THE ROLES OF AUTHENTICATION, AUTHORIZATION & CRYPTOGRAPHY IN EXPANDING SECURITY INDUSTRY TECHNOLOGY

[Please note: This Quarterly Technical Update (QTU) presents information about a number of industry-impacting developments (such as the FIPS 201 standard) and their related technical issues. Its purpose is to introduce technology elements that are new to the security industry, to facilitate the evaluation of these technologies in support of SIA member business and product planning. Due to the scope and purpose of this report, this QTU is a longer document than usual and contains very detailed technical material.]

I. INTRODUCTION

For many years, physical access control systems have been the center of integrated electronic security systems that include access control, ID badge printing, alarm monitoring and CCTV functions. Authentication (verifying identity) and authorization (verifying that the identified person is permitted the requested access at that moment) have typically been performed by physical access control systems more or less as a single step. Present a valid access card, and authentication and authorization are instantly performed.

Depending upon the level of security required, access control systems have been configured for 1-factor authentication (such as card or PIN or biometric), 2-factor authentication (such as card-plus-PIN or card-plus-biomet-

TABLE OF CONTENTS:

ric), or 3-factor authentication (such as card-plus-PIN and biometric).

Cryptography (the science of providing security for information through the transformation of data) initially entered the picture with the use of encryption as a way to protect passwords and other sensitive information in an access control system's computer database. Recently the protection of security system communications became important when Ethernet networks replaced proprietary equipment connections, and as security systems began using Internet Protocol (IP) messages and began to share networks with other business systems. Thus, a number of manufacturers have begun to use encryption in system and network communications. But information security requirements for enterprise-scale integrated security systems go beyond encryption, because additional cryptographic techniques are needed to establish trusted system connections, and to ensure that transmitted data is authentic and unaltered. Therefore, today, authentication, authorization and cryptography are all important elements of sound integrated security systems.

Drivers for Change

Originally, no security industry standards existed for these system elements, each manufacturer could use its own approach with only slight regard for what other manufacturers were doing technically. Now a number of major factors have changed this landscape:

- Interoperability requirements. Large customers (especially the Federal government) require systems in multiple facilities to be interoperable, so that systems from multiple manufacturers can communicate and interoperate. Interoperability involves creating standards-based solutions.
- Convergence of physical and information systems security. Large customers (and again, especially the Federal government) want to integrate the management of physical and information access control, including the use of a single smart card for both physical and information security.
- Common user provisioning. The use of common user provisioning (also called one-step provisioning) is increasing, which means having a single point of employee registration and dismissal (usually in a Human Resources system) with automatic assignment and revocation of both physical and information security privileges.
- Enterprise-Wide Access Control. To implement enterprise-wide access control organizations have to do more than purchase sound security technology, they must also define business processes and procedures for identity verification, card issuance and access management. These processes and procedures must be thorough, accurate and secure enough to justify reliance upon cards dispensed by any authorized issuer within the enterprise. The Federal government's Personal Identity Verification program (as described in Federal Information Processing Standard (FIPS) 201, which defines the PIV standard) is the most significant such program. A key concept is cross-credentialing, where a single credential is used across organizational boundaries.
- Physical security systems are IT systems. Today's electronic security systems are based upon computers and intelligent devices connected over a TCP/IP network. (For example, most digital video recorders are computers running Windows or Linux operating systems.) Thus, more and more customer organizations are classifying se-

curity systems as IT systems and subjecting them to industry and organizational IT standards, from purchase through installation and commissioning, and into ongoing operations and maintenance. (See the June 2005 SIA Quarterly Technical Update for details on the U.S. government's official classification of security systems as IT systems.)

- Adoption of digital certificates. Photo ID cards and handwritten signatures are used for visually establishing identity and for certifying documents and transactions. For example, retail establishments can use photo IDs that include signatures (such as a driver license) to visually verify customer identity and to check the signature on a credit card slip. Digital certificates are the electronic counterparts to driver licenses, passports and membership cards. The keys associated with digital certificates (explained later in this report) can be used to sign electronic information. Digital certificate systems are used to protect information that is sent over public or shared networks, such as email messages. Systems using digital certificates have been proven to have very strong security. Digital certificates—as the enabler of secure e-commerce on the Web—have revolutionized the way many companies do business. The strength of such systems has lead to the widespread adoption of digital certificate technology. The incorporation of digital certificate technology in physical access control systems will be a requirement for integration with IT Systems. For example, the second stage of FIPS 201 requires that access control system biometric and cardholder unique identifiers are signed and authenticated using digital signatures. The government has scheduled such implementations to begin at the end of October 2006.

Authentication, authorization and cryptography were initially built into single systems made to protect physical and information assets by restricting individual access to them. These technologies have now become the enablers and protectors of critical business processes and commercial transactions. Due to the extremely large scale of enterprise-wide identity and access management (millions of users, thousands of assets) and the complexity of the integration requirements, entire systems have been developed just to provide one of these functions (authentication, authorization or cryptography) as a service to other systems.

Will these developments have any impact on the security industry? The unequivocal answer is "Yes". This document in particular will examine the roles of authentication, authorization and cryptography within FIPS 201 compliant customer systems. FIPS 201 divides the compliance processes into two parts: policy goals (PIV I whose deadline—October 27, 2005) and technical goals (PIV II—whose deadline is October 2006).

Both system and device manufacturers are impacted.

Whereas system manufacturers have formerly been able to design their systems as independent system offerings, they now must consider that their products will have to function as a part of a larger overall security systems framework, and that their products may even be dependent upon other systems for one aspect or another of the overall security decision process. Just as device manufacturers have had to support digital communications and stor-

age technology (such as Ethernet networking, TCP/IP protocol, smart cards, and embedded hard drives), so must they now support digital security technology and emerging interoperability standards.

System integrators are also impacted.

Formerly, system integrators were able to sell and install their offerings as all-encompassing stand-alone systems. Now, they must be able to collaborate with two categories of customer stakeholder: business and technical. That generally means collaborating with the customer's IT department to find out what role their system offerings and services can play in the customer's overall system plans, including what IT standards and IT systems integration requirements must be met.

Physical access control system (PACS) system integrators must understand how the various pieces of the overall security systems framework will fit together, including the specific roles that authentication, authorization and cryptography will play in the customer's business systems, since these will impact what they as system integrators can and should propose to provide to the customer. Furthermore, system integrators will often have to partner with IT integrators who are providing credentialing, authentication and authorization solutions as part of an enterprise-wide security initiative launched and managed by the customer's IT department.

Thus manufacturers and integrators will have to invest in IT knowledge, including staff certified in information technology, such as Microsoft Certified Systems Engineer (MCSE), as well as personnel trained and certified in information systems security.

Security Industry Expansion

Companies providing physical security system product and service offerings will have to incorporate the required new information technologies and adjust their sales and service approaches, in order to continue to capture desirable levels of market share. It is important to remember that while these developments do impose some new requirements on SIA member companies, the requirements stem from a significantly expanded role for security technology. Customers (especially the Federal government) are envisioning and planning security deployments on a scale never before attempted. That means significant market opportunities for security industry companies that provide the kind of solutions being envisioned. Industry analysts concur and continue to predict significant growth for the security market based upon the incorporation of these technologies, because they support and enable large-scale system deployments and the improvement of security related customer business processes.

II. TECHNOLOGY

To understand the technology impacts of these developments requires taking a very close look at certain aspects of security access control, and examining them in much more detail than has been needed in the past. It also requires taking a look at the business systems context in which physical security systems will be operating. Furthermore, it involves considering how physical and IT security convergence will affect physical security systems.

As enterprises automate their critical business processes they use information security technology and practices to secure the operations of their business systems. Several aspects of these business trends are worth considering

because they are affecting the new requirements being placed upon security systems:

- Business systems have become very large in scale in terms of both the number of users and the number of system transactions.
- Consequently, the function of information security technology has evolved from its initial role as a protector of personal information access to its current role as an enabler of large-scale business system transactions.
- Thus the concepts of identity and trust now include system identity and transaction trust as well as human identity and trust.
- New information security technology and new standards have been developed to address the new requirements of these systems.
- To function as a part of the overall business systems security framework, traditional security systems and components must now incorporate the new technology and conform to the new standards.
- This has the beneficial side effect of improving the network and system security of traditional security systems, which customers such as the Federal government are requiring (for details see the Quarterly Technical Updates for March and June of 2005).

These trends are occurring in a continually changing business technology landscape, which is evolving as businesses grow. This is resulting in an expanding market for security industry products and services that evolve to conform to or contribute to these trends.

As technology evolves terminology also evolves. Thus it is critical to pay close attention to the meanings of terms when reading or writing about the subjects being discussed in this update. Terms like identity, authentication, authorization and credential have been used to mean a variety of things and have more than one valid meaning. To avoid getting or giving the wrong idea, clarification of terms—including what they mean in the context of a particular system or business process—is vital.

Thus this update pays close attention to terminology in discussing the key technology concepts presented below. Not only is it important for SIA members to have a thorough understanding of these concepts—SIA members must also communicate clearly about them in written and verbal presentations to their current and potential customers. Purchasing decisions and contract awards can be won or lost based upon the clarity, accuracy and effectiveness of communication to the customer.

Identity

In a philosophical sense we think of identity generally as "who or what we are". A more specific definition states that identity refers to the individual characteristics by which a person or thing is recognized or known. That definition relates to identification. "Identity theft" is not actually the stealing of our identity, but the theft of identity information used for purposes of impersonation. Another aspect of identity relates to role. "Bill, Joe's dad" or "Ms.. Smith, Joe's teacher" are examples. How we interact with someone may have more to do with their role in a particular organization or group, than with their individual personal characteristics. For example, Joe could have a substitute teacher, who temporarily assumes the rights and responsibilities of Joe's usual teacher. Mrs.

Smith could cease being Joe's teacher, but she would not cease being herself.

Within the context of a business system or security system, identity generally has one of two meanings. First, it refers to identity information (such as an identifying name or number) that is unique within the system. For security to be manageable, it is important that a person has a single identity within a single domain; for example, a university employee enrolled in a course is one person with the attributes of "employee" and "student," not two people. Additionally, identity information usually includes one or more of the following, depending upon the purpose and function of the system:

- identifying characteristics, which individuals and systems will use to perform an identification.
- system or organizational role, used to determine the specific rights and authority granted.
- the period of time for which the identify information may be relied upon.

Identifying characteristics include personal physical descriptive characteristics such as eye color, hair color, height as well as a photograph used for human visual identification, and information used by systems for automated verification (such as PIN and biometric data).

FIPS 201 spells out a common data model for cardholder identification information, which specifies a minimum set of data elements to be maintained in a Federal agency PACS database.

Second, identity in the context of verification can refer to anything being identified as authentic, including a:

- person
- physical object (such as a security smart card)
- data object (such as a biometric signature on a card)
- computer system

In a security framework involving multiple systems, all of the above elements can have identities that are subject to verification. Systems that interact must be able to identify each other, just as systems and components must be able to verify the authenticity of a card. For example, FIPS 201 includes requirements for high security levels to verify the authenticity of both the card and the encoded data stored on the card. This is different and separate from verifying the identity of the person holding the card.

Identity Management System

An identity management system identifies individuals in a system and controls their access to resources within that system by associating user rights and restrictions with each identified individual. U.S. driver's licensing systems are a simple example of identity management: Drivers are identified by their driver's license numbers and photo ID, and specific user privileges (such as a motorcycle endorsement) or restrictions (such as "corrective lenses required") are linked to the identifying number. A typical PACS is also an identity management system. However, in recent years the term Identity Management has specifically come to mean the management of digital identities, which are the electronic records that represent the people and systems being granted access rights and privileges, and being assigned roles with related authority and responsibility elements in business workflow systems. Thus The Burton Group

defines Identity Management as "the set of business processes, together with a supporting infrastructure, for the creation, maintenance and use of digital identities within a legal and policy framework."

The components of an Identity Management infrastructure include directory services (the management of information used to identify users and resources on a network), authentication, access management and user management facilities such as provisioning, delegated administration and self-service administration (like password resets and smart card issuance kiosks).

Identity Management Systems provide a way to separate identity verification (authentication) from the granting of access. This provides a point of convergence for physical and IT security systems, which can both integrate to the same Identity Management System. FIPS 201 incorporates the concept of having an Identity Management System (IDMS[1]) separate from a PACS. An IDMS is often managed by the Human Resources or Personnel department, as opposed to being managed by security personnel.

There are a number of reasons for having a separate IDMS. An IDMS must support business processes (such as identity verification and background checks) that are outside the scope of a PACS. Where multiple systems (whether security or business applications) must support identity-based transactions, it makes sense to consolidate the management of identity information in a single system as opposed to having to directly manage multiple separate identity data repositories. For example, a university IDMS could provide a single point of management for contact, affiliation, relationship and role information on students, faculty, employees, alumni, affiliates, and prospective students—any of whom may have both physical and information system access rights and privileges.

An enterprise Identity Management System can:

- consolidate and reduce the administrative burden of managing identity information.
- minimize the number of individuals who have access to identity information (both a privacy and a security concern).
- make it feasible to upgrade and enhance the identity management capabilities, including high levels of integration into the Human Resources business processes, without having to alter numerous access control systems.

In large organizations similar reasons exist to support the separation of authentication and authorization functions, especially where there are many applications that utilize those functions. In particular this applies where authentication goes beyond personnel to include items such as documents and e-mail.

Identification

The term identification is sometimes used to mean authentication. However—with regard to electronic systems—identification has a different and specific meaning relating to enrollment, this is the meaning used in the FIPS 201 documentation. Identification is a real-world process of visually or physically verifying an individual's identity (that the person is who he

1 Note that IDMS is also an abbreviation for Integrated Database Management System. IMS is another abbreviation for Identity Management System. IdM and IDM are both abbreviations for Identity Management.

Table 1. PIV Assurance Levels

Assurance Level	Description
Some	A basic degree of confidence in the identity of the cardholder.
High	A strong degree of confidence in the identity of the cardholder.
Very High	A very strong degree of confidence in the identity of the cardholder.

or she claims to be) in an interview using appropriate documentation and references, and assigning the individual a unique identifier (such as a "username" or a unique identifying number) to allow electronic systems to distinguish the individual from other individuals. FIPS 201 refers to this process as the Identity Proofing and Registration process.

This is a critical process. If an error occurs in the identification process—either accidentally (through human or system error) or intentionally—a security vulnerability is introduced that the remainder of the system will not detect but will, in fact, enforce. This is where the trust factor enters in: how confident can we be in the identification process?

FIPS 201 defines Personal Identity Verification (PIV) authentication assurance levels, which are some confidence, high confidence, and very high confidence. In order for these assurance levels to have any validity the identity proofing, registration and card issuance processes must be sound.

To ensure that Identity Proofing and Registration can be managed closely and audited, FIPS 201 requires that the requests for security cards, approvals, images of breeder documents (such as birth certificates), demographic data, biometric information, the assigned identity serial number and its expiration date, and other registration data are securely stored in an IDMS. The IDMS controls the process flow from registration through card issuance. The IDMS must track the status of a PIV credential throughout its life cycle, from initial production request, personalization and printing, activation and issuance, suspension, revocation and destruction. The IDMS may also enable administrators to create or cancel privileges associated with each applicant. (To get a thorough understanding of how FIPS 201 requirements will impact a Federal agency, see the 179-page Federal Identity Management Handbook, available on the Web.[2] The handbook provides a road map for agencies that must meet Personal Identity Verification requirements, and issue compliant Smart Cards to Employees and Contractors by Oct. 2006.)

Thus there can be multiple points of integration for SIA member products and systems, including biometrics. The FIPS 201 standard leverages biometrics at multiple stages including identity proofing, issuance and access. The initial stage of the PIV standard (PIV I) does not require biometrics, but recommends fingerprint biometrics, while the second phase (PIV II) will require two forms of biometrics, a mandatory two fingerprints and optional facial biometrics.

Authentication

A web search for definitions for authentication yields two categories of definition: one which states that authentication is verifying identity, and another which states that authentication is verifying both identity and access privileges. Recent common usage (including FIPS 201) considers that authentication is verifying

2 The Federal Identity Management Handbook and its Implementation Checklist are available at http://cio.gov/ficc/.

identity, while authorization is verifying access privileges. It is important to note that the term authentication is often used loosely, and even within a single document can have both usages.

As mentioned above, FIPS 201 defines three levels of authentication assurance, listed in Table 1 on the previous page.

Within Federal government agencies, three aspects of the overall Personal Identity Verification processes contribute to establishing the assurance levels:

- The thoroughness and accuracy of the identity-proofing process.
- The security of the PIV card issuance and maintenance process.
- The authentication mechanisms, which are used to verify that the person presenting the PIV card is rightful holder of the card.

There are a number of Authentication methods supported by a PIV card.

Visual authentication.

This is verification performed by a security officer, and can be based upon a photograph and/or other identifying information on the card that is verified against a list or database. Prone to human error, visual authentication provides only some assurance.

CHUID (Cardholder Unique Identifier) authentication.

Unlike the typical card number/facility code encoded on most access control cards, the FIPS 201 CHUID takes authentication to a new level, through the use of an expiration date (a required CHUID data field) and an optional CHUID digital signature (defined in a following section). A digital signature can be checked to ensure that the CHUID recorded on the card was digitally signed by a trusted source and that the CHUID data has not been altered since it was signed. The CHUID expiration date can be checked to verify that the card has not expired. This is independent from whatever expiration date is associated with cardholder privileges. In the PIV scheme of things, multiple organizations can make use of a single card issued by another organization. The issuing organization will determine the expiration date for the card, while the other organizations will determine the type of access privileges they grant to the cardholder. Thus the card expiration date will reside in the issuing organization's identity management system while various access privileges (with their own expiration dates) will reside in the identity management, physical and/or logical access control systems of other organizations.

Reading and verifying the CHUID alone provides only some assurance of identity, because it authenticates the card data, not the cardholder.

(For a detailed examination of the CHUID data model and other technical aspects of creating and using FIPS 201 cards, see the Smart Card Alliance Physical Access Council white paper titled, "FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems", downloadable on the Web.[3])

3 Download the white paper at http://www.smartcardalliance.org/alliance_activities/FIPS_201_Impact.cfm.

Table 2. PIV Assurance Levels and Physical Authentication Methods

Assurance Level	PACS Authentication Methods
Some Confidence	• **Visual** by security officer using photo and/or written signature on card • **CHUID** (Cardholder Unique Identifier) contained on the security card
High Confidence	• **Unattended Biometric**
Very High Confidence	• **Attended Biometric** (security officer as witness of biometric presentation) • **PKI**

Biometric authentication.

Biometric authentication can be unattended or attended. Because a security officer can witness the biometric transaction and verify that the cardholder is not acting under duress, attended biometric authentication provides very high assurance of the cardholder's identity. Unattended biometric authentication provides high assurance.

PKI authentication.

To date, this type of authentication has been considered most relevant for logical access control systems, because it requires an online network connection that traditionally has not be available to a standalone PACS. However, because PKI authentication can be used with a PACS to provide the very high confidence level of assurance without biometrics, it is defined and discussed in more detail later in this document, in the section titled "FIPS 201 Use of Cryptography for Physical Access Control Systems". Typically PKI technology becomes more broadly deployed for information security as organizations become more widely networked. A PACS can leverage this existing customer PKI technology. This makes PKI authentication for a PACS more practical. PKI technology can make a PACS more valuable by improving the overall level of security.

It is also important to note that for access control systems in which roles are used to assign system privileges (see the later section titled Role Based Access Control), it can be entirely sufficient to securely identify the role of an individual, rather than the individual's identity. Such an approach can have many benefits including the reduction, or elimination, of data storage at or near access points, as well as improved privacy and system-security related to reducing the number of locations where sensitive, personal information must be transmitted and stored.

Table 2 presents a chart summarizing the various PACS methods of authentication and their associated PIV levels of assurance.

Improving the Management of Authentication

The Federal Identity Management Handbook states, "A robust authentication process based on [digital] credentialing technology can enhance security and create detailed audit trails while increasing protection for employee privacy rights. Ultimately, the impact of these benefits will be strongest when organizations are able to integrate their building security applications with their network security applications. In most cases, such integration is still in the future. However, it is worthwhile to consider such an architecture."[4] SIA member product and system designs should be supportive of such future integrations, to contribute to the relevance and longevity of their products as well as to maximize the

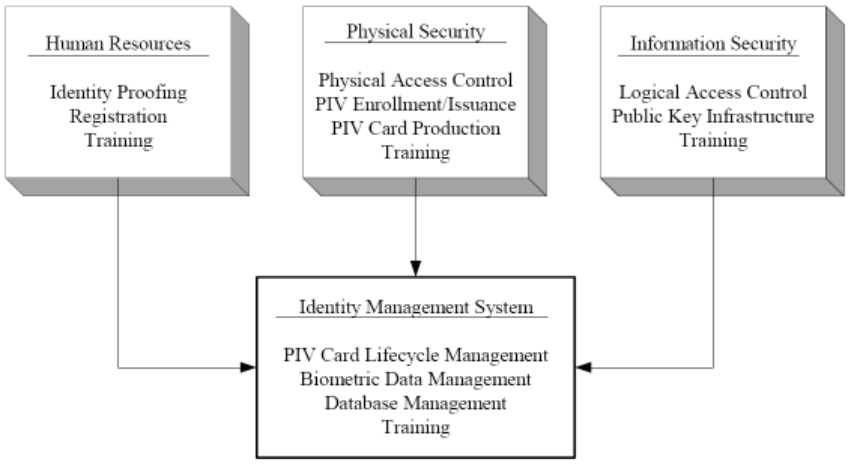
4 Page 125

customer ROI. These are not just technical issues; they impact competition and market share factors, and influence strategic alliance needs and opportunities. While such integrations are in the future, that future is not far off, as Identity Management Systems are available today for providing the kind of integration that the Federal Identity Management Handbook describes. Today, solutions exist that leverage PKI as a means to increase the size and scope of a PACS, and ultimately the benefit from it, by converging physical and logical security.

the emergence of a standardized PIV card that will encourage interoperability and file sharing. A fully integrated system can immediately reflect an employee's status, including changes resulting from hiring, termination, or altered access privileges.

Human resources, physical security, and information security departments can retain their autonomy and still integrate their data by maintaining a common centralized identity management network. The databases could be partitioned and the network might manage

Figure 1. Functionality of an example Identity Management System integration



"In recent years, human resources, physical security, and information security have begun to require and use the same data. Smart cards are already capable of communicating with physical and logical access control applications. If the back-end databases that support the applications could be integrated, an agency could benefit from consolidated security management, faster response rates, improved detection and audit control, and uniform policies. Furthermore, the convergence of PIV cardholder information is supported by

only the PIV cardholder data elements that are required for access control; the remaining files for a cardholder, such as background check results and digital certificates could be managed from a back-end database by the appropriate agency department. The information sent to the network could not be rerouted to another department's network." Figure 19 **[included in this update as Figure 1]** illustrates one possible architecture in which three otherwise autonomous departments consolidate

their PIV cardholder information in a central identity-management system."[5]

Figure 1 diagrams the functional roles in such an integration for an Identity Management System, a PACS, and an information security system.[6]

The Physical Security system shown in Figure 1 could consist of a single manufacturer's integrated security system with badge production and access control capabilities, or it could be a combination of separate products.

Authorization

Authorization is the process of verifying access privileges (also referred to as permissions). It is finding out if the identified person is permitted the access that is being requested, at the date and time of the request. Authorization is equivalent to checking a theatre ticket. At which performance and to which seat does your ticket allow you to go? Authorization is not the same as access control, although the two are often tightly coupled in a security system. For example, after checking your ticket, a theatre may require that you wait for an usher to escort you to your seat. A ticket checker makes sure that your ticket is for the right performance and that you arrived in the right section of the theatre (authorization). An usher walks you to the right row and watches to see that you actually sit in the correct seat (access control).

In a physical access control system, the access control function is completely self-contained. However, a PACS may interact with other systems for one or more of the three functions relating to authorization: defining privileges, assigning privileges (both part of user provisioning) and determining access based upon privileges (authorization).

Because the terms authentication and authorization have been used loosely and sometimes interchangeably (they even sound somewhat similar), some IT companies have replaced authenticate/authorize and authentication/authorization with the terms identify/validate and identification/validation. Thus vendor document terminology is not always identical to FIPS 201 terminology. For example FIPS 201 uses identification to refer to steps in the identity proofing process, and validation to refer to any step where the validity of an item is being checked. Within the context of some FIPS 201 discussions, authorization can also refers to a person being granted the power to issue PIV cards. Thus when reviewing existing vendor documents it is sometimes necessary to align the vendor terminology with that used in government FIPS 201 documents. It also means that SIA members must pay close attention to the terminology that they use in their verbal and written materials. Within this QTU document, authorization means the determining of access according to assigned privileges.

User provisioning is a function that includes elements of both authentication and authorization. Provisioning means to provide users with an authentication means (such as a card and PIN) and authorization privileges. Those two elements combined are what enable access to protected assets. The full scope of user provisioning goes outside of the scope of FIPS 201.

5 Pages 125-126
6 Page 126

The FIPS 201 publication states, "This standard defines authentication mechanisms offering varying degrees of security. Federal departments and agencies will determine the level of security and authentication mechanisms appropriate for their applications. This standard does not specify access control policies or requirements for Federal departments and agencies. Therefore, the scope of this standard is limited to authentication of an individual's identity. ACCESS AUTHORIZATION DECISIONS ARE OUTSIDE THE SCOPE OF THIS STANDARD."[7]

Authorization decisions at a Federal government facility are made by the local PACS manager, who defines physical access privileges of individuals at that facility. To enroll a cardholder, typically some or all of the PIV card's CHUID data is registered in the local PACS, and the cardholder is assigned specific access privileges. The cardholder can then access areas controlled by that PACS as authorized by the assigned access privileges. As has always been the case, access to highly sensitive areas may require the use of multiple identification elements as determined by the organization's policies and assurance level requirements. A combination of a card and PIN, biometric checks, and/or PKI system verification (explained later in this document) may be required. All of the parameters used are registered, processed, and verified by the local PACS (authentication) prior to determining and granting access (authorization and access control).

In the past, many organizations made access authorization decisions on an ad-hoc basis, the recent and continuing strong trend both inside and outside of government is to use security strategy and policy to determine access privileges. The larger the organization, the more critical it has become to have policy-based definition of access privileges. In the private sector, HIPAA and other regulations have also required the regular auditing of access privilege management to monitor compliance with security policy.

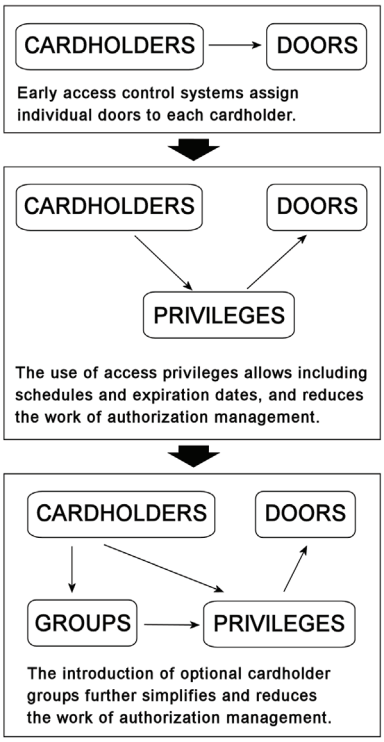
There are two major administrative weaknesses in the policy-driven management of enterprise scale access control systems:

- Identity proofing and registration (identity information management)
- Management of access privileges (authorization management)

The FIPS 201 standards squarely addresses the first weakness. The second weakness is a problem related to scale. The larger the user base and the base of protected assets, the larger the burden of authorization management. The challenge of authorization management is generally much larger for information systems access (which includes networks, databases, business workflow applications, intranets and web servers) than for physical access by several orders of magnitude. This is why many network, database and IT security software companies have produced user provisioning products for managing information access privileges. These products manage privileges across hundreds of information systems and network resources, for which there can thousands to millions of users. For example, in 2002 Lehman Brothers began implementing enterprise-wide access control

7 Page 2

Figure 2. History of authorization in physical access control.



for 19,000 employees spread across hundreds of business units on three continents, and several hundred business-critical applications. They deployed a company-wide user-access privileges-provisioning system and enterprise identity management system (one system to perform both functions). The employee base represented more than 400,000 unique user accounts across their IT resource base. Lehman Brothers reported that with the new system, the time it takes to set up new user access accounts has shrunk from five days to 20 minutes; denying user access has been reduced from one week to a mere 60 seconds.[8] Many other organizations report similar benefits to implementing enterprise-wide systems.

Information systems access control began encountering large-scale authorization management challenges a decade earlier than physical access control. So although FIPS 201 does not provide guidance on authorization management, guidance is available by looking to real-world applications like the Lehman Brothers case study or even the U.S. Department of Defense (DoD). While Lehman Brothers grappled with managing security privileges of 19,000 employees, the DoD wrestled with managing security privileges for 4 million Common Access Card (CAC) users. For both organizations Role Based Access Control (RBAC) is a primary factor in getting a handle on authorization management. First introduced to the IT world about 10 years ago by the National Institute of Standards and Technology (NIST), RBAC did not come in to broad use until recent years, with the widespread appearance of large-scale information systems. As RBAC has become the single-most effective approach to managing large-scale access control, the American National Standards Institute (ANSI) adopted it as a standard in 2004.[9]

Role Based Access Control

The basic concept of RBAC is that within an organization, roles are created for various job functions, and personnel are assigned a specific role. Corresponding roles are created in the access control system, and access privileges are assigned to those roles (as opposed to being assigned directly to personnel). Thus, personnel acquire access privileges by being assigned a role. This use of roles facilitates policy-based management of access control that mirrors the actual job requirements of personnel. RBAC is actually the next step in the progression of physical access control management. At first glance there is a superficial similarity between RBAC and conventional group mechanisms. Figure 2 shows the historical development of physical access control authorization management, culminating in the use of cardholder groups to help simplify the management of authorization.

However, there are some significant differences between RBAC and groups. The purpose of RBAC is to enable and enforce policy-based access control in an auditable manner, and to allow access roles to align with actual personnel roles within the organization, as shown in Figure 3 and Figure 4 at right.

In a PACS, groups are normally implemented as a collection of cardholders as opposed to a collection of privileges. In a PACS that sup-

8 Ted Samson, "Lehman Brothers puts identity in a vise grip," InfoWorld (November 14, 2005).

9 For more information see the RBAC web site: http://csrc.nist.gov/rbac/.

ports cardholder groups, privileges can usually be assigned both to individual cardholders and to groups. The assignment of individual cardholder privileges can bypass group policy, and make the auditing of access authorizations against policy non-feasible for large numbers of cardholders. In a PACS that supports groups of privileges there is no mechanism to enforce policy about the way that privileges are collected into groups.

Thus, in contrast to typical group schemes, RBAC has the following features when properly implemented:

- Privileges are assigned to Roles. This contributes to scalability, since in most large organizations more than one person has the same role (sales person, accountant, auditor, receptionist and so on).
- Roles are assigned to Cardholders. Roles are designed to parallel actual organizational roles, which simplifies management and allows role assignment to be accurately done as part of the Human Resources personnel enrollment process.
- Only one Role is assigned to one Cardholder. This facilitates simple audit of access against organizational policy, since individual privileges don't have to be examined to determine the scope of a cardholder's access. The assigned Role states it.
- Roles are hierarchical—they can inherit privileges from other Roles. This is required in order to parallel real-world organizational functional roles, and to make it possible to implement the "one role per user" rule.

Figure 4 shows how a Cardiologist has privileges specific to a Cardiologist, while also

Figure 3. Role Based Access Control.

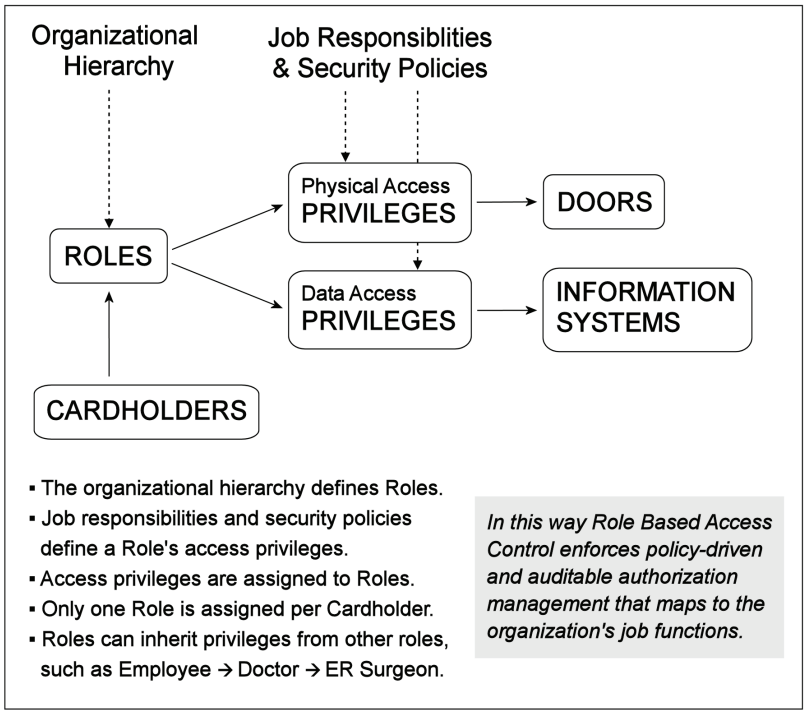
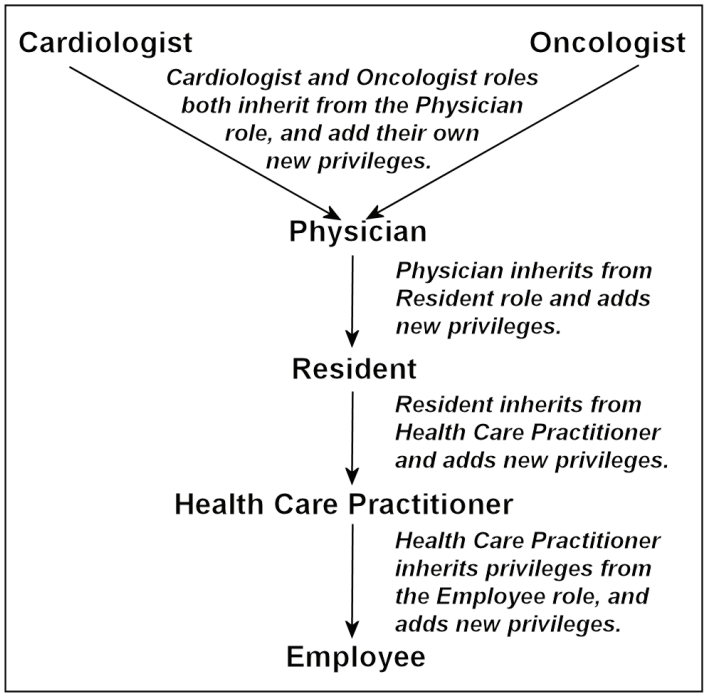


Figure 4. Example of a functional role hierarchy.



inheriting privileges assigned to the roles of Physician, Resident and Employee. A change to Employee access affects all roles that inherit privileges from the Employee role. A change to Cardiologist access privileges would not affect an Oncologist or a Resident, or any role below Cardiologist in the inheritance hierarchy.

RBAC can be used to unify the management of physical and information systems access. The same organizational Roles can be used by physical security and information security to establish appropriate Role privileges, based upon organizational policy and job function needs. This allows policy-based information security to be implemented easily for both physical and electronic forms of information. By utilizing physical and information access control systems that implement RBAC, physical and information security can be synchronized based on policy even if the physical and information access control systems are not integrated. However, the greatest return on investment and business process improvement would come from integrating the physical and information access control systems with an Identity Management System used to manage Roles for the entire organization.

Most Federal agencies are adopting, or have already adopted, RBAC for information security. A significant opportunity exists to improve the management of physical security by leveraging off the existing RBAC efforts of customer organizations.

Although for many organizations information access control is larger in scope and complexity than physical access control, that is not always the case. The Department of Homeland Security's Transportation Security Administration (TSA) plans to issue smart cards to up to 15 million transportation workers who require unescorted access to secure parts of transportation venues. Most of them will not require information systems access. Thus, even without an alignment with information security, there will be large-scale physical access control systems that can benefit from the use of RBAC.

Furthermore, the ability to design, enforce and audit policy-based physical access control can be of significant value to both public and private sector enterprises, especially for critical infrastructure sector organizations and organizations with HIPAA or other regulatory requirements.

Cryptography

The discussion of digital certificates and cryptography has been saved for the latter part of this section on technology impacts. It is easier to grasp the roles of digital certificates and digital signatures within FIPS 201 when the elements of FIPS 201 presented earlier are understood.

Cryptography is the study and practice of protecting information by data encoding and transformation techniques. It includes means of hiding information (such as encryption) and means of proving that information is authentic has not been altered from its original form (such as digital signatures).

In the physical world, a key is the device used to open or close a lock. Thus, in cryptography the information used to "lock" data to protect it is called an encryption key, a cryptography key or sometimes just a key when the context allows it.

Microsoft Word and other programs use a password as the key to encrypt a document, taking the computer's numerical value for each letter (65 for A, 66 for B, and so on) to perform an advanced numerical calculation that transforms each character of the document text. When the same password is typed again to unprotect the document, the reverse transformation is performed.

When the same key is used to encode and decode the information, it is referred to as Secret Key or a Private Key (because it has to be kept secret to protect the encoded information). It is also called a Symmetric Key, because the same key is used for both operations.

Similar to the way in which physical keys must be safeguarded to keep unauthorized individuals out of locked areas, so must secret keys be safeguarded in order to keep the information from being accessed or altered by unauthorized individuals. Like a physical key, the more copies of this key that are made and shared, the higher the risk that one of them may be stolen and everyone compromised.

If a physical access key is stolen, one changes each lock that the stolen key fit, rendering the original key of no use. One can make physical keys "expire" simply by changing the corresponding locks.

The same scenario is not true for information protection because protected information is typically shared, copied and stored (collected). Once the secret key is obtained, all of the collected information protected by that particular key can then be "unlocked". Changing the key only protects newly encoded information. It has no effect on information that was previously encoded. Thus, the management of cryptographic keys can be a more difficult and complex task than the management of physical locks and keys.

To share information that is protected as previously described requires sharing the secret key. To eliminate the information sharing risk explained in the previous paragraph would require using a different secret key for very piece of information protected. This quickly becomes an unfeasible key management problem. For this reason, it is said that symmetric key systems don't "scale up". The sharing of secret keys is not manageable for large systems, which become more at risk the larger the size of the system.

This problem was solved in the mid 1970's, when a new form of protection was developed based upon the fact that a pair of very large numbers can have a special relationship to each other, whereby what you encode with one number (using special methods) you can decode only with the other number, and vice-versa. Yet you cannot figure out one number if you have the other number.

These two cryptographic keys are known as a Public Key/Private Key pair, because the user makes one key public and keeps one key private. If you imagine yourself in the position of having such a pair of encryption keys, you can see their use and value. If you want people to be able to protect information for you that only you can access, you give them your Public Key. Anything encoded with your Public Key can only be decoded and read by you and you alone (using your Private Key, which is why you keep it private). Similarly, if you want to encode something so that only one particular friend can decode it, you use

your friend's Public Key. Your friend uses his own Private Key to decode and read it. Rather than call this method of protection "Public Key/Private Key encoding" it is simply referred to as Public Key cryptography (in contrast to Private Key or Secret Key cryptography). This technique is also known as "Asymmetric Cryptography", because a different key is used to decode the information than was used to encode it. Private and public keys are often referred to as asymmetric private keys, asymmetric public keys, or simply asymmetric keys to refer to them both.

Since no secret keys are shared, public key cryptography allows two parties (or two systems) to securely communicate with each other without prior contact.

There is yet another benefit to the Public/Private pair of keys. Put yourself in the position of wanting to publish some important information. You want to make sure that the information is not altered, so you encode it with your Private Key. Anyone who has your Public Key can decode it, which proves two things: that it came from you and that it was unaltered. (If the encoded message had been altered, your Public Key would not work to decode it.) This is the principle behind a Digital Signature. To sign an e-mail message, cryptographic software built into the e-mail system performs a calculation involving both the private key and the message. The result of the calculation is called a digital signature and is attached to the message. To verify the signature, the message recipient's e-mail system does a computation involving the message and the digital signature. If the result is correct, the signature is verified to be genuine; if not, the signature is fraudulent or the message has been modified.

Thus a Digital Signature is used to perform two types of information authentication: it authenticates the sender by proving who the sender was, and authenticates the information by proving that is has not been altered.

Digital Certificates and PKI (Public Key Infrastructure)

To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's own private key. However, public and private key pairs are just numbers, having no intrinsic association with any person. Some scheme or strategy is necessary to reliably associate a particular person or organization to a particular key pair. The solution is the use of one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as a certificate authority or certification authority (CA), because it issues electronic certificates known as digital certificates. The person or organization to which the digital certificate is issued is known as a subscriber. A registration authority (RA), also part of the third party system, performs subscriber identification and verifies the accuracy of the information in the subscriber's certificate request.

A digital certificate is a specially formatted block of data that among other things: (1) contains the certificate's serial number, (2) identifies the certificate authority issuing it, (3) names or identifies the certificate's subscriber, (4) identifies the period of time for which the certificate is valid, (5) contains the subscriber's public key and (6) is digitally signed by the certificate authority issuing it. By digitally signing the issued certificates, the

certificate authority guarantees the authenticity of the data held in them (See Figure 5 at right).

The certificate authority stores the digital certificates it publishes in a computer database or network directory, which it makes available online (in a local area network or on the Internet) so that software applications can verify digital signatures as needed. Certificate verification is performed automatically by the software of systems that use digital certificates for information protection.

The publication of digital certificates is what enables two parties (or systems) to use certificates to communicate securely without any prior contact.

The international standard governing the format of digital certificates is X.509, a specification for digital certificates published by the ITU-T (International Telecommunications Union - Telecommunication). FIPS 201 requires X.509 digital certificates.

A Public Key Infrastructure (PKI) is a security management system including hardware, software, people, processes and policies (including CAs and RAs), dedicated to the management of digital certificates for the purpose of achieving secure exchange of electronic information. The term PKI is also sometimes used loosely simply as a reference to public key cryptography. Because a digital certificate contains the public key of the subscriber, it is sometimes also called a public key certificate or PKI certificate (FIPS 201 uses all three terms).

Digital Certificate Verification

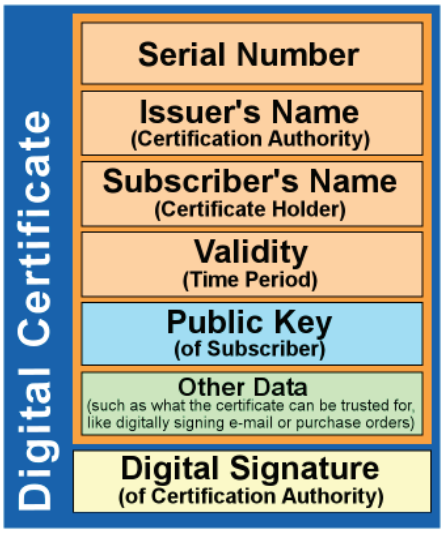
A digital certificate is no longer valid if it has expired or been revoked. Because PIV card authentication certificates typically will last several years, a certificate revocation mechanism is necessary. There are two methods of determining if a certificate has been revoked: checking a locally stored certificate revocation list (CRL) issued by a certification authority, and using the online certificate status protocol (OCSP) to obtain the real-time status of the certificate from a server (which checks its own copy of a CRL issued by a certification authority). For enterprise systems, CRLs can become too large to be copied to local systems each time they are updated. Continual copying would consume too much network bandwidth. Using OCSP allows real-time checking of certificate status without having to copy a CRL to the local system. The OCSP protocol is specified in the "Request for Comments (RFC) 2560" document published by the Internet Engineering Task Force.

When an access control or other system sends a request for certificate status information to an OCSP certificate status server (also called an OCSP responder), the server sends back a response of "good", "revoked," or "unknown." The protocol specifies the syntax for communication between the server (which contains the certificate status) and the system requesting status information. FIPS 201 requires that Certification Authorities issuing certificates for PIV cards maintain both a server providing CRLs and an OCSP certificate status server.

Digital Signature

A digital signature is additional data that is appended to data in transit or storage. It has two significant benefits. First, similar to a written signature, it can be checked to verify who the sender is. Second, similar to a tamper-evident seal on a package, checking the digital signature also reveals whether or not

Figure 5. Primary items contained in a digital certificate.



the data has altered since it was signed. Digital signatures can be used on all types of electronic communications including documents, web pages, e-mail and electronic commerce.

A digital signature is the result of encrypting a hash of the data to be transmitted or stored. A hash (also called a digest) is a number generated by applying a mathematical formula to a document or sequence of text. The hash is significantly shorter than the original text and is unique to the original text. Changing even one letter in the original text will result in a different hash value. This is very similar to the checksum functions commonly used in communications protocols to verify the integrity of the system messages. Typically the creation of a checksum is done by adding up the numerical values of each letter in a message (such as 65 for A, 66 for B and so on) in a special way. This results in a "sum" used to "check" the message. If any letter in the message is changed, the checksum value changes. Hashes are created using very advanced mathematical formulas. The probability of generating the same hash value with two different sets of data is less than one one-thousandth of a percent.

Figure 6 below illustrates the process of creating a digital signature. Figure 7 below shows the process of verifying a digital signature.

FIPS 201 Cryptographic Keys, Digital Certificates and Digital Signatures

FIPS 201 specifies that, at a minimum, the PIV Card must store one asymmetric private key called the PIV authentication key and a corresponding public key digital certificate, and perform cryptographic operations for authentication (such as "challenge and response" described in a later section) using the asymmetric private key. The FIPS standard states that this key must only be available through

Figure 6. Signing a document with a digital signature.

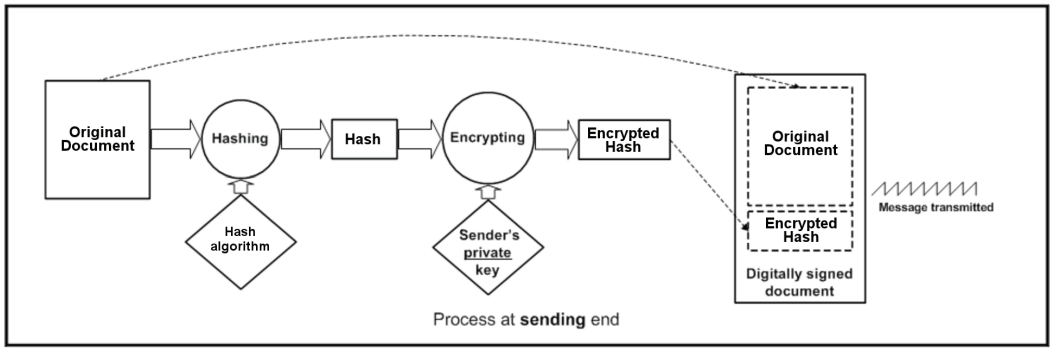
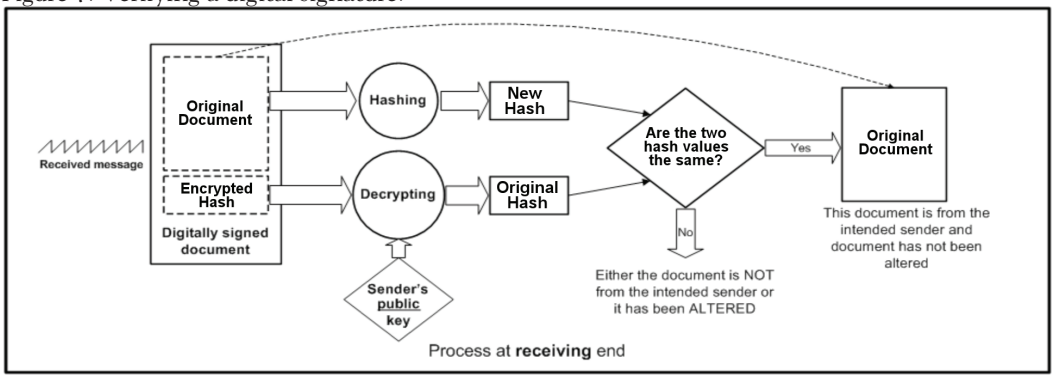


Figure 7. Verifying a digital signature.



the contact interface of the PIV card.[10] Additionally, cryptographic operations are considered privileged operations, and a PIN must be provided by the user before cryptographic operations can be performed. Additionally, there are four optional types of keys that may be stored on the card and used for designated purposes via the contact interface only:

- The card authentication key may be either a symmetric (secret) key or an asymmetric private key for physical access (more on this in the following section). This key is the only key available through the contactless interface, and unlike the other four key categories does not require (or support) use of a PIN to restrict access to cryptographic operations using the key.
- The digital signature key is an asymmetric private key supporting document signing.
- The key management key is an asymmetric private key supporting key establishment and transport. This can also be used as an encryption key.
- The card management key is a symmetric key used for card personalization (initializing the card for a specific cardholder) and post-issuance activities.

The card must hold the X.509 digital certificate for each asymmetric key on the PIV Card.

FIPS 201 specifies that the Cardholder Unique Identifier (CHUID) on the card be digitally signed. A PIV card also contains, at a minimum, two digitally signed fingerprint images. Other biometric data may optionally be stored on the card. All biometric data on the card must be digitally signed using the Common Biometric Exchange Formats Framework (CBEFF) signature block.

The FIPS 201 document references several NIST publications that provide details about these requirements:

- The cryptographic algorithms, key sizes, and other details relating to the use of PIV card cryptographic keys are specified in the NIST publication Special Publication SP 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification.
- The technical acquisition and formatting requirements for biometric data of the PIV system are specified in Special Publication SP 800-76: Biometric Data Specification for Personal Identity Verification.
- The required common format for storing biometric data is specified in NISTIR 6529-A: Common Biometric Exchange Formats Framework (CBEFF).

FIPS 201 requires that the generation, handling and physical security relating to all PIV cryptographic keys shall meet certain specific

10 PIV cards must contain both contact and contactless interfaces, which may be provided by two separate integrated circuit chips (ICC) or by one dual-interface chip. The contact interface must conform to the ISO/IEC 7816 specification, and the contactless interface must conform to ISO/IEC 14443. In most cases, physical access applications will use the contactless interface, which is the type of interface customarily used in our industry. Although the FIPS standard makes provision for additional cryptographic keys to be stored for use with the contactless interface; their use is not mandated and it cannot be assumed that all card issuance systems will support them. There are special cases in which the contact interface will be used for physical access applications, because the interface commands used authenticate to the very high confidence level are not available through the contactless interface.

requirements of FIPS 140-2: Security Requirements for Cryptographic Modules.

FIPS 201 Use of Cryptography by Physical Access Control Systems

Prior to FIPS 201 the use of cryptography in physical access control systems has been for encryption of Ethernet network traffic (front end system to panels, front end system to workstations, and panels to readers). FIPS 201 introduces the additional cryptographic elements of digital certificates and digital signatures to provide strong authentication of the card, the data elements on the card including biometric data, and also of individual card management systems.

Under FIPS 201 the term credential has two meanings: (1) the PIV card itself and (2) the data elements associated with an individual that authoritatively bind an identity to that individual (also called credential data elements or credential elements). Credential elements that are stored on the cards are called logical credentials.

PIV logical credentials fall into three categories:

1. Credential elements used to prove the identity of the cardholder to the card (CTC authentication). PINs are in this category.
2. Credential elements used to prove the identity of the card management system to the card (CMTC authentication). Card management cryptographic keys fall into this category.
3. Credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system. The CHUID, biometric information, and cryptographic keys are in this category.

Furthermore FIPS 201 establishes a means of authenticating a cardholder to the very high assurance level using asymmetric cryptography (PKI), by following these steps:

1. The cardholder is prompted to enter a PIN.
2. By entering the correct PIN, the cardholder activates the PIV card and allows a card reader access to cryptographic operations.
3. A "challenge and response" authentication is initiated by the reader. The card reader issues a challenge request to the card.
4. The PIV card creates a response, and signs it with the PIV authentication private key.
5. The card reader verifies the response digital signature and verifies the related digital certificate (according to X.509 certificate policy). The digital certificate is checked to ensure that it is from a trusted source. The status of the certificate is checked to ensure that the certificate has not been revoked.
6. The response is then validated as the expected response to the issued challenge.
7. The PACS then extracts the Federal Agency Smart Credential Number (FASC-N) from the digital certificate, and passes it as input to the PACS cardholder authorization function.

Note that the above steps for **very high** assurance authentication may require the PACS to have an online network connection for certificate verification and certificate status

checking. Steps 1 through 7 above replace the typical PACS single step of reading a card number from the card. They require that the PACS interact with an external system for certificate verification, either periodically or in real-time, as part of the authentication process.

All PIV cryptographic operations (including those performed by a PACS) require cryptographic modules that have been certified to meet the FIPS 140-2 standard. A cryptographic module is software, firmware, hardware or some combination thereof that implements cryptographic functions such as digital signatures and encryption. A PACS system or component manufacturer must either develop its own cryptographic modules as required for its applications, and get them certified, or utilize already-certified cryptographic modules developed by others. The NIST web site lists over 150 companies with certified cryptographic modules that are either components or complete products.[11]

FIPS 201 Compliance

Within the scope of this QTU the technical elements of FIPS 201 can only be briefly introduced. The phrase "FIPS 201 compliant system" describes a broad spectrum of functionality, not a specific design. For SIA members, determining which parts of the standard to implement will require a thorough examination of the FIPS 201 standard and related specifications, and then reconciling those technology elements with the security system requirements of their intended customer market.

III. CONCLUSION

The growth of enterprise-wide access control requirements, the convergence of physical and logical security, the emergence of Identity Management systems, the classification by customers of physical security systems as IT systems, and the introduction of digital certificates and digital signatures as part of the cardholder authentication process—all of these have changed the technological environment in which PACS systems must operate.

The impacts of the technology elements of FIPS 201 are not confined solely to Federal, state or local government systems. After all, these technologies come from the general world of information technology, where they are being applied to address the challenges of enterprise scale security management in both the private and public sectors.

The widespread adoption of these technologies, as part of very large-scale security system deployments, brings significant opportunities for market growth. To achieve that growth will require the expansion of security industry technology, through product development engineering and service offering expansion by SIA members.

Author
By Salvatore A. D'Agostino, Dave Engberg, and Andrew Sinkov of CoreStreet
Ray Bernard, PSP, of RBCS contributed to this paper
www.corestreet.com
www.go-rbcs.com

11 "FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List", NIST Cryptographic Module Validation Program, http://csrc.nist.gov/cryptval/140-1/1401val.htm

Glossary

algorithm
An algorithm is a step-by-step procedure for carrying out a mathematical computation or a transformation of data, usually used in reference to work performed by a computer.

assurance level
See identity authentication assurance level.

asymmetric cryptography
Asymmetric means that two parts of a thing are not similar (not symmetric). In asymmetric cryptography a private key is used for creating a digital signature, and the related public key is used for verifying the signature. Because the keys for each process are different the processes are described as being asymmetric. Asymmetric cryptography is a synonym for public key cryptography (also see).

asymmetric key
In asymmetric cryptography (also see), an asymmetric key is one key of a pair of asymmetric keys (a public key and a private key). See public key cryptography.

authentication
Simply put, authentication is verifying identity. Authentication is the process of determining whether someone or something is actually who or what it asserts itself to be. In the context of an access control system, it refers to the process of identifying the individual or system requesting access, by checking the credentials presented against the information stored in the system. Also see identify.

authentication assurance level
See identity authentication assurance level.

authorization
Authorization has two meanings: (a) the assignment of access rights to an individual or system in an identity management system or access control system (also see user provisioning) and (b) the decision process by an access control system of determining whether or not access should be granted at the time an access request is made, based upon the rights that have been assigned.

CA
Acronym for certificate authority (or certification authority).

cardholder unique identifier
See CHUID.

certificate
See digital certificate.

certificate authority (also certification authority)
A certificate authority, or CA, is the person or company who issues, revokes and manages digital certificates to subscribers. A CA acts as a trusted "third party" certifying the identity of subscribers to anyone who receives a digitally signed message.

certificate request
A subscriber receives a digital certificate by requesting one from a certificate authority.

certificate revocation list
A list of digital certificates that have been revoked (cancelled) before their expiration date. A certificate revocation list is commonly referred to by its acronym, CRL.

CHUID
In FIPS 201 the cardholder unique identifier (CHUID) is a standard data model for cardholder identification data.

common user provisioning
Common user provisioning (also called one-step provisioning) means having a single point of employee registration and dismissal (usually in a Human Resources system) with automatic assignment and revocation of both physical and information security privileges.

credential
A credential is generally defined as evidence (usually in printed form) concerning one's right to credit, confidence, authority or privileges. Security systems have two categories of credentials used to verify identity and perform authentication of privileges: physical visual credentials (such as a photo ID badge) and electronic credentials (information stored on a security card or in a computer database). Electronic credentials are also called logical credentials. In the context of FIPS 201, the PIV card is a physical credential—a smart card—with specific information printed on it and specific information encoded in the smart card memory. The data encoded on the PIV card is a logical credential.

CRL
Acronym for certificate revocation list.

cross-credentialing
An arrangement between organizations whereby each organization accepts credentials issued by the other. This requires collaboration with regard to many issues including security, privacy, trust, operating rules, policies and technical standards. The intent of FIPS 201 is to enable cross-credentialing for Federal agencies and their contractors.

cryptographic key
A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation to be performed on the data being encrypted or decrypted. The key is used to "lock" the data by encrypting it and "unlock" it by decrypting it. Keys are also used in other cryptographic algorithms, such as digital signatures and other schemes for authentication of information.

cryptography
Cryptography is the study and practice of protecting information by data encoding and transformation techniques. It includes means of hiding information (such as encryption) and means of proving that information is authentic and has not been altered from its original form (such as digital signatures).

decryption
The changing of encrypted information back into readable form using a decryption key.

digital certificate
A digital certificate (sometimes called a digital ID) is the electronic counterpart to a driver license, passport or membership card. It is specially formatted block of data that serves as a form of personal identification that can be verified electronically. A digital certificate is what binds a public key to an identity (a person or system) and is a means of establishing trust in electronic communications. The certificate is issued by a trusted authority (called the certificate authority). This authority stores the digital certificates it publishes in a computer database or network directory, which it makes available online (in a local area network or on the Internet) so that software applications can verify digital signatures as needed. Certificate verification is performed automatically by the software of systems that use digital certificates for information protection (such as e-mail systems).

digital certificate subscriber
The person to whom a digital certificate is issued, usually simply referred to as the "subscriber" in discussions about digital certificates.

digital communications
The use of electronic digital signals (ones and zeros) to send information between electronic devices or systems using wired, wireless (radio) or fiber-optic means of transmission.

digital signature
A digital signature is additional data that is appended to data in transit or storage. It can be checked to verify who the sender is, and to determine whether or not the data has been altered since it was signed. Digital signatures can be used on all types of electronic communications including documents, web pages, e-mail and electronic commerce. Digital signatures are sometimes called public key digital signatures, because the signature is verified using the signer's public key.

electronic credential
Information stored on a security card or in a computer database as evidence of privileges or authority. Also see credential.

encryption
The changing of information into an unreadable form to prevent unauthorized individuals or systems (i.e. those that don't have a decryption key) from reading the information.

Ethernet
Ethernet is a local-area network (LAN) protocol developed by Xerox Corporation in cooperation with DEC and Intel in 1976. It is one of the most widely implemented LAN standards.

FIPS 201
Federal Information Processing Standard (FIPS) Publication 201, commonly known by the shorter name FIPS 201, is titled: Personal Identity Verification (PIV) of Federal Employees and Contractors. It is both a standard and a specification. FIPS 201 specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently

verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.

This standard does not specify access control policies or requirements for Federal departments and agencies.

FASC-N

See Federal Agency Smart Credential Number.

Federal Agency Smart Credential Number

The Federal Agency Smart Credential Number (FASC-N) is one of the data items contained within the CHUID, and uniquely identifies a PIV card. The FASC-N replaces the SEIWG-012 definition, which has been in use for over 10 years.

hash

A number generated by applying a mathematical formula (an algorithm) to a document or sequence of text, used for verifying that the document has not been changed since the original hash value was generated. A hash is significantly shorter that the original text. The hash number is unique to the original document, thus attaching it to a document has negligible impact on the overall size of the document. The algorithm works one-way: it yields the same hash result every time for the same message, and it is not possible in practice for a message to be reconstituted from the hash result. Also, two different messages cannot produce the same hash results. Thus if the sender creates a hash for a document and provides it to the recipient of the document, the recipient (applying the same algorithm) can create a hash value and verify that the hash is identical to the sender's hash, which means that the document has not been altered. Hashes are used in the creation of digital signatures.

identify (identification)

Within the context of a Personal Identity Verification system defined by FIPS 201, identify means the real-world process of visually and physically verifying an individual's identity by verifying identification documents and conducting an in-person interview, before registering the person into the identity

management system. This initial verification of identity is referred to as identification.

In the context of an access control system, identify means to locate the security system's stored identity information that is associated with the security card or other credential presented to the system, and in some cases performing additional verification using that information such as checking a PIN, comparing a stored biometric to a captured biometric, or performing human visual verification of identifying characteristics. This is called authentication. Where roles are used to assign system privileges, it may be sufficient to securely identify the role of the person rather than the individual personal identity when performing authentication.

identity

Within the context of a business system or security system, identity generally has one of two meanings. First, it refers to identity information (such as an identifying name or number) that is unique within the system, plus additional information that usually includes one or more of the following: identifying characteristics, which individuals and systems will use to perform an identification; system or organizational role, used to determine the specific rights and authority granted; and the period of time for which the identify information may be relied upon. Oftentimes one particular part of the identity information is referred to as the identity, such as a name or a role within the system. Second, identity can refer to a person, physical object (such as a security smart card), data object (such as a biometric signature on a card) or computer system that is being verified as authentic by the system.

identity assurance level

See identity authentication assurance level.

identity authentication assurance level

There are three identity authentication assurance levels defined in FIPS 201. They express the level of confidence that the cardholder has presented a credential that correctly references the cardholder's identity. The three levels defined are named Some Confidence, High Confidence, and Very High Confidence. The following terms also have the same meaning and are used interchangeably: PIV authentication levels, PIV assurance levels, identity assurance levels, authentication assurance levels and assurance levels.

identity management

Strictly speaking identity management is the identification of authorized users and their enrollment in a system that is used to manage their identity information. However, the management of identity information is not an end in itself—it is used to facilitate business activities such as physical access control, information systems access control, and workflow automation in accordance with business policies. This identity management is an integrated system of business processes, policies and technologies. Also see identity management system.

identity management system

An identity management system (IDMS) identifies individuals in a system and controls their access to resources within that system by associating user rights and restrictions with each identified individual. The FIPS 201 standard requires that an identity management system be used to manage the identity information

required for the Personal Identity Verification process specified in the standard.

IDMS
Acronym for identity management system.

interoperability
Interoperability refers to the ability of a system or a product to work with other systems or products without special effort on the part of the customer. In the context of FIPS 201, it also refers to the ability of different Federal agencies to utilize the same PIV card and PIV management processes so that sufficient trust is established to allow one agency to accept and utilize a PIV card created by another agency.

logical credential
See electronic credential.

OCSP
See Online Certificate Status Protocol.

Online Certificate Status Protocol
Online Certificate Status Protocol (OCSP), as defined by the IETF RFC 2560, is a method for systems to verify the status of a digital certificate (to determine whether or not it has been revoked) by sending a status query to a server and receiving a real-time response about the status of the certificate.

PACS
Acronym for physical access control system.

PACS 2.2

The short name for a document titled, Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2 , published in July of 2004 by the Physical Access Interagency Interoperability Working Group (PAIIWG) of the Government Smart Card Interagency Advisory Board (GSC-IAB). The document is also commonly referred to as PACS Implementation Guidance Version. 2.2.

PACS Assurance Level
See PACS Assurance Profile.

PACS Assurance Profile
The PACS 2.2 document introduced the term "assurance profiles" and defined high, medium and low assurance profiles. These are similar to but different from the FIPS 201 PIV Identity Authentication Assurance Levels. Some documents refer to these assurance profiles as "PACS assurance levels" or "card assurance levels."

permissions
Permissions is the term commonly used to refer to the access rights provided by information access control systems. In physical access control systems the common term is privileges.

Personal Identity Verification
Personal Identify Verification (PIV) is the term designated in FIPS 201 for the processes and technologies involved in (a) identification: verifying the identity of a Federal employee or contractor at the time of initial identification

and enrollment into a Federal agency's identity management system, and (b) authentication: verifying the identity of the employee or contractor for purposes of physical and information systems access control.

physical credential
A document that contains printed identification information and often contains a photograph, signature, or both as evidence of identity and of one's right to credit, confidence, authority or privileges. Examples of physical credentials are the driver license, passport, and security photo ID badges. See also credential.

PIV
Acronym for Personal Identity Verification.

PIV authentication level
See identity authentication assurance level.

PIV card
A smart card that is designed, issued and managed according to the specifications in FIPS 201 and its related technical documents.

PIV identity assurance level
See identity authentication assurance level.

PKI
See public key infrastructure.

private key
The published key of a public/private key pair. See public key cryptography.

privileges
Privileges is the term commonly used to refer to the access rights provided by physical access control systems. In information access control systems the common term is permissions.

provisioning
See user provisioning.

public key cryptography
Public key cryptography is a form of cryptography which generally allows individuals or systems to communicate securely without having prior access to a shared secret key (symmetric key). This is done by using a pair of cryptographic keys, designated as public key and private key, which are related to each other mathematically. What you encode with one key you can decode only with the other key, and vice-versa. Yet you cannot figure out one key if you have the other key. This allows one key to be made public without risking disclosure of the other key that is kept private.

Thus the two cryptographic keys are known as a "public key/private key pair". Public/private key pairs have a number of uses, including encryption and the computations involved in creating and verifying digital signatures. Public key cryptography is also known as asymmetric cryptography, because a different key is used to decode the information than was used to encode it. Private and public keys are often referred to as asymmetric private keys, asymmetric public keys, or simply asymmetric keys to refer to them both.

public key digital signature
See digital signature.

public key encryption

Encryption using a public/private key pair. See public key cryptography.

public key

The published key of a public/private key pair. See public key cryptography.

public key infrastructure

A public key infrastructure (PKI) is a security management system including hardware, software, people, processes and policies (including certificate authorities and registration authorities) dedicated to the management of digital certificates for the purpose of achieving secure exchange of electronic information. The term PKI is also sometimes used loosely simply as a reference to public key cryptography. Because a digital certificate contains the public key of the subscriber (the person the certificate was issued to), it is sometimes also called a public key certificate or PKI certificate (FIPS 201 uses all three terms).

RA

See registration authority.

RBAC

Acronym for Role Based Access Control.

registration authority

The registration authority (RA) is the person or company responsible for the identification and authentication of digital certificate subscribers prior to certificates being issued by the certification authority. The registration authority does not sign or issue the certificates (the certificate authority does). The registration authority is responsible for the accuracy of the information contained in a certificate request.

Role Based Access Control

The basic concept of Role Based Access Control (RBAC) is that within an organization, roles are created for various job functions, and personnel are assigned a specific role. Corresponding roles are created in the access control system, and access privileges are assigned to the roles (as opposed to being assigned directly to personnel). Thus personnel acquire access privileges by being assigned a role. This use of roles facilitates policy-based management of access control that mirrors the actual job requirements of an organization's personnel.

SEIWG-012

SEIWG-012 is a Federal standard for security card identification that defines a numerical sequence of 40 digits containing several different numbers such as an "agency code" and a "credential code". It is named after the group that developed it, the Security Equipment Integration Working Group (SEIWG), a sub-group of the Physical Security Equipment Action Group (PSEAG), which is a DoD organization that coordinates all of the physical security research and development efforts across the armed services. FIPS 201 specifies a new standard that replaces the SEIWG-012, the Federal Agency Smart Credential Number (FASC-N).

subscriber
See digital certificate subscriber.

symmetric cryptography

Symmetric means that two parts of a thing are similar. In symmetric cryptography the same key is used for both encrypting and decrypting data Also see asymmetric cryptography.

symmetric key
The single key used for symmetric cryptographic operations. See symmetric cryptography.

TCP/IP
TCP/IP is an acronym for Transmission Control Protocol/Internet Protocol, a protocol for communication between computers, used as a standard for transmitting data over networks and the Internet.

user provisioning
Provisioning means to provide users (such as the cardholders in an access control system or the users of a computer-based information system) with two things: (1) a means to authenticate themselves (such as a card and PIN, or name and password), and (2) access privileges. Those two elements combined (a means to authenticate and privileges) are what enable access to protected assets.