AN INTRODUCTION TO PHYSICAL ACCESS CONTROL SYSTEMS

Physical Access Control Systems (PACS) are a key component of the overall security capability of Federal agencies and commercial enterprises as they seek to protect their employees, physical and intellectual property, and other stakeholders' interests. While these systems have been around for many years, the advent of Homeland Security Presidential Directive 12 (HSPD-12) has created a new focus on standardization of credentials and integration of PACS and their capabilities across the federal space.

At a high level, PACS functionality consists of the "four A's": Authentication, Authorization, Administration, and Audit. (Some might add a fifth: Analytics). Commercial PACS products package software components to provide these functions in an integrated and configurable manner. A PACS database stores security hardware device configurations and personnel identity information, to include unique characteristics that identify enrolled personnel who require access to a facility. Personnel are authenticated at areas within the facility based on levels of confidence that are associated with the value of the assets in the particular area. The confidence level is increased as one moves from public areas, like a cafeteria, to sensitive areas, like a data center.

Authentication of identities is a fundamental to the trust foundation and has evolved significantly in recent history. Policies and procedures for vetting identities have moved from local to enterprise (also known as federation), and they rely primarily on the same authentication factors used in determining logical security privileges:

- Knowledge factor – something you know, like a password
- Possession factors – something you have, like a token/credential
- Inherence factors – something you are or a biometric, like a finger print

NIST authentication established four levels to standardize the degree of confidence needed to establish an identity, with Level 1 being the lowest and Level 4 being the highest.

LEVEL	STANDARD	EXPECTATION
Level 1	Little or no confidence in the asserted identity's validity.	No identity proofing is required at this level, but the authentication mechanism should provide some assurance that the same claimant is accessing the protected area.
Level 2	Some confidence in the asserted identity's validity.	Single-factor remote network authentication relies on identity-proofing requirements through the presentation of identifying materials or information.
Level 3	High confidence in the asserted identity's validity.	Multifactor remote network authentication relies on identity-proofing procedures that require the verification of identifying materials and information.
Level 4	Very high confidence in the asserted identity's validity.	Authentication based on proof of possession of a key through a cryptographic protocol provides the highest practical assurance of remote network authentication. This level requires a physical token and strong cryptographic authentication of all parties and all sensitive data transfers between the parties.

Key Standards for PACS

The evolution of smartcards and the impetus of HSPD-12 have promoted the development of several key standards that provide the framework for current and future PACS development and implementations. The International Standards Organization (ISO), International Electrotechnical Commission (IEC), and the National Institute for Standards and Technology (NIST) have issued most applicable standards. Most of the architecture between readers, control panels, and control systems is proprietary.

The most impactful standards are those that address smartcards and their technology. Below are some of the key standards that pertain to these cards:

- ISO/IEC 7810 – deals with the physical characteristics for identification cards.
- ISO/IEC 10373 – addresses test methods relating to identification cards.
- ISO/IEC 10536 – addresses close coupling (<2 millimeters from reader) contactless cards.
- ISO/IEC 14443 – provides standards for proximity contactless cards (< 10 centimeters from reader).
- ISO/IEC 15693 – deals with vicinity card standards (<1 meter from reader).

Other key standards that apply to PACS include:

- Federal Information Processing Standard (FIPS) 201 – defines the standards for Personal Identity Verification (PIV) of Federal employees and contractors
- NIST SP 800-37 – Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-53 – Recommended Security Controls for Federal Information Systems
- NIST SP 800-73-1 – Interfaces for Personal Identify Verification
- NIST SP 800-76 – Biometric Data Specification for Personal Identity Verification
- NIST SP 800-78 – Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- NIST SP 800-96 – PIV Card / Reader Interoperability Guidelines
- NIST SP 800-116 – A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

The PACS Breakdown

To understand PACS, it is important to understand three key concepts:

- Intrusion Detection Systems
- Card Access Control Systems
- Integrated Access Control Systems

Intrusion Detection Systems

An intrusion detection system (IDS) identifies the breach of physical access points such as doors, windows, roof accesses, and other potential points of entry to a physical structure. Modern PACS were built around traditional intrusion detection technology and retain much of

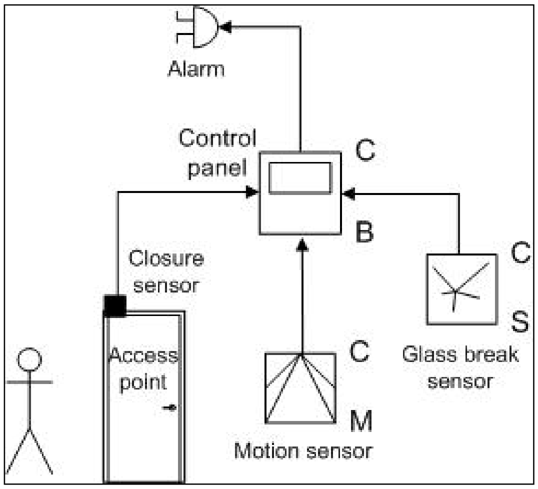

FIGURE 1 - BASIC INTRUSION DETECTION ARCHITECTURE

that architecture. There are four primary elements within a typical IDS: access points, sensors, the control panel, and the alarm (see Figure 1). As a point of reference, these can found in most residential alarm systems.

Access Points - Physical locations have various ingress and egress points throughout their premises. The most common access points include doors, windows, and roof hatches, but may also include vehicle gates and other types of perimeter security and controls.

Sensors - Access points may be armed with sensors that are triggered when certain conditions are encountered. Doors and windows may have contact or magnetic sensors that detect when they are opened or breached. Open spaces may also be monitored using motion (sonic or infrared), thermal, video, or seismic sensors. These sensors are designed and placed to detect their presence and trigger an alert if an intruder gains access.

Control Panel - The control panel is the backbone of an IDS. This panel is the central point where all sensors are wired and where power is supplied. All logic involved in assessing the state of sensors and determining when an intrusion has taken place is accomplished by the control panel. Within a larger facility, multiple control panels are usually networked together to form a complex, integrated system.

Alarm - When the control panel determines that an unwarranted intrusion has taken place, it will trigger an alarm. This typically includes triggering a bell, horn, or some other device to call attention to the intrusion. The control panel may also initiate automated activities such as closing/locking doors or notifying a remote location that is monitored by security personnel.

Card Access Control Systems

Card access control systems are built on an architecture similar to intrusion detection, but they use personal security cards as their primary access credential. Other credentials like PIN or biometric devices are frequently integrated along with more sophisticated software applications and communications platforms. The system grants or denies access when a card is presented to a door reader using the following steps:

1. User presents the card to the reader.
2. Reader decodes the card’s unique information and transmits the data to the control panel.
3. Control panel queries its onboard database of cardholder records and relevant access levels and determines if the user should be granted access.
4. If the card and relevant access level is valid, the panel will demagnetize the door lock. If access is denied, the panel will not unlock the door.

The transaction related data is typically logged at the system server with cardholder name, card number, and event type (access granted or access denied). Figure 3 depicts the access control architecture with access card and card reader technologies.

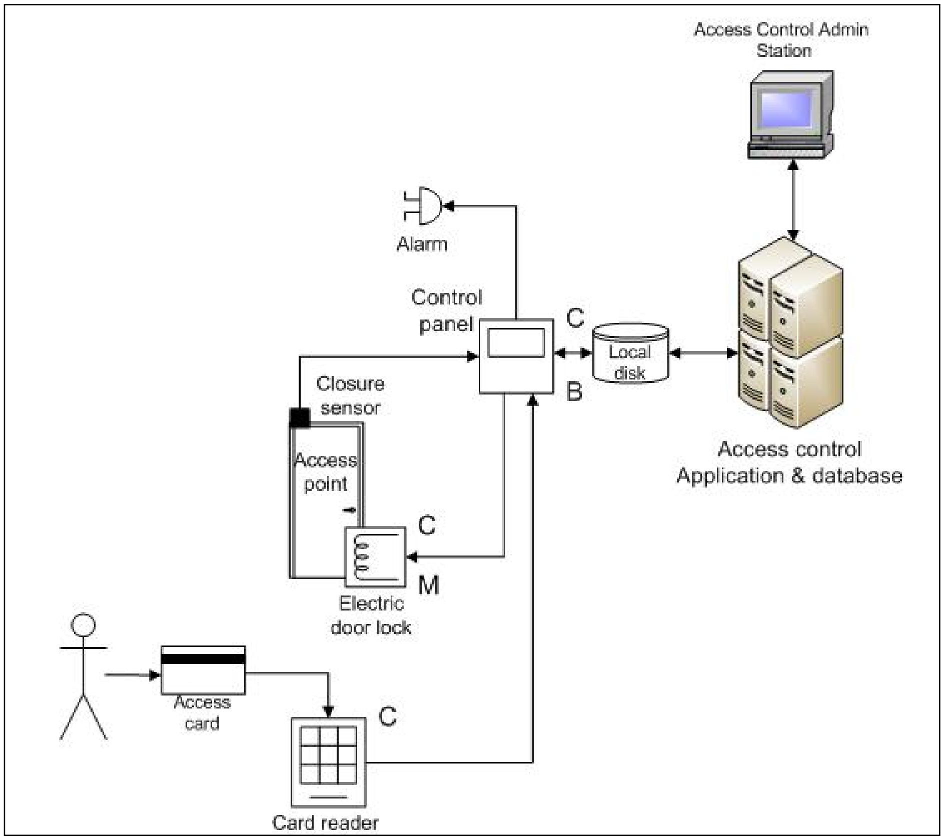

FIGURE 2 - ACCESS CONTROL USING ACCESS CARDS

Building upon our intrusion detection and basic access control architecture, the following components have been introduced by access card technologies: access cards, card readers, an access control application and database servers, local disk storage, and an access control administration workstation.

Access Card - An access card is a possession credential. It is a plastic card with personalized data encoded on it, and the data may be stored on any of the following media types that are embedded or imprinted on the card:

- Contact: Requires the card to be in physical contact with the reader.
  - Magnetic Stripe
  - smartcard (contact type)
- Proximity: Requires the card to be with in RF range of the reader.
  - Wiegand Antenna Coil or Prox technologies
  - smartcard (contactless type)
- Optical: Requires the card to be optically scanned by the reader.
  - Bar Code

Card Reader - The card reader is the device used to read the data from a card. Card readers are wired to the control panel and transmit the information that is read from a card to the panel.

Card readers can be coupled with keypads, and a control panel that is programmed to enforce a two-level authentication (both possession and knowledge credentials) requires a user may also be required to enter a valid passcode to gain entry.

Access Control Application and Database Servers - Control panels for access cards are typically integrated with an access control application and associated database. These software components provide flexibility and enhanced capability in the performance, management, and administration of access card systems. User information is entered into the access control system and is associated with a unique card number. When the control panel presents the card information to the software system, the software system validates the card number and determines whether the user should gain access based upon the privileges that were granted to the user by the security administrator.

Access control applications also allow more sophisticated access policies to be implemented broadly within a site in a timely manner, such as only allowing specified users to have access to a given area when certain conditions exist. These applications and databases can also log intrusion, access, and system health status events as they occur. Such logging can be used to determine usage patterns and to support various analytics and forensic needs.

Local Disk Storage - Due to data bandwidth constraints within the access control system, control panels are usually supported by a local disk database contained within the panel to speed access decisions. Once a user has been successfully authenticated to the access control application, a local copy of the user’s profile may be downloaded to the local disk for future authentications. The local disk database must be periodically refreshed from the access control application to ensure that a user’s status is properly reflected.

Access Control Administration Workstation - The access control administration workstation is the point where a user’s information is established and managed within the system. The application may also provide a graphical user interface that allows the system administrator to manage system configuration in addition to user records.

Integrated Access Control Systems

In 2004, Homeland Security Presidential Directive 12 (HSPD-12) mandated the establishment of standards for identification of Federal government employees and contractors. The resulting forms of identification are to be:

- Issued based upon sound criteria for verifying an individual employee’s identity.
- Strongly resistant to identity fraud, tampering, counterfeiting, and exploitation.
- Rapidly authenticated electronically.
- Issued only by providers whose reliability has been established.

Key standards that apply to HSPD-12 are identified in a subsequent section of this paper.

HSPD-12 also requires the use of a common identification credential for both physical and logical access to Federally-controlled facilities and information systems. As a result of this directive, access control systems are becoming much more integrated and standardized across sites and across Federal agencies. Figure 4 depicts changes to the basic access control architecture to support HSPD-12.

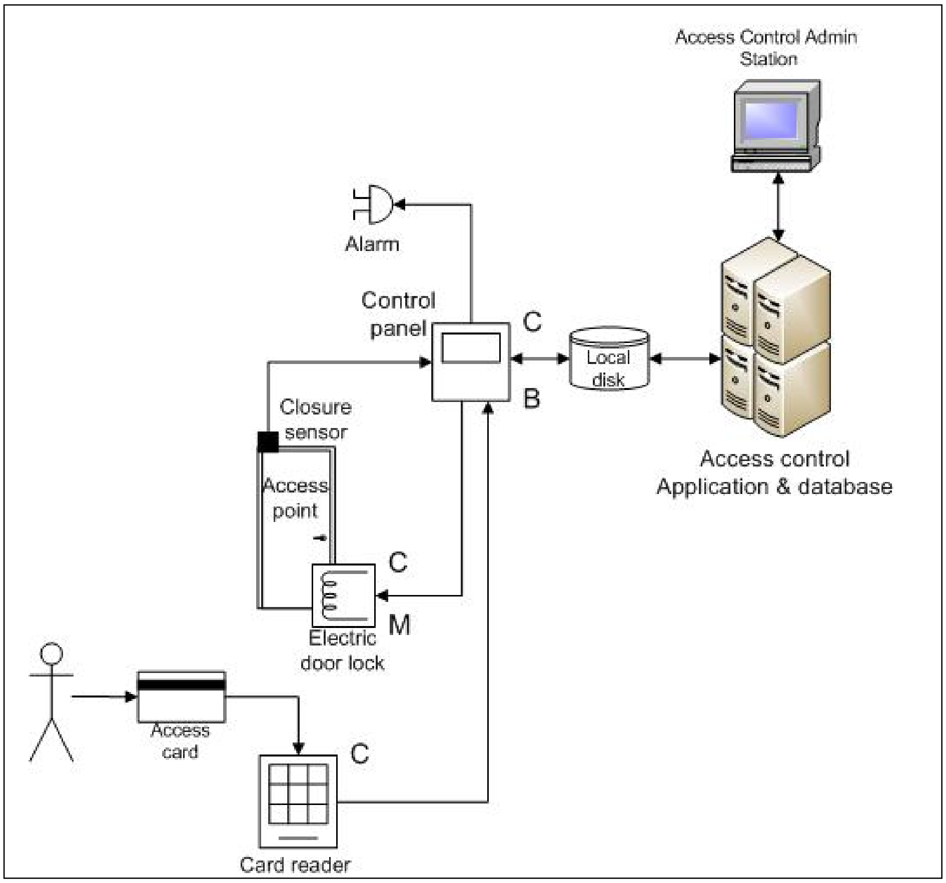

FIGURE 3 - INTEGRATED ACCESS CONTROL

Several new components have been added to the PACS architecture and some existing components have enhanced functions. Below is a brief overview of these components:

PIV Card - The Personal Identification Verification (PIV) card is a new, more versatile access card and is the foundation for the HSPD-12 requirements. PIV cards represent many improvements over the magnetic stripe cards; they have been designed around the new standards and support all but the most rigorous of identification requirements.

PIV design and implementation is based upon contactless technology that only requires the card to come into proximity of the card reader. PIV cards use microcontroller units (MCUs) embedded within the card, which allow the card to carry more data and provide computations on the card itself. The contactless technology on these cards means that they can support very sophisticated authentication standards, but some authentication standards still require contact capability. For this reason, most PIV cards also support contact technology and are called dual-interface cards.

PIV cards support the Federal Information Processing Standard (FIPS) 201 that incorporates four base standards:

1. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73: “Interfaces for Personal Identity Verification”, which specifies the interface and data elements of the PIV card.

2. NIST SP 800-76: “Biometric Data Specification for Personal Identify Verification”, which specifies the technical acquisition and formatting requirements for biometric data of the PIV system.
3. NIST SP 800-78: “Cryptographic Algorithms and Key Sizes for Personal Identity Verification”, which specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.
4. NIST SP 800-116: “A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)” which:
   - Discusses the different PIV Card capabilities to align risk-based assessment with the appropriate PIV authentication mechanism
   - Introduces the concept of “Controlled, Limited, Exclusion” areas to employ risk-based PIV authentication mechanisms for different facility areas
   - Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations
   - Recommends to Federal agencies an overall strategy for implementing PIV authentication mechanisms with agency facility PACS

Contactless Card Readers - PIV technology requires enhanced card readers that support advanced capabilities to integrate keypads and biometric readers. Since PIV cards use MCUs and may carry encrypted user data, much of the authentication process can be performed between the reader and the card with minimal communication with the control panel.

A card reader can capture and verify authentication information, such as passcodes entered into a keypad and biometric scans at an appropriate reader. Encryption and decryption may occur between the card and card reader or between the card reader and the control panel, mitigating the security risks associated with contactless and providing a highly secure communication channel.

Biometric readers - Biometric readers support the “who you are” credential requirements needed for high-confidence authentication and are readily supported by PIV technology. PIV cards can be loaded with biometric templates for various user metrics and a user’s measurements can be validated at the integrated card/biometric reader.

Identity Management System - The Identity Management System (IDMS) is the backbone of the PIV implementation. The standardized nature of PIV allows for centralized identity verification and credential management; it also facilitates integration of access control systems from many sites and across agencies.

Identity management covers the full life cycle of a user’s identity for Federal purposes. These lifecycle phases are:

1. Identify proofing and registration of an individual.
2. Enrollment in local PACS.
3. PIV card revocation or termination.

Identity proofing encompasses the processes to verify that an individual is, in fact, who they say they are. These processes require a National Agency Check with Inquiries (NACI) and having all required forms properly adjudicated and on file. These processes may require an individual to appear in person to a PIV official before a credential can be issued. Individuals may be required to provide multiple forms of identification, including picture identification issued by state or federal governments. Final registration occurs when all proofing has been completed and approved and the individual's data is entered into the IDMS.

Once an individual user is set up in the IDMS, he or she can be enrolled into the local PACS. The method of enrollment is dependent upon the specific PACS systems and the agency IDMS. It can be a fully automated "push down" of the user data or as simple as capturing the identification of a PIV card. Generally, the enrollment process encompasses the following activities:

1. Enter cardholder demographic data as required by the site administrator.
2. Enter the Card Holder Unique Identifier (CHUID) or a defined subset of the number. This is the number stored on the card and binds the user to the card.
3. Validate the PIV "chain of trust" to the level required by the site's agency.
4. Assign access privileges.

Lastly, the IDMS manages and tracks the PIV card revocation or termination. Granting or denying a user's privileges at a given site is the responsibility of the site security manager. However, the revocation of a PIV card means the card is no longer valid and should not be used for identity authentication. This level of management falls under IDMS responsibility.

Online Credential Status Protocol server - The Online Credential Status Protocol (OCSP) server handles queries regarding the status of a given PIV card. Having their digital certificates revoked by the issuing authority normally invalidates a PIV card. Once a certificate is revoked, the issuing authority makes this information available to OCSP servers, and the certificate may be added to Credential Revocation Lists (CRLs). The architecture of the PACS environment must ensure that appropriate CRLs are checked prior to granting access to a PIV. The IDMS may query these lists and push the data down to the appropriate PACS, or the PACS may query the appropriate servers to check the lists directly.

Card Management Issuance System - The Card Management Issuance System (CMIS) is responsible for creating, maintaining, tracking, and terminating PIV cards. While the IDMS manages user identification data and authorizes the creation of a credential, the CMIS manages the physical creation and issuance of the PIV cards. These functions include loading appropriate user data onto the card (e.g. CHUID and biometric data) and delivering the card to the user. By their nature, biometric measurements for an individual may change over time, as a result of a person's aging or due to other physical changes such as eye surgery. The PIV cards must be updated appropriately to reflect these changes. The CMIS is also responsible for managing PIV card termination to ensure that it cannot be re-used.

Technology Change Drivers

As noted in the discussion of PIV cards and contactless card readers, significant processing capability is now being pushed down to the lowest level components in the HSPD-12 environment, and the old component hierarchy is becoming less relevant. The basic architecture of today's PACS is still based on a hub-and-spoke configuration with the control panel as the hub. This architecture is based upon a hierarchy of functions and the limited capabilities of the various components. Due to the nature of this architecture, PACS have evolved in a site-centric manner driven by multiple proprietary vendor designs.

The reality of this evolution is that sites throughout a multiple-facility enterprise can have widely differing hardware and software implementations supported by different vendors. Consequently, managing user credentials and permissions across sites is redundant, is time consuming, and carries the inherent risk that changes to a user's access privileges may not be reflected consistently or on a timely basis.

In future HSPD-12 environments, the implementation of internet protocol version 6 (IPv6) will enable all components in the architecture to become IP addressable and will support a more peer-to-peer architecture. As components become IP addressable, they will become more standardized, commoditized, and less proprietary. There are data security issues with this direction since data that would previously pass through the control panel may be directed across a network. However, as these issues are addressed and resolved, overall PACS costs should be reduced. One can foresee systems where a smart card reader could access the access control system directly or query an OCSP server to validate a certificate without having to pass through the control panel and access control applications.

The increased security of wireless technology also presents an opportunity for evolving the physical access control architecture. Especially where facilities are distributed over a relatively close geographic location, a wireless mesh network allows a central access control system to manage multiple card readers without incurring potentially prohibitive costs to rewire the facility. This model leverages the encryption/decryption handshake between the PIV card and the control panel and couples it with WPA2 standards for secure wireless transmission of data to the access control system when required.

Conclusion

HSPD-12 has definitely changed the landscape for the evolution of PACS and will continue to do so. Older proprietary intrusion detection and access control architectures are being challenged to accommodate the new requirements. Standards mandated by HSPD-12 and related technology developments in the areas of smartcards, smart readers, and IP addressability will drive changes to the architecture for PACS design and implementation. Broader rollout of smartcards and HSPD-12 compliance will increase demand for PACS integration with Identity Management Systems, and evolving security policies will drive higher dependence on real-time certificate authentication from the issuing authorities. These backend systems will likely become the focus of future PACS architectural designs.