Using FIPS 201 and the PIV Card for the Corporate Enterprise

A Smart Card Alliance White Paper

Publication Date: October 2008

Publication Number: IC-08002

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

About the Smart Card Alliance

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

Copyright © 2008 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Table of Contents

Smart Card Alliance © 2008

Using FIPS 201 and the PIV Card for the Corporate Enterprise

Corporate enterprises have always required employees to carry cards or badges that verify the employee's identity and allow the employee to access enterprise resources. However, changes in both the regulatory environment and the amount of risk that enterprises face from unauthorized access are driving executives to reevaluate their identity management practices. How should a potential employee's identity be verified? How can corporate security ensure that only authorized employees have access to facilities, enterprise networks, and computers? How can authorized employees use identity credentials to access enterprise resources easily and efficiently?

Establishing a robust identity management framework within an enterprise requires both the implementation of new business processes and the selection of appropriate credentialing technology. While there are many approaches to enterprise identity management, industry and government have worked for over 10 years to develop both a standardized identification process within the government and specifications for proving an individual's identity and providing individuals with a secure identity credential. The process and technical specifications, which are now being implemented throughout the Federal Government, are documented as Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*. This standard provides an identity management framework that enterprises should regard as a best practice in the design and implementation of their own identity management programs.

This white paper provides a high level overview of FIPS 201 and a summary of the benefits of considering this standard as a starting point for achieving identity assurance and access control across the corporate enterprise.

1. Identity Credentials: The Move to Smart Cards

Identity cards and badges have evolved from printed tokens to secure documents that incorporate machine-readable technology. Legacy credentials asserted a privilege and, to bind the credential to the holder, identity information may have been printed or even written on the card or badge surface.

To validate credentials rapidly, issuers must provide an infrastructure that can verify the current standing of the credential holder. Machine-readable credentials became the norm to facilitate rapid verification. As a result, credentials that are read visually fill a different role than credentials that are read electronically. A printed badge can assert both identity and a privilege. A credential that is read by an electronic system asserts identity only. The system determines the privileges authorized for the credential holder.

An increasing number of government organizations and corporate enterprises are now using smart cards as their employee identity credentials. A smart card-based identity credential stores the employee's identity information securely, so that the information can be accessed for fast, automated identity verification and used to determine the employee's authorization to access corporate resources.

Using smart cards enables the issuer to assert that the receiving party can place a high degree of trust in the information on the card. This information can include personal information (for example, a biometric or signed digital photo) or privileges (such as an electronic purse or digital certificates that allow computer logon). Additionally, because a smart card has computing power, it can require the user to provide authentication in the form of a PIN or, in some cases, a biometric before the card communicates with the interrogating system. And finally, a smart card can use cryptographic methods to establish a secure communication channel between the reader and the card (for example, using a challenge and response to require the interrogating system to authenticate itself to the smart card prior to any communication taking place).

In any secure identity credentialing system, the issuance process is as important as the credential's security. The issuance process needs to bind the person to background identity checks and testing that take place before the credential is issued. After the credential is issued, the credential life cycle management process needs to incorporate authentication, revocation, and reissuance processes. Relying parties will only trust a credential if they believe that the issuance and life cycle management processes are secure.

2. U.S. Government Smart Cards: CAC and PIV

The U.S. Federal Government has been issuing smart card-based employee identity credentials for some time.

One of the earliest and most influential government deployments is the Department of Defense (DoD) Common Access Card (CAC), which was designed to be the standard DoD ID card and the primary card enabling both physical access to buildings and other controlled spaces and logical access to DoD computer networks and systems. Since October 2000, when deployment began, DoD has issued over 12 million CACs and implemented the issuance infrastructure worldwide. Support for the CAC can be found on Windows®, Apple®, and Linux® systems, and it can even be used with portable mobile devices (such as the Blackberry® smartphone). DoD has reported compelling results in reducing fraud as a result of using the CAC to log onto DoD networks and sign e-mail messages—a 46 percent decrease in DoD network intrusions and 30 percent decrease in socially engineered e-mail attacks[1].

The Federal Government's move to smart cards accelerated with the issuance of Homeland Security Presidential Directive 12 (HSPD-12) on August 27, 2004. HSPD-12 mandates the need "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification." HSPD-12 specifically calls for the use of a common identification credential for "gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."

As a result of this directive, the National Institute of Standards and Technology (NIST) published FIPS 201. FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for a government employee and contractor ID card—the PIV card. The FIPS 201 PIV card is a dual-interface smart card that is now being issued to all Federal employees and contractors.

A growing number of approved vendors of logical and physical access systems and applications have developed products built on FIPS 201 and industry standards for smart cards. FIPS 201 has attracted international attention and is under consideration for government, public safety, and critical infrastructure personnel in other countries. Within the next five years, 12 million[2] PIV cards will be used in the Federal Government alone, driving a significant expansion of FIPS 201 infrastructure and applications.

3. Logical and Physical Security Convergence

While the FIPS 201 standard provides Federal agencies with a blueprint for designing and implementing a comprehensive smart card credentialing program, it will also have a significant impact on programs in the private sector. The signing of HSPD-12 and the subsequent creation of FIPS 201 has been termed a "landmark event for the industry."

> For the first time, a formal standard exists that will allow agencies to purchase biometric and credentialing solutions with the assurance of interoperability and mutual levels of trust. With solid vetting requirements and rigid smart card and biometric interoperability standards, the ID solutions industry is rapidly moving to support it. Other federal ID programs like [the Transportation Worker Identification Credential] TWIC, Registered

[1] "DoD Implementation of Homeland Security Presidential Directive-12," Inspector General, U.S. Department of Defense, Report No. D-2008-104, June 23, 2008, p. 38 (http://www.dodig.osd.mil/Audit/reports/fy08/08-104.pdf)

[2] Figure provided by the General Services Administration.

> Traveler and the First Responder [Authentication] Card initiative have pledged to follow the same technical standards, allowing them to be more rapidly and affordably deployed.[3]

Organizations are pointing to the standard as a means of achieving a more holistic approach to security, incorporating personnel security (vetting, background checks, security training and awareness), logical security (network and application access), physical security (facility access, including video analytics), and incident monitoring and response. Although the current state of enterprise security may arguably be the best ever, enterprises still have a long way to go in terms of recognizing and breaking down various security "stovepipes" that result in disjointed and less-than-efficient security implementations.

Security convergence is a real and growing concept in the commercial world. Enterprises such as Sun, Boeing, Pfizer, Unisys, Lockheed Martin, Northrop Grumman and others are implementing smart card-based badges that provide employee access to both physical and logical resources. Government identity programs internationally are providing smart cards that securely support multiple applications from different issuers.[4] Vendors are building capabilities into systems so that physical access control systems can communicate with enterprise identity management systems and provide consolidated access control.[5]

Consolidating access control will enable corporations to realize some of the benefits that government agencies are beginning to enjoy. Centralizing operations that are often performed locally, such as personnel screening and vetting, can improve overall IT security and physical security. In addition, removing redundant stovepipe functions across an enterprise reduces costs.

4. Best Practices for Identifying Employees

One of the most important benefits of using a FIPS 201 model in the enterprise is the strong assurance that the identity associated with a credential belongs to the correct individual. Special care needs to be taken early in the process so that the identity and associated credential can be trusted across logical and physical access control applications and across locations.

FIPS 201 and the personal identity verification process identify a number of required steps and individuals and describes individual roles in the process.

- **Sponsorship**. A sponsor's duty is to vouch for an applicant's need for an enterprise credential and authorize applicant enrollment. The sponsor may also authorize the cost incurred by the credentialing process.
- **Enrollment**. The enrollment process is designed to verify the identity of an applicant and collect information from the applicant. Applicants must bring two forms of identification and are fingerprinted and photographed at enrollment. The information collected is used to perform suitability checks and create the credential.
- **Adjudication**. Trusted adjudicators determine whether an applicant should receive a credential based on the results of the suitability check. Identity vetting procedures (e.g., National Agency Check with Inquiries, or NAC-I, education, employment, credit history, and verification of claimed skills) are part of the adjudication process, with disqualifiers defined as part of vetting procedures. Successfully passing adjudication triggers credential production. The level of adjudication varies from organization to organization, depending on the level of security/access required. Adjudication can be structured so that individuals who need access to something like a network operations center or security operations center are subjected to more extensive adjudication.

[3] "The Rapidly Emerging Identity Solutions Industry," Stanford Group Company, July 20, 2006.
[4] See Appendix A for an overview of the Malaysia MyKad identity initiative.
[5] See Appendix B for an example use case and approach for consolidating physical and logical access systems.

- **Credential Production**. Credentials can be personalized in a centralized facility or at local issuing stations. Relevant information is printed according to the standards, security features are added, and the electronic smart card chip is encoded with personal data.
- **Issuance and Activation**. When an applicant arrives to pick up the personalized credential, the issuer verifies the applicant's identity by reverifying the identity documents presented at enrollment and matching the applicant's fingerprint to the one used to enroll. The credential is then "unlocked," digital certificates and a PIN are loaded onto the chip, and the credential is released to the applicant for use.
- **Credential Use**. Activated credentials can be used to validate identity electronically and access secure physical locations and computer networks.

All of these process steps must be supported not only by technology but also by policies and procedures. It is only by the consistent execution and enforcement of policies and procedures that the overall integrity of the system can be ensured. FIPS 201 provides a best-practice framework for the entire identity proofing and issuance process that can be used by enterprises implementing robust employee identity management systems.

5. Enterprise Use of FIPS 201 Technologies

Enterprises have the opportunity to leverage the work that the Federal Government has done in FIPS 201 to define identity vetting and verification processes and specify conforming identity credential technology. While only Federal agencies can issue "official" PIV cards, enterprises can follow FIPS 201 processes, use FIPS 201-defined technologies, and implement credentials that are *PIV interoperable* or *PIV compatible*, as appropriate.

A PIV interoperable credential is a credential that meets the FIPS 201 technical standards (and can therefore work with PIV infrastructure elements, such as card readers) and also follows the FIPS 201 process for issuing credentials. Following the FIPS 201 process for credential issuance allows all Federal relying parties to trust the card, across organizations. This trust is established by a common enrollment, registration, and issuance process and a strong authentication credential that leverages a cross-certified and federated public key infrastructure. A PIV interoperable credential would be of great value to enterprises that do business with the government and have a requirement to issue interoperable identity credentials. In addition, related organizations within an industry could decide to follow common FIPS 201 processes to establish a basis for trusting identity credentials across organizations.

A PIV compatible credential is a credential that meets the FIPS 201 technical specifications but does not follow the FIPS 201 process for credential issuance. Federal relying parties cannot automatically trust the card. Enterprises issuing compatible credentials can benefit by being able to use the growing range of products on the FIPS-201 Approved Products List[6]. Cards, readers, software, and other products can be purchased from a variety of vendors, be connected, and function as a system.

Enterprises can choose to implement interoperable or compatible credentials. FIPS 201 provides a defined framework and technical specifications for enterprises to follow for both. By basing identity credentialing efforts on FIPS 201, enterprises can:

- Follow a proven process for employee identity vetting
- Implement an identity vetting process that provides the basis for trusting identities across organizations or with Federal agencies
- Implement an identity credentialing solution that has the potential to be interoperable and compatible across organizations or with Federal agencies
- Acquire proven products and services that meet FIPS 201 technical specifications from multiple vendors

[6] The FIPS 201 Approved Products List is available at http://www.idmanagement.gov.

6. Strengths of FIPS 201 for Enterprise Identity Credentialing Programs

The FIPS 201 standard delivers the following benefits to both government organizations and commercial enterprises:

- Specifies a "useful" and "secure" identity card that supports a wide range of use cases
- Enables card support across a wide range of PCs, servers, and mobile devices
- Defines processes and technical specifications that enable interoperability across organizations
- Fosters competition to reduce prices

The FIPS 201 PIV card offers the following advantages over other smart card-based approaches for enterprises:

- It is supported by a wide range of manufacturers and integrators.
- It does not compel an organization to use a single vendor for key components.
- It provides flexible authentication, signature, and encryption functionality.
- It is well positioned to take advantage of emerging technologies, such as biometrics.
- As a standard that will be used by Federal agencies to issue credentials to millions of U.S. Federal employees and contractors, it has the advantage of scale.
- It provides the framework to support interoperable identity credentials across organizations.

Because of these factors, implementing a FIPS 201 PIV-card-based approach to identity credentials can be extremely beneficial to organizations outside of the U.S. Federal government. An organization using the FIPS 201 model and standard can take advantage of a high level of functionality at economical volume prices. The identity technology has been thoroughly scrutinized and is trusted at the highest levels. And the credentialing process is flexible and has been thoroughly vetted to represent best practice.

While this approach sounds very compelling, there is a drawback. The FIPS 201 standard and specifications were designed strictly for credentialing U.S. Federal government employees and contractors, not for issuing general purpose credentials worldwide. Certain parts of the FIPS 201 PIV card specification are therefore U.S. government-specific and must be tailored for use in a commercial or non-government environment. Some parts, like the requirement for NAC-I vetting, are procedural and can be replaced with a different process in a commercial implementation. Others, like the numbering for the cardholder unique identifier (CHUID), are government-specific and not defined for private organizations.

Fortunately, these issues are currently under active consideration by NIST and the General Services Administration, and guidance on using FIPS 201 PIV technologies and standards for private enterprise implementations is expected by the end of 2008. In addition, the American National Standards Institute B10.12 work group is defining a new standard, the Generic ID Card Specifications (GICS), which is an open specification for commercial identity credentials. GICS is a superset of the FIPS 201 command set for the PIV card; it allows extensions for additional data elements and applications that organizations may want to support in employee credentialing implementations.

7. Conclusion

The standardization of identity credentialing processes and approaches is a major step forward for identity management in both enterprises and government organizations. Standardization fosters interoperability. Standardization simplifies implementation by driving the industry to develop products, applications, processes, and practices that meet the standard and are interoperable. Standardization provides enterprises with a greater variety of products at a lower cost.

The FIPS 201 standard has established a foundation for both government and commercial identity credentialing programs. By using FIPS 201 as the basis for an employee identity credentialing system, enterprises can move toward standardized processes and technologies that enable interoperability and are supported by commercial off-the-shelf products from multiple vendors.

So what should an enterprise do next? A good first step is to get educated on FIPS 201—particularly the FIPS 201 identity verification processes and technologies—to see how it can be used to meet requirements for high assurance identity verification, secure interoperable identity credentials, and authentication for physical and logical access. By using FIPS 201, enterprises can take advantage of the investment being made by the U.S. government and industry to implement standards-based identity credentialing programs.

8. Publication Acknowledgements

This report was developed by the Smart Card Alliance Identity Council and Physical Access Council to provide an overview of FIPS 201 for corporate enterprise executives and to describe the benefits of using FIPS 201 as the foundation for enterprise identity management programs. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Identity and Physical Access Council members for their contributions to this report, including: EDS; Fargo Electronics; Hirsch Electronics; IDmachines, LLC; IDTP; Lockheed Martin; Northrop Grumman Corporation; PricewaterhouseCoopers; SAIC; SI International; Thales e-Security; Tyco International; Unisys; U.S. Department of Defense.

Special thanks go to the following Identity and Physical Access Council members who participated in the white paper development:

- Bray Becker, Lockheed Martin
- Sal D'Agostino, IDmachines
- Paul Evans, EDS
- Mohammed Hamza, SI International
- Steve Howard, Thales e-Security
- Gary Klinefelter, Fargo Electronics
- Gilles Lisimaque, IDTP
- Cathy Medich, Smart Card Alliance
- Phil Myers, Unisys
- Dwayne Pfeiffer, Northrop Grumman
- Roger Roehr, Tyco
- Lars Suneborn, Hirsch Electronics
- Robert Van Spyk, U.S. Dept. of Defense
- Robert Wilberger, PricewaterhouseCoopers
- Chris Williams, SAIC

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance Physical Access Council

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

Identity and Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Additional information about the Identity and Physical Access Councils and about the use of smart cards for secure identity and access applications can be found at http://www.smartcardalliance.org.

Trademark Notices

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

Apple® is a registered trademark of Apple, Inc., registered in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Blackberry® is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

9. Appendix A: Security Convergence in Identity Programs

Security convergence is a real and growing concept of operations in the commercial world and in some foreign countries. For example, the Malaysian government has issued more than 21 million national identity cards to its citizens as part of the MyKad program. These multi-application smart cards not only verify identity at border crossings, they also serve as driver's licenses and can be used to pay for highway tolls, parking, and public transportation. Malaysian citizens can also use the card for ATM transactions. The card contains personal data, including Malaysia’s equivalent of the U.S. Social Security number, banking/tax information, and confidential health care information for use by authorities during emergency situations. The successful implementation of these cards is an impressive illustration of the ability of government agencies and private sector organizations to cross personal and technology security barriers and share information while still ensuring the privacy of the information and of individual identities.

10 Appendix B: Example Use Case – Physical and Logical Access Consolidation

The goal for the consolidated system in this use case is to enhance physical and logical security by using the local physical access control system (PACS) to enable and disable user accounts that are managed by the Active Directory (AD) directory service. The PACS is used to send an enterprise-unique cardholder identification number (in FIPS 201 terminology, the cardholder unique identifier (CHUID) or global unique identifier (GUID)) to the AD server.

The following describes how the consolidated system would manage user access;

> Bob, an employee of ACME Corporation, arrives at work. Bob presents his ID card to a PACS reader to enter his building. As the PACS completes the validation and authorization check of Bob's credential and grants access, it sends an enterprise-unique identification number to the AD server. At the same time, the AD server disables an external account that Bob uses to log on from his laptop when traveling or working from home.
>
> When Bob arrives at his office and uses the same card to log onto his desktop computer, the AD account is already enabled, and Bob begins his work day. If Bob is authorized to use computers in other areas, he simply takes his card with him when he leaves his office to work at those computers. Bob uses the same card as his normal access control credential when he needs to move between controlled areas. This prevents Bob from leaving the office with the card in his computer and remaining logged on while away.
>
> At the end of the day, Bob exits his area and uses the card at a PACS reader designated as an exit reader. At this point, the PACS sends the same unique ID number to the AD server, which disables the internal account and enables the external account.

This use case connects functions inherent in AD and functions developed by leading PACS manufacturers. PACS components are becoming increasingly IT-centric, and interoperable applications such as those described in this use case are becoming a reality.

Implementing the system described in the use case requires three basic subsystem functions:

- A server running the AD directory service for account and provisioning management
- A PACS for credential and user location updates
- A management console to control and manage the connected subsystems

Figure 1 illustrates one possible system approach.

As shown in this use case, implementing a consolidated system requires a minimum of basic components. While implementation details differ from one enterprise to another, the basic conceptual approach would be the same.

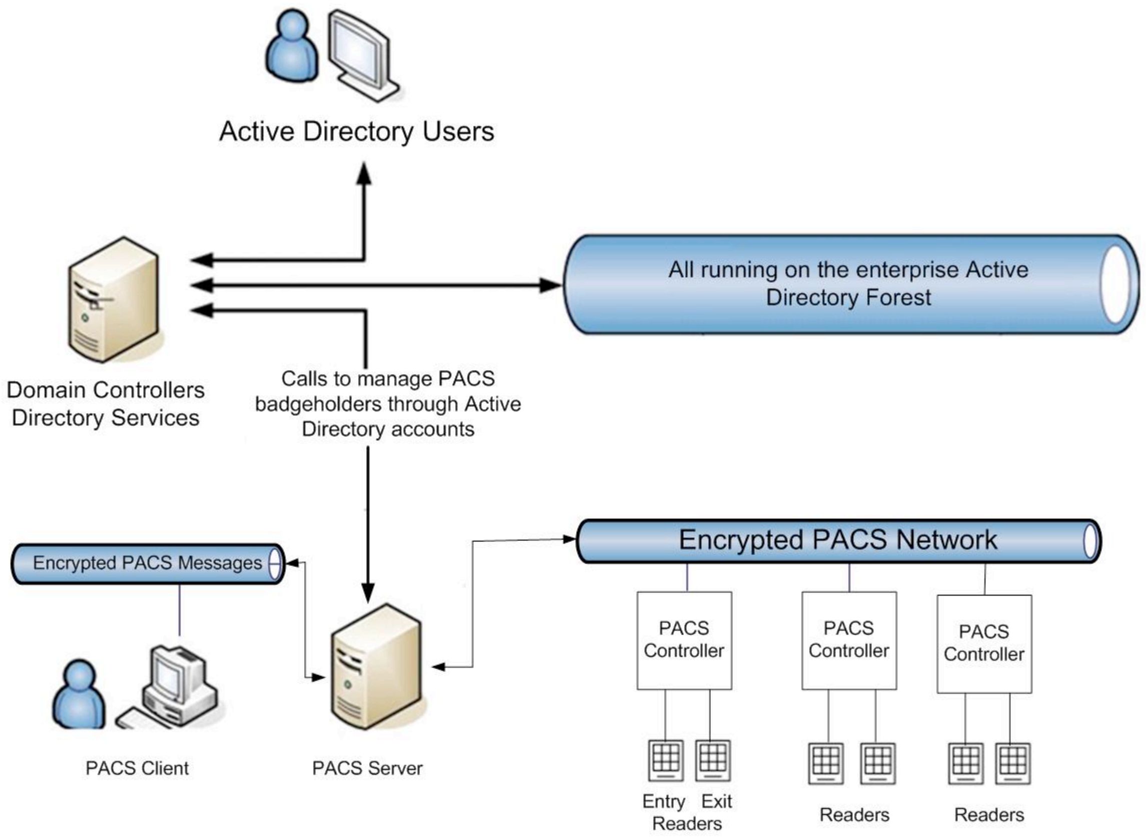

Figure 1. Conceptual Foundation for Consolidating Physical and Logical Access