor. Once the authentication/ validation is completed, access privileges are added and the user is added to the PACS database. From this point on, the user may use the card to request access to the authorized areas. The PACS will need to be field-configured for where one-, two-, or three-factor authentication is required, based on associated Controlled, Limited and Exclusion area assignments.

2. **Central registration**. Central registration is a growing requirement. This process means that cardholder information may be downloaded to a local PACS using an enterprise network of PACS that are connected to a central personnel database that includes people who have already registered a valid card. When the person arrives at a local site, the registration is already partially completed for setting the authentication requirements. The only remaining item is to assign the proper authorization to the individual. Some agencies are automatically assigning "basic" or "general" access authorizations to cardholders whose information has been downloaded. This means that those cardholders are able to simply enter the local sites and proceed to certain authorized areas without needing to visit the security office to be provisioned in the local system. However, for broader access to additional areas, a later trip to the security office might be required. This approach is convenient and requires careful PACS design and planning.

NIST SP 800-116 R1 shows recommended use cases for how, at a local level, a PACS should authenticate PIV credentials, based on site-specific threats/risk assessment as described in the next section. SP 800-116 R1 does not make recommendations about how to conduct threat /risk assessments, but does imply

that the completed assessment should produce up to three levels of classification above uncontrolled: Controlled, Limited and Exclusion. It is important to coordinate the facility security assessment with all tenant agencies in a facility, after determining mission criticality, symbolism, facility population, facility size, and threat to tenant agencies.

Facility assessments are often conducted by the Federal Protective Service in accordance with the Interagency Security Committee (ISC) Risk Management Process for Federal Facilities[5] to identify, assess, and prioritize the risks to be addressed for the facility. Secondary assessments should be performed to determine the classification of risk for interior areas, to derive Controlled, Limited and Exclusion. Reference Table 5 for area classification description, color association, and required level of authentication factors.

Controlled 1 FA Area
Limited 2 FA Area
Exclusion 3 FA Area

Figure 9 - Sample Facility Access Areas and Classification [Source: GSA PACS Ordering Guide,[6] pg. 34]

Tenant agencies located in a GSA-operated facility may request that GSA add additional access control points to a PACS that is already installed at perimeter access control points. In this use case the GSA PACS is expanded to accommodate additional doors/readers using NIST SP 800-116 R1 authentication mechanisms as per the tenant agency threat/risk assessment. Tenant agency employees are registered in the GSA PACS and provisioned according to tenant agency policies.

Should a tenant agency decide to use its own PACS, then the tenant agency must have its own perimeter to enter its own space. The tenant agency is responsible for managing its own space, PACS and user provisioning/de-provisioning processes. A tenant agency employee may be registered in two different PACS in the same building. Both PACS must be included on the GSA FIPS 201 Evaluation Program

[5] https://www.dhs.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf.
[6] "Physical Access Control System (PACS) Customer Ordering Guide," Vn 2.0, GSA, June 2018, https://www.gsa.gov/cdnstatic/General_Supplies__Services/Guide_to_PACS_v2%2006-12-2018.pdf.

Approved Product List;[7] both PACS must be engineered and configured correctly for PIV credentials to be used as intended in a PACS regardless of the owning agency.

GSA and the tenant agency(s) must agree on policies for how the user credential and identity data are shared and maintained in a PACS user database that is shared with an "outside" agency.

Multi-tenant facilities should establish a facility security committee (FSC), composed of representatives from each agency paying rent within the given facility. The FSC plays a pivotal role in security issues/risks that have the potential to impact all tenants or the entirety of the facility.

There is little, if any, relevant process difference if the facility is agency-owned or leased.

Although NIST SP 800-116 R1 provides guidance for implementing PIV credentials and proper authentication beginning with FSL3 facilities, the Secure Technology Alliance Access Control Council added Table 6 that may be considered when a federal agency desires to implement PIV credentials and PKI authentication at all FSL designations. However, it can be readily deduced that FSL1, FSL2 and FSL3 align to Controlled, while FSL4 aligns to Limited, and FSL5 aligns to Exclusion.

Table 6. Recommended Authentication Factors Based on Facility Security Level (FSL)

FSL Determination	Authentication Factors Required	Authentication Mechanism(s)	Interface
FSL1	None	PKI-CAK (recommended)	Contactless
FSL2	None	PKI-CAK (recommended)	Contactless
FSL3	One (1) Factor	PKI-CAK	Contactless
FSL4	Two (2) Factors	PKI-AUTH	Contact
FSL5	Three (3) Factors	PKI-AUTH + BIO	Contact

[7] https://www.idmanagement.gov/approved-products-list/.

6 Deployment Considerations

This section summarizes industry best practices for deploying PIV-enabled PACS and includes recommendations from the Secure Technology Alliance Access Control Council.

When deploying, agencies should:

- Follow the threat/risk assessment determination of the classification that applies to the entry point to each area (Controlled, Limited, Exclusion).
- Select PACS equipment that is included in the GSA Approved Products List and services from service providers with the Certified System Engineer ICAM PACS (CSEIP) certification.
- Plan for how to accept high assurance credentials issued by other agencies.

6.1 Rollout Considerations

Agencies moving towards FICAM-compliant PACS should consider the impact to the federal facility population when modernizing PACS assets. Installation of FICAM-compliant PACS solutions requires agencies to establish PKI authentication capabilities that are used when registering a PIV card to the PACS and when presenting PIV cards to card readers during physical access requests. Agencies implementing strong authentication for access control require cardholders to present their PIV or PIV-Interoperable (PIV-I) card to a card reader capable of performing a proper PKI challenge, based on the required factors of authentication.

A FIPS-201-compliant PACS implementation requires that all card readers support strong authentication and that all issued credentials contain the appropriate PKI certificates. Use of a "hybrid or mixed-mode" card reader is contradictory to FIPS 201 compliance by allowing the use of card products that do not support proper PKI authentication.

6.2 PIV Identifiers

The primary identifiers on a PIV card are the Federal Agency Smart Credential Number (FASC-N), Card Universal Unique Identifier (Card UUID), and the Cardholder Universal Unique Identifier (Cardholder UUID). These identifiers are found in the PIV card CHUID data element (see Appendix A, Table 9, for details) and are typically stored in the PACS database when PIV cards are registered. Each PACS included in the GSA FIPS 201 Evaluation Program APL is capable of selecting and processing the correct identifier based on the card that is presented to the PACS reader.

6.3 PACS Registration

Registration of a PIV card can occur by two means:

1. Local single-card enrollment through the PACS solution enrollment
2. Bulk enrollment of cards through the use of the PACS product application programming interface (API) capability based on agency/enterprise authoritative identity management repositories and/or systems

The first mechanism can be used in any environment, allowing the PACS enrollment capability to harvest and validate card data as new cards are registered. The second mechanism, integration of the API, can be leveraged in an environment where an agency has an identity management solution. This API integration provides more instantaneous provisioning (or de-provisioning) as the card/cardholder

identity data can be "pushed" to the PACS system or the identity data can be "pulled" from identity management services by the PACS through integrated automated processes.

6.4 Temporary Badges

Agencies considering the use of temporary cards for physical access need to define the use cases for temporary card issuance and usage. Currently there is no Federal guidance on this issue. Each agency must consider its own needs and policies for temporary badges. Agencies have considered, and some employ, high-assurance credentials such as PIV-I, Commercial Identity Verification (CIV), or Transportation Worker Identification Credential (TWIC) for temporary credentials where a PIV credential would prove expensive or impractical to issue to a range of cardholders.

The following groups can have a need for temporary badge/credential usage:

1. **Employees/contractors** who need to access the agency's facility, but who do not meet the PIV issuance requirements, such as only being employed for six months or less (per OMB M-05-24[8]).
2. **Visitors** from other government agencies who are subject to local security policies to determine if a visitor who has a PIV credential issued by a different agency may use his/her PIV card for unescorted access to the visited site if properly registered and assigned authorization privileges. Students and the general public are usually provided an escort while visiting. Some agencies' security policies require issuing a temporary visitor badge that may be registered in a local PACS and used as temporary access credential. Each agency and location may have their own policies for visitors.

When an employee's or contractor's PIV card is lost or stolen, it is considered compromised. Cardholders experiencing a loss or theft of the PIV card should contact the agency security department immediately, and the agency should perform a revocation of the PIV card, which includes revocation of the PKI certificates. In addition, the account associated with the PIV card should be disabled in the local PACS. Agencies that employ strong authentication and certificate validation practices can minimize risk, since the revocation of the PIV card's PIV Authentication and Card Authentication certificates will prevent the successful validation of a stolen PIV card during physical access attempts at a PACS.

6.5 The CHUID-Only "Authentication" Issue

The previous version of SP 800-116 included the CHUID authentication mechanism as an option for transitioning from Unrestricted to Controlled areas. The CHUID, however, is not included in SP 800-116 R1 as it has been deprecated, since the CHUID provides "little or no" confidence in the identity of the cardholder. New PACS implementations must support other approved authentication mechanisms (e.g., PKI-CAK), and older systems must be updated to comply with current requirements.

Agencies were directed in 2011 to PIV-enable their existing IT and PACS systems, or upgrade to new PIV-enabled implementations. (See OMB M-11-11.[9]) Many agencies complied, but many of their PACS installations were based solely on CHUID-only authentication. These existing systems are at risk due to

[8] M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," OMB Memorandum, Aug. 5, 2005, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf.

[9] M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors," OMB Memorandum, Feb. 3, 2011, https://www.cac.mil/Portals/53/Documents/m-11-11.pdf.

the ease with which the CHUID can be read by handheld devices and played back to the PACS. Handheld devices such as Android smartphones have demonstrated that they can easily be programmed to read the CHUID from PIV cards, store the CHUID, and play it back to PACS PIV card readers through the smartphone's Near Field Communication (NFC) contactless interface. This vulnerability negates the intent of HSPD-12 (e.g., resistance to cloning, forgery, alteration and terrorist exploitation).

Section 9, Appendix B provides a tutorial on PKI authentication, which shows how it is superior to CHUID authentication. The use of CHUID-only authentication simply provides an identifier (see Section 6.2), and thus, cannot be considered an authentication mechanism. As a result, FIPS 201-2 has deprecated the CHUID-only mechanism.

7 Summary and Conclusion

This guide was developed to focus on the content of SP 800-116 R1 that provides the essential information required to successfully implement PIV with PACS, without including discussion of how the card is made or how it works "under the hood." Alternative visual diagrams are provided to enhance understanding of the applications and approaches to meet the requirements.

This guide enables the reader to more quickly grasp the required concepts and apply the correct authentication mechanisms to their facility and access control use cases. An analogy is: NIST SP 800-116 R1 is a "dictionary;" this guide uses this dictionary to craft a story suitable for the unique needs of a PIV-enabled PACS solution implementor.

To simplify the process, implementors should define three progressive levels of security based on risk assessments.

- Begin with one-factor authentication for Controlled areas,
- Progress to two-factor authentication for Limited areas, and
- Use three-factor authentication for Exclusion areas.

After authentication mechanisms are determined, it is easier to scope the PACS configuration, procurement and implementation. This also assists in the process of defining acceptance tests performed to an agency's satisfaction.

8 Publication Acknowledgements

This guide was developed by the Secure Technology Alliance Access Control Council.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

Special thanks go to **Lars Suneborn** (Secure Technology Alliance in 2018, ID Technology Partners currently), who managed the project, recruited participation, contributed content and reviewed this document.

The Secure Technology Alliance thanks the following Council members who contributed to writing and/or reviewing this guide:

- **Mark Dale**, XTec, Inc.
- **Tony Damalas**, SigNet Technologies
- **Derek Greenland**, Lenel
- **Ryan Kaltenbaugh**, Lenel
- **Roger Roehr**, Integrated Security Technologies
- **Gerry Smith**, ID Technology Partners
- **Lars Suneborn**, ID Technology Partners
- **William Windsor**, DHS
- **Rob Zivney**, ID Technology Partners

Trademark Notice

About the Secure Technology Alliance Access Control Council

The Secure Technology Alliance Access Control Council focuses on accelerating the widespread acceptance, use, and application of secure technologies in various physical and digital form factors for physical and logical access control as applicable to both persons and non-person entities. The group brings together, in an open forum, thought leaders, manufacturers, and implementers from both the public and private sectors. The Council identifies topical areas which further the use of technologies that are important to the access control community.

Additional information on the use of smart card technology for identity and access control applications can be found on the Secure Technology Alliance web site at http://www.securetechalliance.org.

9 APPENDIX A: PIV Data Elements and Authentication Mechanisms

Table 7. PIV Card Data Elements

PIV Card Data Element	Description
Cardholder Unique Identifier (CHUID)	The CHUID contains PIV-related identifier and card validation data objects that include the FASC-N, Card Universal Unique ID (UUID), Cardholder UUID, Card Expiration Date, and Digital Signing Certificate. These data objects are used during physical access to identify the cardholder and ensure that the cardholder has the privileges to access specific entry points within the PACS purview.
Personal Identification Number (PIN)	The PIN is a secret that only the cardholder knows. It usually consists of a string of six or eight numeric characters. The PIN protects specific data elements and functions on the card such that a cardholder must enter a PIN before the card can perform cryptographic functions for the PIV Authentication Certificate, and access biometric elements on the card (i.e., iris, fingerprint templates, and facial image) during authentication. The PIN is used to perform these functions, which are only allowed through the PIV card's contact interface. Note that the Card Authentication Certificate can be accessed through either the contact or contactless interface, and cryptographic functions can be executed without entering a PIN.
Card Authentication Key (CAK) • ***Card Authentication Certificate*** • ***CAK Private Key*** • ***Symmetric Card Authentication Key (optional)***	The Card Authentication Key refers to both the Card Authentication Certificate (which contains the Card Authentication Certificate public key) and the Card Authentication private key (which cannot be accessed outside of the card) associated with the public key within the digital certificate. The Card Authentication Certificate can be read from the PIV card through either the contact or contactless interface, and PACS systems can use this certificate to determine (through cryptographic challenge techniques during authentication) that the card contains the CAK private key that is associated with the CAK public key in the certificate. Alternatively, the CAK may contain a Symmetric Card Authentication Key that may be used for symmetric authentication, where the PACS system knows the symmetric key that is on the PIV card, and the PACS can perform a challenge to ensure that the keys match.
PIV Authentication Key (PIV Auth) • ***PIV Authentication Certificate*** • ***PIV Authentication Private Key***	The PIV Authentication Key refers to both the PIV Authentication Certificate (which contains the PIV Authentication Certificate public key) and the PIV Authentication private key (which cannot be accessed outside of the card) associated with the public key within the PIV Authentication Certificate. The PIV Authentication Certificate can only be read from the PIV card through the contact interface, and PACS systems can use this certificate to determine (through cryptographic challenge techniques during authentication) that the card contains the private key that is associated with the PIV Authentication Certificate public key.
Fingerprint Templates	Fingerprint templates are compressed biometric data objects that contain key characteristics of the cardholder's fingerprints that can be used to do a biometric fingerprint match during authentication. There are usually two fingerprint templates, consisting of the left and right index fingers of the cardholder. In rare occasions where no fingerprints can be acquired from the cardholder during registration, facial and/or iris biometric authentication can be performed as an alternative biometric authentication mechanism.
Iris Images	Iris images are compact biometrics images of the cardholder's left and right irises, which may be used for biometric authentication of the cardholder. These data elements are optional and may not necessarily be present on all PIV cards.
Facial Image	The facial image is a JPEG-formatted data object that contains the photographic image of the cardholder. This is the same facial image that is printed on the face of the PIV card. The facial image supports visual authentication by a guard or attendant, and may also be used for automated facial authentication.

Table 8. PIV Authentication Mechanisms [Sources: NIST SP 800-116 R1, FIPS 201, SP 800-73-4; SP 800-76]

Authentication Mechanism	Description
Contactless Interface	
PKI-CAK	PKI-CAK is an authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card Authentication Certificate and the separate CAK private key. PACS card readers and head-end PACS components read the Card Authentication Certificate from the card through the contact or contactless interface, and send a random set of data bytes (i.e., nonce) to the PIV card where the nonce is encrypted with the CAK private key and sent back to the PACS. The PACS decrypts the encrypted nonce using the public key in the Card Authentication Certificate. If the decrypted nonce matches the nonce sent to the PIV card, then the PACS is assured that the PIV card hosts/owns the correct CAK private key associated with the Card Authentication Certificate, and thus the PIV card is authenticated.
SYM-CAK	SYM-CAK is an authentication mechanism that is implemented by a symmetric key challenge/response protocol using the Card Authentication Key (CAK) symmetric key, which is known to the PACS due to prior PIV card registration into the PACS. The PACS card reader and head-end PACS component sends a random set of data bytes (i.e., nonce) to the PIV card where the nonce is encrypted with the CAK symmetric key and sent back to the PACS. The PACS decrypts the encrypted nonce using the known symmetric key. If the decrypted nonce matches the nonce sent to the PIV card, then the PACS is assured that the PIV card hosts/owns the correct CAK symmetric key, and thus the PIV card is authenticated.
Contact Interface	
PKI-AUTH	PKI-AUTH is an authentication mechanism that is implemented by an asymmetric key challenge/ response protocol using the public key of a PIV Authentication Certificate and the separate private key. PACS card readers and PACS components read the PIV Authentication certificate from the card through the contact interface, generate and send a random number (nonce) to the PIV card where the nonce is signed with the PIV Authentication private key and sent back to the PACS. The PACS decrypts the signed nonce using the public key in the PIV Authentication Certificate. If the decrypted nonce matches the nonce sent to the PIV card, then the PACS is assured that the PIV card hosts/owns the correct private key associated with the PIV Authentication Certificate, and the PIV card is authentic.
BIO, BIO-A, [BIO (-A)]	BIO is a biometric authentication mechanism that is based on performing biometric matching of the PIV card fingerprint templates, iris images, or facial image against fingerprints, irises or facial photo captured at the time of access to an entry point controlled by the PACS. This authentication mechanism requires live finger, iris or photo capture at the PIV card contact reader at the entry point, and the biometric matching occurs on the PIV card reader or head-end side of the PACS. BIO-A is an authentication mechanism identical to the BIO authentication mechanism with the addition that the access is "attended" by a human (e.g., guard) who witnesses the BIO authentication. BIO and BIO-A are usually used in conjunction with PKI-AUTH in order to provide an additional authentication factor; i.e., "something you are." The "BIO(-A)" acronym indicates that either BIO or BIO-A may be used as an authentication mechanism.
OCC-AUTH	OCC-AUTH is a biometric authentication mechanism similar to BIO/BIO-A, but only for fingerprints. OCC stands for "on-card comparison." It is very similar to BIO authentication with the difference that the card reader captures the live fingerprint of the cardholder at the entry point, processes it, and sends it to the PIV card, where the fingerprint match is performed on the PIV card against the stored fingerprint templates, and the PIV card returns the result of the match to the reader.

Authentication Mechanism	Description
Attended	
VIS	Visual (VIS) authentication entails inspection of the topographical features on the front and back of the PIV card. A human guard or attendant 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 VIS authentication mechanism cannot be verified electronically, and thus, should not be used as the sole authentication mechanism when another mechanism is practical.

Table 9. CHUID Data Elements and Unique Identifiers

CHUID Data Element	Unique Identifier	Description
Federal Agency Smart Card Number (FASC-N)	✓	The FASC-N is a 25-numeric character sequence that provides a set of data elements that support identification of a PIV card (i.e., the FASC-N Identifier) and PIV cardholder Persona Identifier), and also contains issuance source information (i.e., Agency Code, System Code, Credential Number, Credential Series, Individual Credential Issue, Person Identifier, Organizational Category, Organizational Identifier, and Person/Organization Association Category). A subset of the FASC-N, the FASC-N Identifier, is a fully qualified number sequence that uniquely identifies the PIV card, and is a combination of the Agency Code, System Code, and Credential Number. The FASC-N and CHUID were originally defined in early versions of "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS)" and were adopted for inclusion in the PIV card data model (FIPS 201 v1 - 2005) in order to support and ease the transitioning of legacy PACS to PIV-enabled PACS.
Agency Code		
Organizational Identifier		
DUNS		
Card Universal Unique Identifier (Card UUID)	✓	The Card UUID is a 16-byte binary representation of a valid Universally Unique Identifier (UUID) (RFC4122) that uniquely identifies the "card" (e.g., 70af3fab-507e-4310-8047-21965f6697e3). The Card UUID was added to the PIV data model to support an alternative card identifier from the FASC-N. The Card UUID has been applied for use in the PIV-Interoperable (PIV-I) card data model. PIV-I credentials were originally issued by non-Federal issuers (e.g., private-sector organizations), but some agencies are now issuing PIV-I cards for short-term or temporary employees or contractors whose terms of engagement at the agency are less than six months. For non-Federal issuers, a PIV-I credential may have no valid Agency Code, System Code or Credential Number to populate the FASC-N. Up until the recent past, agencies issued PIV cards with a Card UUID set to all zeros (e.g., 00000000-0000-0000-0000-000000000000), but are now issuing a valid UUID for PIV cards. The Card UUID changes every time a PIV-I card is reissued, replaced or updated.

CHUID Data Element	Unique Identifier	Description
Cardholder Universal Unique Identifier (Cardholder UUID) (optional)	✓	The Cardholder UUID (not to be confused with the CHUID, "Cardholder Unique Identifier") is an optional 16-byte binary representation of a valid Universally Unique Identifier (UUID) (RFC4122), as with the Card UUID. However, the Cardholder UUID uniquely identifies the "cardholder" instead of the "card." Thus, reissued, replaced or updated PIV cards for a cardholder will have the same Cardholder UUID, which can span multiple issuance of PIV cards for an individual across an agency, or across multiple agencies (pending a Cardholder UUID clearinghouse that issues Card UUID's across all agencies). When a new credential is issued, a PACS can simply match the Cardholder UUID with the Card UUID in the new credential and assign access privileges.
Card Expiration Date		
Authentication Key Map		
Issuer Asymmetric Signature (Content Signing Certificate)		

10 APPENDIX B: How PIV Digital Certificates and Keys Are Validated During Authentication

A digital certificate is a data object that proves an entity (e.g., PIV card) has control of a public key (within the certificate), and an associated, but separate private key. Digital certificates include information about the embedded public key, information about the identity of its owner (e.g., PIV cardholder), and information on how to validate the digital certificate with the certificate's issuer (i.e., certificate authority).

Digital certificates are based on PKI asymmetric cryptographic key pairs; i.e., the public key and the private key. These keys are the basis of the PKI authentication topics discussed in this document. The key pairs are mathematically linked when generated, such that data can be encrypted with the private key and decrypted with the public key (and vice versa). Private keys never leave the devices (e.g., PIV cards) that own the associated digital certificates with their paired public keys.

For PIV smart cards, two digital certificates can be read from the cards through either the contact or contactless PIV-card interface. These two digital certificates are the Card Authentication Key/Certificate (CAK) and the PIV Authentication Key/Certificate. See Table 9 in Appendix A for a more detailed description of these digital certificates and their applicability for contact and/or contactless interfaces to smart card readers used for PIV card PKI authentication at points of entry controlled by a PACS.

Figure 10 provides a simplified illustration of how these keys and certificates can be used to perform PKI authentication (employing the challenge/response technique) at PACS entry points to verify that a person is in possession of a valid PIV card.

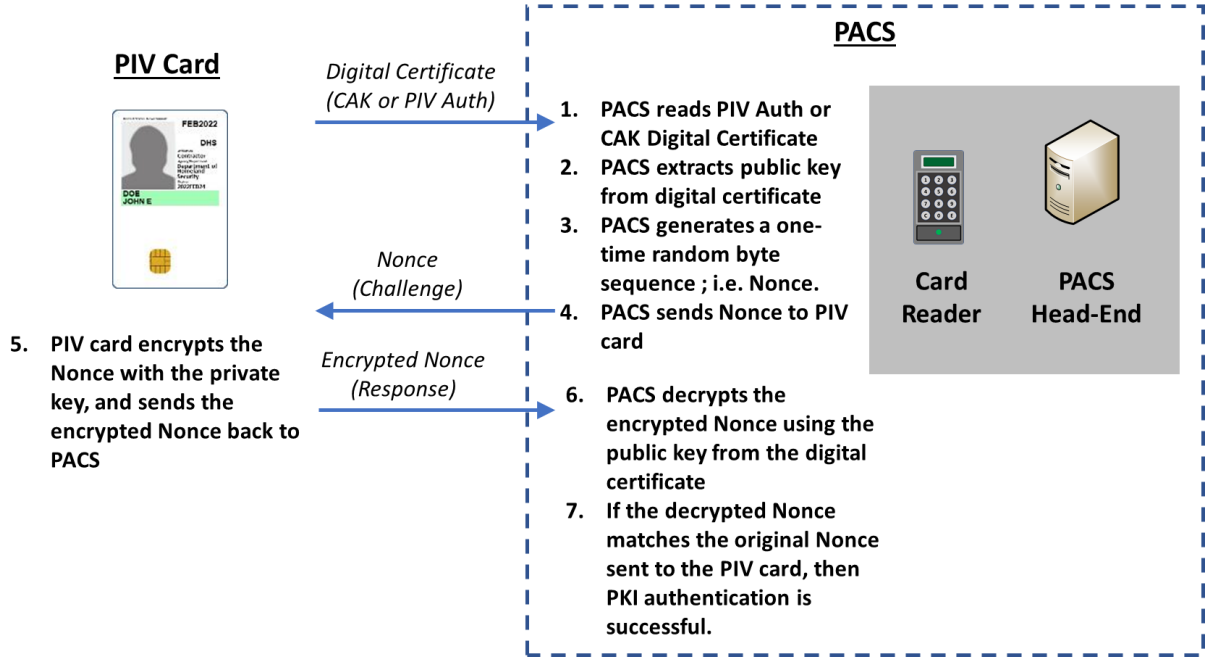

Figure 10. PKI Authentication at the PACS

11 APPENDIX C: Limitations of Legacy Physical Access Control Systems

Most legacy PACS were designed to use simple access cards that used short card identification numbers/identifiers. A card identifier is used to identify a specific card and user record and access the authorization level in the PACS card/user database. Due to limitations in storage and wiring at the readers and control panels, these legacy PACS could not process the longer identifiers and data elements introduced by the federal PIV cards (e.g., CHUID, and digital certificates) and could not perform the required authentication mechanisms. In general, legacy PACS do not support cryptographic certificate-based authentication, and typically cannot be readily retrofitted or upgraded for the necessary support.

Most legacy PACS used, and many still use, a proprietary data model that, for security reasons, limited interoperability of cards among systems made by different manufacturers, and in many cases, also limit interoperability among different locations where systems of the same manufacturer are deployed.

Authentication Capability

Legacy PACS readers often use proximity or magnetic stripe technology to interface with identity cards and use proprietary protocols to communicate data and execute processes. Some of these proprietary protocols employ cryptography, but not in ways acceptable for PIV credentials.

The introduction of high-assurance credentials, such as but not limited to PIV cards, has had a dramatic impact on PACS manufacturers. In this context, a high-assurance credential is defined as an identity credential that provides a high level of assurance that:

- The presented card is issued by a trusted issuer;
- The information in the card is not altered by an unauthorized entity;
- The card is authentic and valid;
- The person who is presenting the card is indeed the authorized user of the card; and
- The person presenting the card is still employed by the claimed organization.

To support these requirements, FIPS 201 added a standardized contactless and contact interface, PIN, biometric fingerprints, optional iris images, and cryptography to the card that could be used to attain a higher level of identity authentication assurance. The capability to perform bidirectional data communication is fundamental to the deployment of secure building access. Adding cryptography to the cards permits agencies to validate the data objects on the card and authenticate the cardholder. Adding credential expiration and credential validation requirements also strengthens authentication.

This enables improved control of access privileges. An APL-Listed PACS that is configured to automatically check validity status of registered PIV cards as a component of an enterprise PACS enables access privileges to be removed within one day for a card that is revoked. This is especially beneficial when a person leaves the employer organization and had been issued a card that was registered for access privileges in many systems in many locations.

Door Reader Interface

PIV and PIV-I cards use identifiers that are designed to accommodate significantly larger user populations and have a much larger, more unique identifier than previously used. These large identifiers presented a significant challenge for most PACS manufacturers.

The FIPS 201 requirement to authenticate the card and cardholder and validate the authenticated credential required major engineering and research and development efforts for the PACS manufacturers.

New card-to-reader and reader-to-PACS interfaces had to be developed.

Communication Infrastructure

Wiring associated with the existing PACS being considered for an upgrade or retrofit must be assessed for capacity to transmit data bidirectionally, and at higher speeds. Many recently installed systems use higher bandwidth cables, which might be 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 replacement of older, legacy wiring. Even so, existing wire can be used to pull new wire, reducing labor costs, and conduits can often be reused as well.

Hardware Upgrades

Often the existing controller panels and conduit infrastructure can be reused, replacing only the printed circuit boards, power supplies and battery backup when retrofitting or upgrading. This approach can realize significant cost savings.

Software Upgrades

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

A PIV-enabled PACS that is listed in the GSA FIPS 201 Evaluation Program Approved Products List eliminates or substantially reduces each of these limitations, relative to legacy PACS installations.