Smart Card Alliance

Authentication Mechanisms for Physical Access Control

A Smart Card Alliance Physical Access Council White Paper

Publication Date: October 2009

Publication Number: PAC-09002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1 Introduction

In December 2003, the Office of Management and Budget (OMB) issued M-04-04, "E- Authentication Guidance for Federal Agencies."[1] Subsequently, the E-Authentication Initiative (EAI) was established to assist agencies in their efforts to develop trust relationships with their user communities through the use of electronic identity credentials. Homeland Security Presidential Directive 12 (HSPD-12), signed in August 2004, set the policy for a common identification standard for Federal employees and for contractors who are conducting business with Federal agencies and who require access to physical and information technology (IT) resources. In February 2005, in response to HSPD-12, the National Institute of Standards and Technology (NIST) Computer Security Division developed Federal Information Processing Standard (FIPS) 201 *Personal Identity Verification (PIV) of Federal Employees and Contractors,*[2] and, subsequently, Special Publication (SP) 800 73-1 and SP 800 73-2, *Interfaces for Personal Identity Verification*,[3] to define the technical requirements and specifications for a common identity credential. These identity credentials are referred to as personal identification verification (PIV) cards.

The EAI provides the capability for any government agency to validate an electronic identity credential to authenticate an individual's identity before that individual is granted access to IT or physical resources. To accomplish this, the PIV card incorporates multiple technologies that, in combination, establish a level of trust in both the individual's claimed identity and the validity of the credential itself. The process relies on possession of the PIV card, methods that bind the credential to an individual through biometric verification, and special knowledge (a personal identification number (PIN)). Authentication and validation are accomplished using cryptography and public key infrastructure (PKI) to validate the PIV certificate to a certificate authority (CA). The validation process is accomplished according to a common, federated identity model that defines both the policy and the technical infrastructure for identity management.

Applying these electronic identity credentials to a physical access control system (PACS) requires both technical infrastructure and guidance policies. HSPD-12, FIPS 201, NIST SP 800-73, and NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*,[4] are examples of the regulatory and guidance framework that are required for successful implementation of a project of this magnitude.

Recognizing that implementation will take time, goals and plans should be developed to guide the migration of current PACS while still satisfying continuity of operations and resource constraints. Migration plans may include strategies such as using multi-technology PACS readers that enable the gradual transition to a PIV card-enabled PACS; these would allow proprietary legacy identity cards and PIV cards to work side-by-side in the same PACS.

SP 800-116, published in November 2008, provides useful guidance on where to deploy the various PIV authentication mechanisms. However, a number of scenarios are not covered. Local security authorities are left with unanswered questions when faced with legacy technologies and occasionally conflicting regulations. This document highlights some of these situations and suggests some additional authentication mechanisms for security authorities to consider.

[1] http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

[2] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[3] http://csrc.nist.gov/publications/PubsSPs.html

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

2 NIST SP 800-116

NIST has released a document that is likely to have a significant impact on all PACS in use at Federal government facilities. The document, SP 800-116, is titled *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*. At the heart of this document is the message that a comprehensive security risk assessment will enable facility security managers to define the necessary authentication mechanisms to be deployed in response to threats to different secure areas of a facility.

SP 800-116 redefines how the PIV card issued to Federal government employees and contractors should be authenticated for physical access control. This new recommendation goes well beyond what typical PACS implementations have done in the past. Such a drastic change will cause all Federal government agencies to reevaluate their systems, their ability to achieve compliance, and the costs associated with upgrading. Additional authentication methods will also need to be considered before making final decisions on how a facility should be secured.

In FIPS 201, NIST defines a *normative* document as one specifying mandatory items or requirements. Other documents can be referenced for informational purposes and, thus, are only *informative* with respect to FIPS 201. Such documents present recommendations or comment on general considerations. SP 800-116 is an informative document; while providing very specific information, it does not prescribe requirements associated with FIPS 201.

SP 800-116 is intended to show the authentication methods that are available using the PIV credential. SP 800-116 recommends the number of factors and types of authentication that should be used to identify people who are entering different areas. However, SP 800-116 is silent on many common identity authentication methods that are not part of the PIV card, such as PIN-to-PACS (see Section 4.2.4) or biometrics stored on a server.

Another useful section of SP 800-116 is the description of a PIV Implementation Maturity Model. This is an excellent mechanism for identifying and tracking the progress made toward a full implementation of the PIV credential for physical security.

2.1 SP 800-116-Defined PIV Authentication Mechanisms

The goal of access control is to admit only authorized personnel to a particular location. Authentication mechanisms use authentication factors to achieve this goal. A process relying on one or more authentication factors in an identity-based transaction constitutes an authentication method.

The authentication of an identity is based on verification of one, two, or three of these factors:

- Something you have (for example, possession of a PIV card)
- Something you know (for example, knowledge of a PIN)
- Something you are (as proved, for example, through presentation of live fingerprints by a cardholder)

FIPS 201 provides a standardized framework that allows interoperability of PIV and PIV-I[5] credentials. Without such a standard, agencies would be unable to trust the identity vetting associated with and the authenticity of credentials issued by other agencies. Providing this framework for trust is a crucial element of HSPD-12.

[5] FIPS 201 was initially developed for interoperability of the PIV credential issued to Federal government employees and contractors. However, other non-government programs have adopted the standard. Therefore, a variety of terms have arisen to define various levels of expected interoperability with the Federally issued PIV cards. PIV-I describes a card based on FIPS 201 that is not issued by an agency of the Federal government and therefore is not a PIV card. However, the PIV-I card meets all of the requirements of FIPS 201 and is interoperable with PIV cards through the Federal Bridge. PIV-compatible cards are cards that are developed to provide similar functionality to the PIV card but cannot guarantee the uniqueness of the prescribed FASC-N. (This card may be unique within a closed environment or may use the GUID as a UUID defined in RFC 4122 to provide the desired level of uniqueness.)

SP 800-116, Table 7.1 provides the following definitions for authentication mechanisms.

2.1.1 One-Factor Authentication

According to SP 800-116, the following authentication methods are considered one-factor methods—something you have or something you are.

- *CHUID + VIS* (something you have): Authenticates the Cardholder Unique Identifier (CHUID) with CHUID signature verification and a visual (VIS) inspection of the credential.
- *CAK* (something you have): Performs a challenge and response using the card authentication key (CAK). Note that, according to FIPS 201, the CAK is an optional key and can be either symmetric or asymmetric. SP 800-116 assumes that the CAK is present and asymmetric.
- *BIO*, or *biometric* (something you are): Matches the fingerprint template stored on the card to a live sample collected at the reader. The biometric data object must be signed in order to be trusted and recognized as an identity factor.

2.1.2 Two-Factor Authentication

According SP 800-116, the following authentication methods are considered two-factor methods: both possession and physical attributes (something you have and something you are), or both possession (something you have) and something you know.

- *BIO-A* (something you have (the card) and something you are): BIO-A (biometric attended) authentication is the same as BIO, except that a trusted agent is present and witnesses the transaction.
- *PIV Auth Key*, *PKI Authentication* (possession and something you know): With this method, the PIV card is inserted in a contact reader and a PKI challenge and response to the PIV authentication key (PIV Auth Key) is performed. Access to the PIV authentication key requires the PIN for the card. This method validates the card and, therefore, the use of the PIN from the card (PIN-to-card).

2.1.3 Three-Factor Authentication

According SP 800-116, Card + PIN + BIO-A is considered a three-factor method: possession, something you know, and physical attributes. CHUID + VIS or CAK is used to authenticate the card as described above. In addition, the PKI Auth Key and BIO-A are used to achieve three-factor authentication.

SP 800-116 does combine multiple authentication mechanisms to provide a higher level of trust in a claimed identity for authorizing access to areas requiring more robust security. However, SP 800-116 does not cover how to combine PIV authentication methods with non-PIV methods to provide the same level of trust. These non-PIV methods provide the cognizant security authority (CSA) or security manager with a wider range of options and may reconcile otherwise conflicting requirements.

The Smart Card Alliance has written a number of white papers to explain these options. These white papers can be downloaded free of charge from http://www.smartcardalliance.org/pages/activities-councils-physical-access.

2.2 Impact of SP 800-116 Authentication Mechanisms on PACS Integration

As SP 800-116 authentication methods are increasingly deployed and used, they will impact access control points.

First, PIV card transaction times are longer than cardholders are used to, and this may reduce the throughput at access control points. Second, some of the authentication mechanisms use optional data objects that may not be available for all PIV credentials. This may become an issue when personnel whose credentials were issued by another issuer try to use their credentials on an agency's PACS. And last, PKI, BIO, and BIO-A authentication mechanisms require a contact reader, which may be an issue for outdoor access points.

2.3 Challenges for Authentication Using SP 800-116

With all of the new capabilities and requirements, interoperability of the PIV credential across different PACS may require system upgrades or system replacement.

The intent of a PACS is to allow access only to those individuals with credentials registered at a particular authorization level with the PACS. In an interoperable world, all PACS should, at a minimum, be able to read a presented credential to determine whether access is authorized. This interoperability requires that all credentials be encoded using a common data structure that is designed to guarantee a unique identifier for each credential within the intended user population. NIST recognized this requirement, and also recognized that not all agencies would be able to make use of very large identifiers like the Global Unique ID (GUID) or be able to support digital certificates and PKI. Therefore, a minimal solution is also allowed: the Federal Agency Smart Card Number (FASC-N), including the expiration date.

NIST faced a difficult situation. If agencies are allowed to implement solutions for access control without card authentication, there is potential for counterfeit cards to be used undetected in the system. If such an event occurs and the system breached is in compliance with FIPS 201, the breach will erode trust in the standard, which was designed to meet the security requirements of HSPD-12. As a result, NIST published SP 800-116 to provide guidance on using PIV credentials with PACS.

To mitigate vulnerabilities of this kind, data objects (such as the CHUID) can be digitally signed. The PIV card can use the private-key CAK to sign a challenge from the reader. The successful completion of the CAK challenge-response indicates that the data object can be trusted. A similar approach can be used to authenticate a biometric template stored on the PIV card, preventing template substitution.

When implementing a FIPS 201-compliant PACS, each security manager will need to consider the following:

- Evaluate and define upgrades required for the operational (legacy) PACS.
- Assess and inventory the types of PACS in use. Multiple facilities under a security manager's control may have PACS manufactured by different manufacturers. Each PACS may be a different version and model than every other PACS, so an enterprise-wide solution could be more complex.
- Identify funding for PACS upgrades.
- Determine the FIPS 201 training required for PACS owners and operators. The learning curve may add to the challenge of defining the upgrade path.
- Determine how the PACS upgrade will handle longer data streams and larger user records. Even if a PACS has been upgraded to accept PIV cards, only the first three to five fields of the FASC-N (providing up to 16 digits of an identifier) are processed. While this provides for a unique credential, it does not provide support for the level of authentication detailed in SP 800-116. Since most legacy or current generation PACS control panels do not satisfy the requirements of SP 800-116, additional integration will be required. For example, a new generation of PACS card readers is emerging that can offload some cryptographic and PKI authentication requirements. In this case, the reader may need an Ethernet connection to the certificate authority (CA) or the Federal Bridge to handle the certificate revocation list (CRL) or online certificate status protocol (OCSP) functions associated with PKI.
- Determine the ability for the legacy PACS to be upgraded to support PKI (in most cases replacement will be required), or define acceptable options to SP 800-116 that meet security requirements without using PKI.

3 System-Level Considerations for Authentication Mechanisms

Figure 1 shows a typical PACS architecture. A card reader (CR) is located at each access control point such as a door or gate. The PACS user presents their ID card to the reader and the reader sends the card data to the access control panel (ACP) for a decision to grant or deny access. This decision is based on parameters determined by local or agency-specific policies that are programmed into the system by PACS operators using one or multiple workstations connected to a PACS server. This approach allows multiple operators to perform simultaneous system operations (e.g., adding/deleting users, generating reports, monitoring and processing system alarms).

A PACS server stores all user records and access privileges, as well as other system parameters. In addition, the PACS server maintains system events, such as access transactions, and makes them readily available for audit purposes.

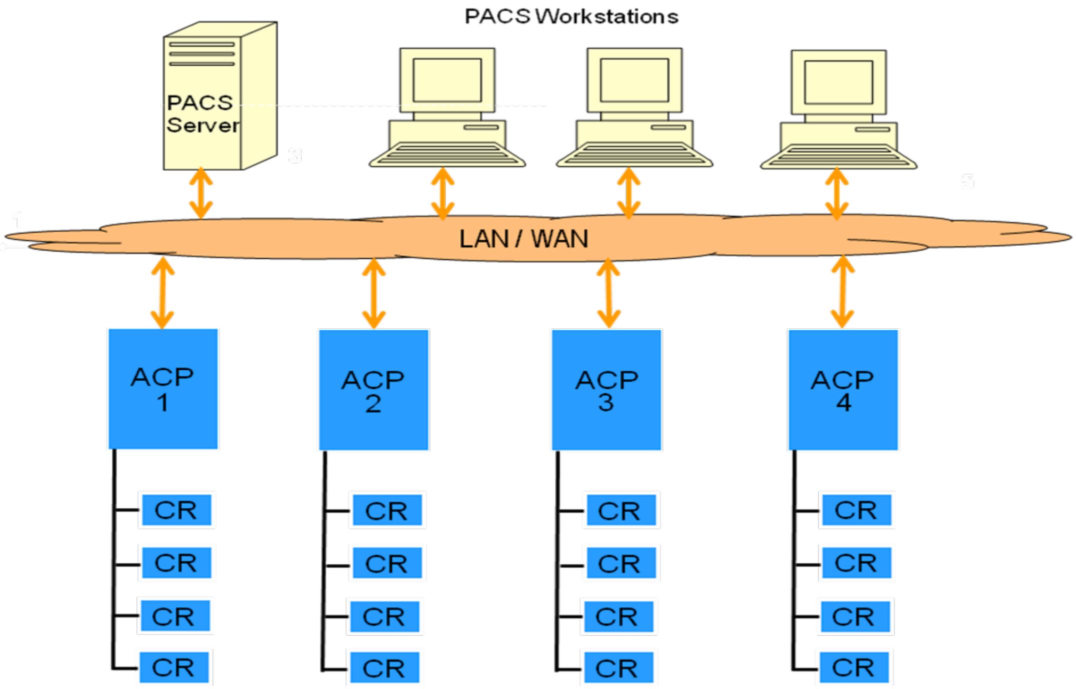

Figure 1. Typical PACS Architecture

3.1 Identity Object Repositories

Identity objects, such as biographical data objects, biometric data objects, or digital data objects (PKI-associated), can be stored in various modules or containers that are designed for such purposes (identity object repositories). Security mechanisms (such as cryptography) can be incorporated to offer secure repositories for sensitive information (e.g., personally identifiable information). In a PACS, such repositories may include the reader unit itself, the ACP, and the host database, which is located on the PACS server or on a separate database server. Note that any module that uses cryptography to secure data must comply with FIPS 140-2 *Security Requirements for Cryptographic Modules*.[6]

It is necessary to communicate or transfer identity objects among the various components of a PACS implementation. Securing the data that is associated with identity identifiers, both during this transfer (in

[6] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

motion) and when the object is deposited in an identity repository (at rest), is necessary to assure the overall security of PACS key management and is a consideration when data is encrypted.

Identity repositories are storage locations for the objects that are intended to be secure and kept from unauthorized access. The availability of this data must be protected using identification and authentication methods applicable to logical or digital systems. The type of access control typically associated with logical access control systems (LACS) can also be applied to a PACS, as a PACS is now officially classified as an IT system. (The FISMA certification process is now required for PACS.) Data and data storage locations are now subject to access control, as are associated networks and network domains.

Since authentication mechanisms are required to execute data access inquiries, the assurance levels associated with these inquiries can also be classified using the e-authentication assurance levels of confidence: Some, High, and Very High. Achieving the different levels of confidence can be accomplished by using multi-factor authentication options (see Section 2.1.3). A PACS using a three-factor authentication process can offer very high confidence that the identifiers belong to the cardholder. The identifiers available on the PIV credential can thus be used for a data access request as well as for access to a physical portal. This identification and authentication security layer is important, as otherwise false identities or even valid (but not authorized) identities can be entered into the database

In addition to the challenge and response typically associated with a credential at the reader and with the user of the PACS as an IT system, component-to-component communications or module-to-module communications must also be secure and data integrity must be maintained. Each module that decrypts data must re-encrypt the data before passing it to the next system component. A PACS can incorporate both intrasystem encryption techniques for use in communications processes and IT-defined mechanisms such as secure sockets layer (SSL)-supported connections. To assure that the entire end-to-end process is trustworthy, each link of the chain should maintain the same level of confidence as the entire chain.

3.2 PACS Provisioning

HSPD-12 and FIPS 201 forced a paradigm shift on PACS. One of the fundamental changes for PACS is the manner in which identities are established for use in granting access to cardholders. Requests received from portal devices when credentials are presented to readers are now subject to an end-to-end control procedure that is established locally and may be connected to the government PIV IT infrastructure.

Traditionally, the PACS for a facility was under the administrative control of a security officer or the director of security for the facility, and typically the credentials issued for use with the PACS were established by the same department or in cooperation with a different department in the same organization. Under these conditions, the processes relating to establishment of an identity, the provisioning of the PACS, and managing the life cycle of the credential were isolated to and controlled by the same organization.

This independent and flexible process is no longer applicable to a PACS that satisfies FIPS 201 requirements. The main reason is that an identity and the associated identity objects (identifiers) are no longer under the control or sole jurisdiction of the PACS owner or administrator. The former closed-loop PACS environment no longer exists. New credentials are created by a process outside of the PACS credentialing and badging environment. As a consequence, the unique identifiers that the PACS relies on to grant access are “unknown” to the PACS administrator, and therefore, credentials presented to PACS components are not recognized. To be recognized, they have to be registered (or provisioned) into the PACS by a process that transfers the correct identifiers from the credential into the PACS database so that card or credential profiles within the PACS application can use them to assign and maintain an individual enrollee's privileges.

Three fundamental methods are used to provision unique identifiers into a PACS application’s database. First, a live, in-person enrollment process can be performed (for HSPD-12, this is the established FIPS 201 process). As part of the enrollment process, unique identifiers are collected or created and transferred through a provisioning mechanism directly to the PACS application database (or transferred to the database from the HSPD-12 identity management system (IDMS) central identity store). This passes the unique identifier created by the FIPS 201 process to the PACS for enabling privilege configuration.

The second method transfers the identity objects or identifiers from a database considered to be the "authoritative database" for the PACS database. The authoritative database could be a human resources (HR) database that has been provided with the FIPS 201 unique identifiers created by the FIPS 201 process. The HR database now becomes the authority for the PACS database. The identifiers encoded on the card are the same as the identifiers in the PACS database.

The third method transfers identity objects or identifiers from the PIV card to the PACS database through a provisioning process referred to as "data harvesting" or PIV card data collection and PACS provisioning. This process identifies the card itself as the authoritative data source, since it was created using a trusted process defined by FIPS 201. To assure that the unique identifiers collected and provisioned into the PACS are usable by the PACS application, middleware is often used between the data harvesting and PACS connection elements to assure that the raw data is parsed and provisioned in accordance with the data model expected by the PACS.

A variety of post-provisioning authentication mechanisms can be enabled, depending on which containers are opened on the PIV card and what data elements are retrieved and provisioned into the PACS. For example, if all of the digital certificates are captured and stored, certificate status can be checked periodically. If an expiration date is captured and used as the valid date for PACS privilege activation periods, then PACS authorization can be suspended after the expiration date is reached, in full compliance with FIPS 201 requirements. Stored certificates can also be periodically validated in accordance with the 18-hour window allowed for de-provisioning if a certificate is found to be revoked. For authentication mechanisms to be enabled, authentication objects must first be captured from the credential. Those provisioned in the PACS can be established for automatic and repeated validation, while those captured at the portal and not stored will be checked at the time of access request.

During the provisioning process, manual and automated procedures can be established to assure that the data being captured and provisioned is authentic. If the database-to-database method is used, IT best practices and standards can be implemented to create secure transmission links, and PKI can be used to digitally sign or encrypt the data (e.g., using SSL connections for communications). These procedures follow IT security best-practices models for machine-to-machine communications. If the data harvesting method is used, the expiration date, PIN, facial image, and fingerprint template can be challenged and authenticated when the PIV card is presented to the PACS.

As part of PKI-based authentication (further described in Section 4), the certificates available from the credential can also be verified against a valid chain of trust by using path discovery and validation. If the chain can be traced back to a trust anchor, the data source can also be trusted. Performing similar validation checks against the signing certificates can also offer assurance that the data has integrity.

The use of established protocol standards, such as online certificate status protocol (OCSP) and server-based certificate validation protocol (SCVP), within the defined infrastructure for cross-certified PKI networks can also enable periodic real-time checks on or downloads of current certificate revocation lists (CRLs). This provides up-to-date status information on issued certificates. To comply with FIPS 201, when any PIV credential certificate is revoked, privileges and authorizations configured in a PACS must be removed within 18 hours of notification of revocation.

4 Additional Authentication Mechanisms for PACS

4.1 Requirements Driving Alternative Authentication Mechanisms

Not all possible authentication mechanisms are mentioned SP 800-116. This section describes some additional methods, their use, and the regulations mandating their implementation. This section also describes some emerging technologies that have been evaluated, tested, and successfully deployed by the PACS industry.

The following sections provide examples of requirements that are driven by functional necessities at a local level and that may dictate or require alternative authentication methods (for example, to accommodate throughput or equipment location).

4.1.1 Legislative Requirements

Legislative requirements that affect PACS configuration and user ID validation are often contradictory. For example, Section 508 of the Rehabilitation Act requires Federal agencies to make special arrangements so that people with disabilities that could affect their ability to access physical and logical resources (such as visual impairment or missing limbs) can access these resources. Section 508 requires Federal agencies to give disabled employees access to facilities and information that is comparable to the access available to others.

Section 508 could result in the need for multiple authentication methods, such as the option of using either a biometric or a PIN at certain access control points. It may also affect the height at which the readers are placed and the physical configuration of access control points to achieve acceptable throughput rates while accommodating all PACS users. In some cases, following SP 800-116 could conflict with conforming to Section 508.

4.1.2 Environmental and Site-Specific Requirements

In many cases, card readers are placed at weather-exposed outdoor access points, such as at maritime facilities or vehicle perimeter gates at manufacturing plants. This environment may preclude the use of contact smart card readers, due to concern over moisture and other airborne contaminants entering the internal reader electronics. In addition, variability in the environment across various access points within an installation may require the employment of different operational biometric modalities at selected access points, each driven by site- or location-specific environmental characteristics. One example would be a location where the variability of the lighting may preclude the use of certain biometrics, such as face or iris recognition.

4.1.3 Throughput Considerations

High volume access points may require fast end-to-end transaction times including card presentation or read, PIN entry, and biometric presentation or processing. As a result, concern over card presentation and data transfer times may suggest contactless operation with information stored off the card to minimize delays. One example would be the use of an operational biometric, where the biometric data is stored in the PACS, to eliminate the need for the user to enter a PIN to access the reference biometric stored on the card.

4.1.4 User Requirements

When biometrics are used as the primary authentication mechanism, it should be recognized that a small percentage of the population may not be able to provide a suitable biometric sample (for example, due to a disability). In this case, an alternative authentication mechanism or procedure may be required for people who cannot enroll using the primary biometric. Alternative mechanisms could include an alternate biometric (such as vein recognition in lieu of the reference fingerprint biometric), entry of a PIN, or visual inspection by a security guard.

For example, if a person cannot enroll a fingerprint, a special code can be placed in the PIV card memory and a PIN assigned as the primary authentication mechanism for this person. When the card is read, the reader will see the special code and prompt the person to enter a PIN instead of a biometric.

4.1.5 Migration Considerations

Legacy PACS may use a dedicated PIN managed by the PACS, or "*PACS PIN*." This PIN is separate and distinct from the PIN assigned at PIV card activation. However, it can be the same numerical value. Several agencies use PIV cards with a PIN to release a unique identifier from the card (the PIN-to-card mechanism). Often these card and reader technologies produce a different data stream from the 14-digit FASC-N, requiring the PACS to process both FASC-N and other data streams at the same location. Local security authorities may cooperate with system suppliers and integrators to identify the best way to accommodate these different user procedures and system processes and arrive at an appropriate authentication mechanism.

4.1.6 Policy Requirements

Agencies or contractors who must comply with intelligence community or Department of Defense (DoD) requirements such as the *Joint Air Force–Army–Navy (JAFAN) Manual 6/9*, the *Director of Central Intelligence Directive No. 6/9* (DCID 6/9)*, OPNAV INSTRUCTION 5530.14d,* and similar requirements, operate under conditions not mentioned in SP 800-116.

These security environments have specific requirements for physical access to a sensitive compartmented information facility (SCIF) and a special access program facility (SAPF). The main differences between these requirements and the requirements in SP 800-116 are the methods by which users are identified. DCID 6/9 requires either Card + PIN-to-PACS or biometric identification.

DCID 6/9 requires that the authentication mechanism used have a probability of no more than one in 10,000 that an unauthorized individual can gain access, while the probability that an authorized individual is refused access can be no more than one in 1,000. These requirements are significantly stricter than the biometric matching accuracy requirements contained in FIPS 201 or SP 800-76. A PIV card-based biometric component alone may not satisfy these requirements. To achieve these levels of performance with biometrics alone may dictate combining multiple biometrics, including “operational biometrics” selected specifically to achieve these aggressive levels of performance.

Additionally, these regulations require that the PACS control panel be located within the protected area. Communication lines that carry data such as personal identifiers must be either cryptographically protected or otherwise adequately shielded and supervised, to maintain system integrity and prevent surreptitious data manipulation when the data is transmitted from outside devices (readers) to the control panel.

The large numbers of facilities that must operate under these conditions have led PACS manufacturers to develop and deploy systems that comply with these requirements. By far, most SCIFs employ a Card + PIN-to-PACS authentication method. Since no card type is specified, the PIV card can be used in these facilities when deployed in conjunction with a PIN-to-PACS capability.

During the transitional period, when the PACS must support both legacy and PIV cards, access procedures to SCIFs (or SAPFs) are affected both technically and by policy. Technically, the same PIV migration considerations exist for SCIF PACS as for non-SCIF access control points; the policy impact is only now being recognized.

DCID 6/9 and current policy consider the traditional Card + PIN-to-PACS as a required two-factor authentication mechanism. SP 800-116 is silent on this type of authentication method. It is important to recognize that SP 800-116 is informative and does not prohibit implementation of these widely used authentication methods. It is also important to recognize the impact to these facilities if SP 800-116 becomes a normative document.

Harmonizing the access process at access control points minimizes the differences between the two approaches and eases both deployment and implementation of the PIV at such locations. One way to achieve this harmonization is to use a reader capable of reading both legacy cards and the free-read FASC-N from PIV cards. The reader sends the card data to the PACS, which then opens the specific user record that contains a “secret” PIN created during the PACS registration and provisioning process. The cardholder is prompted to enter the PIN, which is sent to the PACS for verification. Once the PIN is verified, the PACS begins the authorization process and either grants or denies access.

There may be, in addition, agency-specific policy impact if alarm sensors deployed within these restricted areas are affected when the PACS authorizes entry to a cardholder. It is possible to use either the PIV card or legacy cards to disarm and arm sensors in these areas.

Expanding PIV card usage to include this alternative authentication method satisfies DCID and enhances security at these locations.

4.2 Alternative Authentication Mechanisms

This section describes multiple authentication mechanisms that incorporate a mutual authentication protocol (MAP), mutual registration, and widely-deployed mechanisms such as combinations of cards, PINs, and biometric factors. Before any data such as biometric templates or PINs are transmitted, techniques can be used to authenticate the data, card and reader and to ensure the confidentiality of the exchange. (For details on these protocols, see Section 10.) The mechanisms discussed in this section are not currently described in the PIV specification.

4.2.1 Operational Biometrics with Enrollment on System and Match on System

FIPS 201 restricts access to the reference biometric fingerprint data stored on the PIV card. This restriction may prevent the efficient use of biometrics as an authentication mechanism in access control systems that require high throughput. In FIPS 201, biometric matching to the reference biometric fingerprint templates stored on the PIV card can only take place after the PIV card is inserted into a contact reader and a PIN entered.

An agency that wants to implement biometrics for physical access using the contactless interface without an additional requirement for PIN entry should consider using operational biometrics. Using operational biometrics, an agency will enroll biometric data separately and store data in an agency-specific data repository (e.g., PACS server, control panel, or reader). The FASC-N read from the contactless PIV card acts as a reference pointer to the specific biometric data to be matched for user authentication. Matching can take place at the PACS server, control panel, or reader. The biometric data can be stored in a different location than the location where the matching takes place.

In an operational biometric implementation, any biometric technology can be used, including fingerprint, iris, face, vein, or hand geometry. Interoperability among agencies is achieved during PACS registration when the reference fingerprint biometric can be matched after the PIV card is read and the PIN entered. Enrollment of the operational biometric can be as simple as copying the reference biometric fingerprint templates to the local PACS server or conducting a separate biometric enrollment immediately following PACS registration. The person is enrolled in the PACS database and the person’s biometric information is captured and stored, indexed by either an identifier that is assigned by the PACS itself or an external identifier that the person presents at the time of verification (e.g., FASC-N/GUID from the PIV card).

This method provides one-factor authentication when an index value on the PIV card (FASC-N or GUID) is used to find the reference biometric in the PACS database (since the card is not authenticated). The fact that the identifier comes from a card can sometimes be considered to be a second authentication factor (what you have). However, since the card is not authenticated, considering this a second factor opens the risk of successfully authenticating a counterfeit card.

When biometric verification is attended (i.e., the card is visually verified by an attendant), the second factor (what you have), while not electronically verified, exists—the features printed on the card are verified by the attendant. This method provides two authentication factors when used in conjunction with card authentication: what you have (the card) and match-on-system biometric verification that the cardholder is who the cardholder claims to be (who you are).

4.2.2 Reference Biometric with Match on System and Contactless Read of Encrypted Biometric Template on Card

Another alternative to the FIPS 201 requirement for PIN entry and contact read of the reference biometric is to define a separate, agency-specific application that is resident in the memory of the PIV card and co-located with the FIPS 201-compliant PIV application. To ensure agency interoperability, each of the two card applications can be independently accessed by a reader by selecting the appropriate application identifier. The agency-specific application can define a different protocol that permits contactless reading of the reference biometric fingerprint template without requiring PIN entry.

To protect personal privacy when transferring data from the card to the reader over the contactless interface, the fingerprint templates stored in the agency-specific application would be encrypted. Decryption of the fingerprint templates could be accomplished through the use of a symmetric key (privacy key), generated during card production and unique to each card. The privacy key may be stored in a separate, non-PIV applet so that it may only be accessed through the contact interface or by reading the magnetic stripe.

This approach to contactless biometric reading presents some unique challenges for the PACS. If the encrypted biometric templates are to be read from the card through the contactless interface, the reader must have some way of first obtaining the privacy key. This requirement can be met by configuring the reader to include a magnetic stripe reader and swiping the card before presenting the card to the contactless interface. As an alternative, the privacy key can be stored at the reader or PACS server following a one-time local PACS registration process. This approach is currently implemented by the Transportation Worker Identification Credential (TWIC) program described in Section 5.1.

4.2.3 Reference Biometric with Enrollment on Card and Match on Card

Agencies also have the option of implementing biometrics using on-card matching. Match-on-card (MOC) is designed to enable biometric authentication of the cardholder using either the contact or contactless interface, without a requirement for PIN entry. In MOC-enabled systems, the biometric matching algorithm resides on the card, and the live sample biometric data is sent from the reader to the card over a secure interface. The match result is sent back to the reader by the card over the same interface. When reference biometrics are used for MOC, the enrolled biometric fingerprint images used to generate the reference biometric templates stored on the PIV card are also used to generate the template for MOC. However, the MOC fingerprint template would be placed in an agency-specific container on the card that is not specified by FIPS 201. The MOC matching algorithm also resides in this container.

Contactless MOC operations provide a secure communication session between the card and the reader to ensure that the transaction data is encrypted and transmitted securely. MOC also eliminates the need for administering a separate off-card database of biometric templates (as previously described for operational biometrics).

Several smart card manufacturers have implemented MOC using fingerprints as a supported feature on their card products, and NIST has conducted feasibility studies and performance testing on this approach using fingerprint technology. NIST findings indicate that MOC can achieve adequate performance levels in both accuracy and throughput while providing a cryptographically secure contactless communication session between the card and the reader. The results are published in NIST Interagency Report (NISTIR) 7452 *Secure Biometric Match-on-Card Feasibility Report*,[7] and NISTIR 7477 *Performance of Fingerprint Match-on-Card Algorithms Phase I and II Report*.[8]

4.2.4 Operational Biometric with Enrollment on Card and Match on Card

The approach described as operational biometric with enrollment on card and match on card is identical to the MOC technique described above. However, with the use of operational biometrics, instead of the

[7] http://csrc.nist.gov/publications/nistir/ir7452/NISTIR-7452.pdf
[8] http://fingerprint.nist.gov/minexII/minex_report.pdf

reference fingerprint biometric, any biometric technology can be used, including a proprietary fingerprint or any iris, face, vein, or hand geometry technology.

This method would require the following:

- An available container on the card (possibly for each PACS) in which to store the operational biometric
- Secure communication between the card and the PACS (or at least between the card and the biometric reader), preventing the cardholder's biometric template from being exposed during contactless communication
- Mutual authentication between the card and the PACS biometric terminal, allowing the card to convey back to the PACS cryptographic proof of the biometric verification

In addition, this option may require one of more of the following:

- The use of authentication protocols such as PLAID, OPACITY, or SPAKE (discussed in Section 10) to allow a MOC with at least one operational biometric
- The use of mutual registration, which includes a mutual authentication protocol (which could be ISO/IEC 11770-2, PLAID, OPACITY, or SPAKE).
- It is important to note that as soon as a secure session is established between the card and the PACS, adding a third authentication factor (what you know) is quite easy. The third factor could be a PIN, verified by the card (sent ciphered to the card, with cryptographic proof sent back to the PACS), or as in PLAID, a hash value (sent ciphered by the card to the PACS, allowing the PACS to verify that the PIN presented is what the card expected). Mutual registration also allows a specific PACS PIN to be sent by the card to the PACS (as proof of cardholder knowledge) when the correct PIN is presented to the card (releasing secret information by the card, protected by a cryptographic channel).

4.2.5 PIN-to-PACS as Single Factor Knowledge

PACS have used (and in many instances continue to use) a PIN as the primary, single authentication factor as well as a second component in areas where physical access requires two-factor authentication. Several different types of PINS are used, each serving a distinct purpose, and each can be validated in different PACS components. The PIN is entered on a keypad and sent to the PACS for identification, validation, and authorization. In this deployment, the PIN-to-PACS is a unique secret identifier.

This method, which is used by many PACS, does not require a physical token and is not covered by the options in SP 800-116. The method assumes that the identifier (the PIN) assigned to a person is a unique identifier that identifies that person in the PACS authorization database. This unique identifier is also a secret the person has to protect.[9] The person should not use the number for any purpose other than PACS identification; other uses risk disclosing the secret to unrelated entities.

In large organizations, this method may require the person to memorize a large number. PIN length is determined based on the number of users at a site and should be selected to yield an acceptable user-to-permutation ratio.

For example, when the PIN is used as a single-factor identifier, a 1-to-10,000 ratio is achieved when there are four digits (0000–9999) in a fixed-length PIN and one user. If the same PIN length is used at a location with 100 users, the ratio is 100 to 10,000, or 1 in 100. The ratio can be improved by using PINs of different lengths. Varying the PIN length, so that some users have (for example) a three-digit PIN and others a four-digit PIN, increases the number of possible code permutations and improves the ratio. For example, if PIN length can be either three or four digits, the number of permutations increases from 10,000 to 11,000. In this example, the ratio is improved slightly, to 1 in 110. A six-digit PIN offers 1

[9] The Social Security Number (SSN) has been used in a similar fashion for many years (as a secret unique identifier), but with the multiplication of its use (shared by unrelated entities), the SSN became impossible to protect as a secret.

million permutations; using variable PIN lengths of three, four, five, or six digits creates 1,111,000 possibilities, and so on.

To further strengthen trust in this method, both the PIV credential and the PACS include a feature that limits the number of invalid PIN entries a system will accept. Should this limit be exceeded, the PIV credential locks. In a PIV credential, this limit is set to three incorrect entries. PACS often allow a user-defined number of attempts before a PIN tamper alarm is generated.

4.2.6 PIN-to-Card

With the PIN-to-card authentication mechanism, a card is presented to the reader and the user provides a PIN for the card to validate. This then unlocks the card and the card releases a unique identifier. The PACS uses this identifier to find an entry in its database for access authorization.

This method requires a trusted method to transfer the identifier from the card to the PACS. Unless the card is a trusted entity, the PIN presented to the card has no assurance value for the PACS. The PACS trust in a PIV card is obtained after a successful card cryptographic authentication is executed (using the CAK or PIV Auth Key). Because a CAK can be executed without a PIN being presented to the card, only use of the PIV Auth Key transfers back to the PACS the required trust in the PIN presented to the card.

Systems that rely on a single operational biometric often use a PIN as a back-up mechanism when certain individuals are unable to enroll that biometric factor. The system recognizes that the person has been issued a BIO PIN and uses the successful entry of a matching BIO PIN to authorize access.

When mutual authentication (trust) is established between a card and the PACS (as with the PLAID, SPAKE, OPACITY protocols, or mutual registration), it is possible both to present a ciphered PIN over the interface to the card and to receive from the card a cryptographic validation of the PIN. Without receiving trusted proof from the card, PIN presentation to the card has no assurance value for a PACS.

4.2.7 Card with PIN-to-PACS

Systems that require secret information (a PIN) in addition to a unique identifier for the user achieve two-factor authentication (what you have and what you know) when the unique identifier is released from a hard-to-clone physical device.

Although details vary from PACS to PACS, the fundamental concept remains the same. The authentication method includes matching both a unique identifier (such as a card number or FASC-N) and a PIN. During the process of assigning access privileges to the cardholder, a private PIN is created and included with the unique card number (FASC-N) and indicates access authorization in the individual's user record. Most PACS store and maintain user records in the PACS control panel. The user access request and PACS process is as follows:

1. A user presents a PIV card to a PACS reader.
2. The reader processes the card data (signed or unsigned CHUID or CAK, depending on the level of assurance required for the "what you have" factor), and the FASC-N is released and sent to the PACS control panel.
3. The controller uses the FASC-N to locate and open the user record in the database. The user record includes a private PIN. The system then prompts the user to enter the private PIN.
4. The PIN is sent from the keypad to the PACS control panel for comparison (validation) against the private PIN in the user record.
5. When the PIN entered matches the private PIN, the system initiates the authorization process and makes the access decision.

To further strengthen trust in this method, both the PIV credential and the PACS include a feature that limits the number of invalid PIN entries a system will accept. Should this limit be exceeded, the PIV credential locks. In a PIV credential, this limit is set to three incorrect entries. PACSs often allow a user-defined number of attempts before a PIN tamper alarm is generated.

Depending on how the card is verified (see the previous section) and the length of the PIN, various levels of assurance can be obtained using this two-factor authentication method.

It is worth noting that the PIN is compared only to the single private PIN contained in one individual user record. All other user records remain closed and are untouched by the validation process. The risk of a card being successfully matched with the PIN belonging to a different user is therefore eliminated. To minimize the risk of cardholders forgetting their PINs, some agencies allow people to select their own private PINs.

Like other data, the PIN must be properly protected to avoid inadvertent or unintended exposure. Countermeasures include securing the PIN entry process, supervising both the communication line and the data packet sent from the keypad to controller, and securing the data repositories where user records are stored and maintained.

When a PIN is used in conjunction with a token (as described above), the risk of an exposed PIN is reduced. The PACS will not grant access to a user who enters a PIN without a card or to someone who presents a card without a valid PIN. Both must be entered before the PACS authorization process begins. The process is very similar to that used at an ATM.

5 Example Implementations Using Alternative Authentication Mechanisms

5.1 Transportation Worker Identification Credential

The Transportation Worker Identification Credential (TWIC) program is a joint program of the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) within the Department of Homeland Security (DHS). The objective of TWIC is to strengthen the security of the U. S. maritime infrastructure through background vetting of civilian maritime workers and issuance of tamper-proof biometrically-enabled identification credentials to eligible workers. TWIC was developed in response to the legislative requirements contained in the Maritime Transportation Security Act (MTSA) of 2002 (Public Law 107-295) and the Security and Accountability for Every Port (SAFE Port) Act of 2006 (PL 109-347). Currently, over 1.3 million maritime workers have enrolled in the TWIC program and have received a TWIC card. Possession of a TWIC card is now required for unescorted access at 3,200 land-based and outer continental shelf (OCS) facilities and on over 10,000 vessels that are subject to MTSA regulations.

In the early stages of defining the technical requirements for the TWIC card, the maritime industry expressed concerns about the proposed approach, which called for the TWIC card to be fully compliant with the FIPS 201 standard. The maritime community felt that FIPS 201 was not an appropriate standard for high volume physical access control situations in which rapid access is an operational requirement. Their concerns were based on the fact that FIPS 201 allows access to the biometric data on the smart card only through a contact interface, thereby requiring insertion of the card into a contact interface slot on a reader. Given that many of the reader devices would be exposed to the extremes of weather at seaports, there was concern that contact readers would allow airborne contaminants to infiltrate the reader electronics, resulting in maintenance problems. The maritime industry also objected to the FIPS 201 requirement for entry of a PIN to access the biometric data on the smart card after insertion of the card into the reader.

The resulting TWIC Reader Hardware and Card Application Specification, published by TSA, implements an alternative authentication mechanism that allows contactless reading of the reference fingerprint template from the TWIC card without requiring PIN entry. To protect personal privacy, the fingerprint templates stored on the card are encrypted. Decryption of the fingerprint templates is accomplished through the use of a diversified symmetric key called the TWIC Privacy Key (TPK), which is generated during card personalization by TSA and is unique to each TWIC card. The TPK can only be accessed through the contact interface or through a swipe read of the magnetic stripe.

However, this approach to contactless biometric reading presents some unique challenges for the implementer. If the encrypted biometric templates are to be read from the TWIC card through the contactless interface, the reader must have some way of first obtaining the TPK in order to decrypt the templates prior to performing the biometric match. This can be achieved by storing the TPK in the local PACS server after a one-time local PACS registration process. Another alternative is to use a reader that has both magnetic stripe and contactless smart card capability. In this scenario, the cardholder would swipe the TWIC card before presenting the card to the contactless interface.

It should also be noted that in addition to the application described above, the TWIC card includes a separate FIPS 201-compliant PIV application, which is co-located in the memory of each TWIC card. Each application can be accessed independently by a reader by selecting the appropriate application identifier (AID).

5.2 Aviation Credential Interoperability Solution

The Aviation Credential Interoperability Solution (ACIS) program is designed to strengthen aviation security through the strategic application of proven, secure identity authentication and related access management concepts and technologies. The goal of ACIS is to establish standard, consistent processes across the aviation industry for enrollment, card issuance, vetting, and credential management. ACIS will enable the necessary components for identity interoperability between airports and between other FIPS 201 interoperable solutions (e.g., TWIC, First Responder Authentication Credential (FRAC)). In addition, ACIS will support real-time secure identity verification and allow for credential integration with airport biometric access controls and security technology, while reducing the need for multiple IDs for transient aviation workers.

The ACIS concept represents a distinctive operational approach, as it includes both centralized and decentralized components. The initial focus of ACIS is on local and transient personnel working at commercial airports—airport operators and aircraft operators. Although ACIS is technically compatible with PIV and includes interoperable certificates complying with PIV-I for non-Federal issuers, it includes considerations that address the performance requirements not addressed by PIV and an approach that allows for local control of the PACS. The ACIS identity credential scheme is a relatively simple concept, compared to the operational use of the ACIS credential in a local access control environment. The ACIS concept separates the ideas of identity and access control, enabling PACS security by using locally managed cryptographic keys supported by mutual registration.

ACIS distinguishes between identity-based access control and privilege-based access control. ACIS identity-based access control is compatible with PIV identity verification methods for access control and would typically be used in situations where a cardholder requires infrequent or one-time access through an attended access control point (e.g., a pilot going through a passenger security checkpoint). Privilege-based access control verifies the claimed identity of the cardholder and the reason for access when the person enrolls for access. At this time, the PACS authority grants the access privilege and either uses the person's identity credential or issues (electronically) a privilege credential that can be loaded on the person's ACIS credential. This gives the PACS much faster access to the privilege credential it controls and manages (including its own set of keys), without having to execute identity-based verification for each access.

The ACIS credential allows identity-based verification using the PIV interoperable credential whenever such verification is required, but also allows the PACS to issue and manage local access control credentials without having to share any numbers or secrets with other access control authorities. This architecture allows airports and air carriers to issue identity credentials to their employees and contractors (acting as identity authorities) in a common manner, allowing these credentials to be trusted as identity documents. It also allows access control decisions to be made as they are today, using privilege-based credentials issued and managed by the access control authorities of each airport.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council to describe PIV card authentication mechanisms defined in NIST SP 800-116 and to describe additional authentication mechanisms that were not covered in SP 800-116, but that are important for organizations implementing PACS to increase security. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Physical Access Council members for their contributions. Participants involved in the development of this report included: AMAG Technology, CSC, Diebold, Gemalto, Hirsch Electronics, HP Enterprise Services, Identification Technology Partners, IDmachines, JMF Solutions, LLC, Roehr Consulting, XTec, Inc.

Special thanks go to **Lars Suneborn**, Hirsch Electronics, who led the white paper project, and to the following Physical Access Council members who contributed to the development of this white paper:

- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Diebold
- **Marty Frary**, JMF Solutions, LLC
- **Walter Hamilton**, Identification Technology Partners
- **Andy Jones**, XTec, Inc.
- **Lolie Kull**, HP Enterprise Services
- **Richard Lazarick**, CSC
- **Gilles Lisimaque**, Identification Technology Partners
- **Cathy Medich**, Smart Card Alliance
- **Neville Pattinson**, Gemalto
- **Roger Roehr**, Roehr Consulting
- **Adam Shane**, AMAG Technology
- **Lars Suneborn**, Hirsch Electronics

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.

Trademark Notice

7 Glossary

The following terms are used in this document as defined below. References for the definition of each term are shown in brackets after the definition.

Access control panel (ACP)
An intermediate component of a PACS that interfaces readers or sensors to the PACS server. The ACP may be designed to be independent of the host when offline, storing transactions and making access decisions, and then reporting the transactions processed to the host on reconnection. Functionality varies by design and configuration.

Applet
A small application that performs one specific task, sometimes running within the context a larger program perhaps as a plug-in. The term typically also refers to programs written in the Java programming language which are included in an HTML page.[10] A PIV card contains a PIV applet.

Assurance
How surely an authentication process can conclude that an identity object or identifier is in fact what it claims to be. Assurance is measured in accordance with the *level of confidence* offered for the claim. SP 800-116, Section 3, refers to four levels of assurance (defined in OMB Memorandum M04-04 and NIST SP 800-63, *Electronic Authentication Guideline*[11]): Level 1 - Little or NO Confidence; Level 2 - Some Confidence; Level 3 - HIGH Confidence; Level 4 - VERY HIGH Confidence. [SP 800-116]

Authentication
A process that establishes the origin of information, or determines an entity's identity. In the SP 800-116 publication, authentication often means the performance of a PIV authentication mechanism. [SP 800-116] For a PACS, authentication takes place "in context," where benefit is derived from previous authentication decisions when making a new access control decision. That is, when the presented identifier (biographical, biometric, or digital identity object) is authenticated in context (accepted by the application based on a previous authentication decision), the transaction or access attempt can continue to the next step or level. Authentication is the process of establishing confidence in user identities (identifiers or identity objects). The authentication process asks the questions "Are you in fact who you claim to be? Is the identity object proven or assured (see *Assurance*) to be what it claims?"

Authentication methods
Mechanisms that are used to execute authentication actions.

Authorization
A process that associates permission to access a resource or asset with a person and the person's identifier(s). [SP 800-116] In a typical PACS application, the permission is permission to enter or pass through a controlled portal or access point – that is, granting access.

Biometric
A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. [FIPS 201]

Card reader (CR)
A device that interfaces with a PIV card, credential or token and an access control panel .

Certificate revocation list (CRL)
A list of revoked public key certificates created and digitally signed by a certification authority. [FIPS 201]

Certification authority (CA)
A trusted entity that issues and revokes public key certificates. [FIPS 201]

Cognizant security authority (CSA)
An individual or agency having jurisdiction over security-related policies. [DCID 6-9]

[10] http://en.wikipedia.org/wiki/Applet
[11] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63-Rev.%201

Credential
Evidence attesting to one's right to credit or authority. In this standard, it is the PIV card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. [FIPS 201]

Credential validation
The process of determining if a credential is *valid* – i.e., it was legitimately issued, its activation date has been reached, it has not expired, it has not been tampered with, and it has not been terminated, suspended, or revoked by the issuing authority. [SP 800-116]

Cryptographic key (key)
A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. [FIPS 201]

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, specified in the document "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" [TIG SCEPACS], and included in several data objects on a PIV card. [FIPS 201]

Identifier
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. [FIPS 201]

Identity verification
The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV card or system and associated with the identity being claimed. [SP 800-116]

On-card
Data that is stored within the PIV card or a computation that is performed by the integrated circuit chip (ICC) of the PIV card. [FIPS 201]

Online certificate status protocol (OCSP)
An online protocol used to determine the status of a public key certificate. [FIPS 201]

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 administrator
A special operator of the PACS who has the highest level of access to the physical access control software application, application configuration tools, and all database information. The PACS administrator can also assign administrative rights to other individuals (e.g., operators) based on their roles and the PACS functions they must perform. The administrative rights assigned can be equivalent to the highest administrator privileges or a subset.

PACS operator
An operator of the PACS software application who uses assigned privileges to perform any function allowed within the PACS application by that operator level. Certain operators may be assigned to enroll credentials or manage PACS access provisioning from credentials.

PACS user
An authorized cardholder who uses the credential and PACS to request access to facilities at access control points.

Personal identification number (PIN)
A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. [FIPS 201]

Validation

The process of determining that an identity credential was legitimately issued and is still valid – i.e., has not expired or been terminated. [SP 800-116]

Verification
The process of determining if an assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer. [SP 800-116] For a PACS, verification occurs when unique biographical, biometric, or digital identifiers (i.e., data objects linked to a person's identity) are asserted by presenting a credential and, when the data objects are compared with previously recorded or stored identifiers, a match is found.

8 Appendix A: Standards Efforts

This appendix describes several standards efforts that relate to physical access control systems.

8.1 oBIX/OASIS

oBIX /OASIS, the Open Building Information Exchange technical committee, is an industry-wide initiative to define XML- and web services-based mechanisms for building oBIX I instrument enterprise control systems. The mission of the oBIX technical committee is to develop a publicly available web-service interface specification that can be used to obtain data in a simple and secure manner from HVAC, access control, utilities, and other building automation systems, and to provide data exchange between facility systems and enterprise applications. In addition, the committee will develop implementation guidelines, as needed, to facilitate the development of products that use the web service interface.

Web site: http://www.obix.org/

8.2 BACnet

Developed under the auspices of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), BACnet, a data communication protocol for building automation and control networks, is an American national standard, a European standard, a national standard in more than 30 countries, and an ISO global standard. The protocol is supported and maintained by ASHRAE Standing Standard Project Committee 135.

Web site: http://www.bacnet.org/

8.3 SIA OSIPS

The Security Industry Association Open, System Integration and Performance Standards (SIA OSIPS) was adopted by a consensus of industry volunteers in accordance with SIA's standards development policies and procedures. It is intended to facilitate product compatibility and interchangeability among different security system manufacturers' products, simplifying the task of combining disparate products.

The OSIPS is a set of eight specific component interface standards, including standards for access point controllers, digital video, and back-end data exchange. ANSI adopted the SIA OSIPS Digital Video standard in 2008.

Web site: http://www.siaonline.org/

8.4 PSIA

The Physical Security Interoperability Alliance (PSIA) was founded with the objective of defining, recommending, and promoting standards for the interoperability of IP-enabled security devices. Participating companies include leaders in the security camera, video management software, access control, and system integrator segments of the market. The PSIA is a not-for-profit open industry group that will identify existing and emerging standards relevant to the physical security industry, work to enhance them to support industry requirements, and encourage their adoption by member companies and the industry. In addition, the group reviews and vets specifications that are submitted as open standards.

Web site: http://www.psialliance.org/

8.5 INCITS M1-Biometrics

The International Committee for Information Technology Standards (INCITS) is the primary focus for standardization in the United States in the field of information and communications technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1 (JTC1). JTC1 is responsible for international standardization in the field of information technology. The Executive Board of INCITS established Technical Committee M1, Biometrics, in November 2001, to ensure a high priority, focused, and comprehensive approach in the United States to the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting.

The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes such as homeland defense and the prevention of identity theft, as well as other government and commercial applications based on biometric personal authentication. Specific standards applicable to authentication mechanisms include the fingerprint minutiae data interchange standard, associated conformance testing and fingerprint quality standards, and performance testing for access control biometrics standards. Note that INCITS includes the following additional technical committees within the security/ID technology area:

- Identification Cards and Related Devices (B10)
- Cyber Security (CS1)
- Biometrics (M1)
- Radio Frequency Identification (RFID) Technology (T6)

Web site: http://www.incits.org/

8.6 ISO–JTC1

International Organization for Standardization (ISO) Joint Technical Committee 1 (JTC1) is composed of 18 subcommittees grouped within 11 technical directions. The focus for JTC1 is standardization in the field of information technology, including the specification, design, and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of information. The mission is to develop, maintain, promote, and facilitate the IT standards required by global markets that meet business and user requirements concerning the following:

- Design and development of IT systems and tools
- Performance and quality of IT products and systems
- Security of IT systems and information
- Portability of application programs
- Interoperability of IT products and systems
- Unified tools and environments
- Harmonized IT vocabulary
- User-friendly and ergonomically designed user interfaces

Three of the subcommittees within JTC1 of greatest interest to this topic are the following:

- SC 17—Cards and Personal Identification
- SC 27—IT Security Techniques
- SC 37—Biometrics

ISO web sites: http://www.iso.org/
http://www.iso.org/iso/iso_catalogue/catalogue_tc

JTC1 web site:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45144

9 Appendix B: Case Studies

When HSPD-12 was issued five years ago, the memo stated that PIV cards would have to be electronically authenticated rapidly to meet compliance. The directive states that the cards would be used for physical and logical access control. However, currently many Federal agencies are still using the PIV card as an expensive “flash pass” and not implementing the full capabilities of the card.

Currently, most Federal facilities have not implemented a solution for physical access control that meets today’s standards and requirements. Many systems are out of date; this may be due to the archaic technology of the PACS or incompatibility with the increasing use of smart card technology. However, the Department of State has implemented a physical access control solution capable of high assurance level challenge-response authentication that showcases authentication for access control for an agency nationwide. The solution implemented meets all Federal standards as well as the criteria for suggested standards (namely, SP 800-116).

The Department of State (DOS) HSPD-12 Implementation Program provides for credential management and enrollment and issuance of smart card credentials to new employees and contractors at DOS facilities. The issued PIV credentials are used not only for identification purposes but also for physical access control nationwide. Domestically, DOS has over 4,000 access control points, with readers accepting the FIPS 201 PIV cards in addition to GSC-IS smart cards. Additionally, the DOS solution is a service shared with six other agencies, including USAID and the Peace Corps.

The system issues approximately 500 credentials per week. There is full challenge-response authentication of more than 100,000 credential transactions per day for card usage. The system represents successful integration of a FIPS 201 access control solution, with CHUID readers integrated into the legacy readers. As part of the solution, FIPS 201 access control readers were delivered to over 4,000 entry points.

The system architecture is designed to accommodate changing requirements and technology improvements. The readers incorporate the HSPD-12 PIV II interoperability standard and have the ability to support all SP 800-116 defined levels of security. The PIV card, PIN, and biometrics are used for authentication, based on various levels of threat assessment.

The implemented solution is at the core of access control, which allows for an effective workflow. The individual access control devices can be grouped to efficiently allow individuals the access they need to the facility.

10 Appendix C: Mutual Authentication and Mutual Registration Protocols

10.1 Mutual Authentication

A smart card and a terminal can communicate as follows:

- Using plain text (no confidentiality protection for the communication interface)
- Using static ciphering protection, where data stored in the card is ciphered by a key known by the client using the terminal
- Using a session key for encryption (confidentiality between parties)

When a card is presented to a terminal, it is important to authenticate the card and its holder, but sometimes it may be just as important to protect the card from revealing information to a non-trusted terminal. This requires the card to authenticate the terminal as well.

Various solutions are available to provide confidentiality or terminal authentication or both, all with their own advantages and disadvantages. These solutions are called mutual authentication protocols (MAP) with session key establishment. Some are ISO standards and can be found in the ISO/IEC 1170 series of standards; others are being developed specifically for smart cards by various organizations. These protocols include PLAID (developed by the Australian government), OPACITY (developed by ActivIdentity), and SPAKE (developed by Gemalto). PLAID and OPACITY have been announced by their owners as royalty-free and are both being proposed for inclusion in the ISO authentication protocols listed in ISO/IEC 24727-6.

10.2 Mutual Registration

The concept of mutual registration is similar to the concept of a visa in a passport. A credential (such as a passport) is issued by an identity authority (such as a country, a Federal agency, or a motor vehicle authority) and a different authority (such as the government of a different country) uses the credential to grant access to the legitimate bearer of the credential.

Just as one must register for a visa when planning to enter a country other than the country that issued one’s passport, the identity document holder must ask for permission to access places that are not controlled by the issuer of the document. As is the case for passports, the idea of mutual registration is that access authorization is noted not only in the PACS, but also in the identity credential itself, allowing the PACS and the credential to share trusted data without having to repeat a complete identity verification cycle each time.

The concept allows each PACS to create a virtual access control card – i.e., a "visa for access" – which contains information specific to the particular PACS. This virtual card works for access control just as if the PACS had issued a separate card, with its own number, its own biometric data, and its own PACS PIN (if the PACS decides to impose these requirements).

The process consists of writing information related to each PACS onto the credential. This information is used later by each PACS. Each PACS registered in the credential is identified by a unique number (UUID generated by the PACS). The PACS then loads the associated entry securely onto the credential once. This is done at the time of mutual registration. The credential now has the information it needs later to use that credential efficiently for access control.

The information consists of the algorithm and the key that will be used by the PACS and the credential to perform mutual authentication and generate a session key, such as ISO/IEC 12770-2-AES, OPACITY, PLAID, or another available standard protocol. It may also add a local identifier allocated by the PACS to the credential (instead of using a long, complex identifier generated by the identity authority), an operational biometric, a local PACS PIN which will be presented by the credential to the PACS, or any other information the PACS wants to receive from the credential after the credential has been authenticated.

Once this process is complete, the PACS and the credential have shared information. Because there is no need to use public key mechanisms, the mutual authentication process is much faster than processes that use asymmetric algorithms. The mutual authentication process does not require path validation, and it also allows for the creation of a session key, permitting the secure exchange of information such as a PIN or biometric data over any interface, contact or contactless.

Since there is a very clear separation between the identity authority and the access control authority, the mutual registration process allows each PACS authority to continue to be autonomous, allocating and managing access control identifier numbers and authenticators according to need, without having to share secret information such as a key, PIN, or biometric with any other authority.

10.3 PLAID

The Protocol for Lightweight Authentication of IDentity (PLAID) is an authentication protocol that uses standards-based symmetric and asymmetric cryptography in a unique way to protect the communications between smart cards and terminal devices. Extremely fast and highly secure strong authentication of the smart card and data objects is possible without exposing card or cardholder identifying information or any other repeating information useful to an attacker. PLAID is being developed by the Australian government for use in all of their identity credentials and is proposed to ISO for open reference.

The objective of PLAID is to provide a fast method for a credential and a terminal to establish mutual trust (authentication) and a session key that can then be used to secure further exchanges. The protocol also has a very important feature for identity credentials, which is that it protects all types of personal information exchanged over the interface (contact or contactless) and never exposes any permanent identifier in clear text (i.e., there is no way to track a particular credential).

PLAID uses asymmetric and symmetric cryptography (currently RSA and AES) and is optimized to minimize execution time. For example, the key recommended for RSA authentication is 1984 bits, which limits the number of physical blocks exchanged during the mutual authentication process. On existing FIPS 140 cards, the complete process (mutual authentication plus establishment of a session key) takes about 650 ms the first time it is invoked and 400 ms the second time.

Another interesting feature of the proposed protocol is that it will provide a way for the terminal to verify the credential's PIN without exposing the PIN in clear text during the exchanges and without forcing the user to present a PIN (for a second-factor authentication) while holding a contactless credential in front of the terminal.