



WHITE PAPER

---

# The Business Benefit of HSPD-12



Where it all comes together.™



**CONTENTS**

+ Overview	3
History and Purpose	3
HSPD-12 and FIPS-201	4
Personal Identity Verification (PIV)	5
FIPS 201 and the Shared Service Provider (SSP) Program	6
+ Planning for and Deploying HSPD-12 Solutions	7
Control Objectives	7
Interoperability and Access Control Benefits	8
Authentication and Federated Identity Strategies	8
+ About the Author	9



# The Business Benefit of HSPD-12

## + Overview

In August 2004, the President of the United States signed an executive policy directive intended to unify the government's identification badge systems through a new standard. The debate over the development of the standard uncovered a number of technological and process hurdles that must be cleared before true interoperability can be achieved across all government organizations. The directive and the resulting standard both place significant new responsibilities on federal managers up to and including the heads of departments and agencies. The responsibilities are consistent with the desire of Congress and the administration to invest top federal managers with accountability for crucial aspects of security risk management. This white paper outlines those responsibilities, describes their relevance to the agency mission and strategic IT goals, and analyzes issues facing federal managers when implementing HSPD-12.

### History and Purpose

Homeland Security Presidential Directive/HSPD-12 was issued on August 27, 2004 by President George W. Bush. Its purpose is to eliminate "wide variations in the quality and security of forms of identification" used to access secure federal facilities and information resources. It reiterates "the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." To further these aims, HSPD-12 (the Directive) calls for establishing "a mandatory, Government-wide standard for secure and reliable forms of identification."

HSPD-12 is not the first initiative pertaining to electronic credentials for federal employees. In 1996, President Bill Clinton included in the Budget for Fiscal Year 1998 the administration's desire "to adopt 'smart card' technology so that, ultimately, every employee will be able to use one card for a wide range of purposes, including travel, small purchases, and building access." The Department of Defense Common Access Card (CAC) program has over 4 million cards in use today. Smart card vendors and information technology experts have been promoting the virtues of smart cards since at least 1985. However, HSPD-12 does not mention smart cards or any other technology other than to require identification that "can be rapidly authenticated electronically."

What HSPD-12 does emphasize are the issues of quality and security in federal identification. The goals for the new identification standard are concise. The standard must specify identification that (quote):

- a) is issued based on sound criteria for verifying an individual employee's identity;
- b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- c) can be rapidly authenticated electronically; and
- d) is issued only by providers whose reliability has been established by an official accreditation process.

The focus in HSPD-12 on the reliability, trustworthiness, and verification of the processes that form the foundation of an identification system can trace some of its origins to work performed by government organizations such as the Federal Identity Credentialing Committee<sup>1</sup> (FICC). The FICC, through its efforts in 2002-2003 to mandate a uniform identification system for the Federal Government, learned that it had to first provide a basis for agencies to trust the quality of a credential issued by another agency.

It is fair to say the primary purpose of HSPD-12 is not to compel agencies to buy a smart card for every employee and contractor. Rather, it is to direct the attention of federal government managers to the processes they use to issue and maintain their identification credentials, the methods they use to validate and attest to those processes, and the management of risk and quality throughout the life-cycle of the credential. The reason for this assessment is simple. Without direct management involvement in these process initiatives, even the most technologically advanced smart card system might fail to win widespread acceptance and in so doing will fail to achieve the President's objective of enhancing security and efficiency. This is consistent with major information technology and security policy initiatives for federal agencies including GISRA<sup>2</sup>, FISMA<sup>3</sup>, OMB<sup>4</sup> Circular A-130, and various OMB technology guidance memoranda, all of which place major emphasis on agency managers becoming more effective at managing risk, rather than relying mainly on technology adoption as the solution to information processing and security needs.

#### HSPD-12 and FIPS-201

HSPD-12 directs the Secretary of Commerce to promulgate a standard for secure and reliable forms of identification to achieve the aims of the Directive. The National Institute of Standards and Technology (NIST) is the Bureau within the Department of Commerce that is charged by Congress with developing standards for information technology and security. On February 25, 2005, two days before the date specified in HSPD-12, NIST published Federal Information Processing Standard (FIPS) Publication 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (the Standard). In keeping with the focus of HSPD-12 on personal identification, and with the feedback from agencies on FICC's earlier credential efforts, FIPS 201 makes two fundamental security policy decisions at the outset:

- a) to separate the identification and authentication process from the access control decisions
- b) not to impose any access control policies or requirements on agencies.

This means agencies retain complete control over the granting of access to any card holder who requests access to agency facilities, computers, networks, or services, regardless of the level of access specified on the card. This is an important first step in overcoming barriers to the acceptance of credentials by other agencies. Early drafts of FIPS 201 also used the term "integrated circuit card" instead of smart card, perhaps to avoid association with many abandoned smart card initiatives over the last two decades. Regarding smart cards, FIPS 201 makes another significant policy and technical decision:

- c) not to adopt the Government Smart Card Interoperability Standard (GSC-IS 2.1) for smart card functionality or interoperability.

<sup>1</sup> <http://www.cio.gov/ficc/>

<sup>2</sup> The Government Information Security Reform Act of 2000 (Public Law 106-398, Title X, Subtitle G expired 2002)

<sup>3</sup> The Federal Information Security Management Act of 2002 (Public Law 107-347, Title III)

<sup>4</sup> The Office of Management and Budget, Executive Office of the President. <http://www.whitehouse.gov/omb/>

This decision carries a high price in terms of deployment delays while smart card hardware and software vendors retool for a new standard. Vendors who made significant investments in the GSC-IS that have not yet resulted in profitable sales were taken aback by the switch. In addition, the detailed standards regarding smart card functionality, cryptographic methods and algorithms, and format of biometric data continued to unfold in the months following the publication of FIPS 201. While this has been of great concern to some implementers, VeriSign believes the availability of smart card technology will not be an obstacle to a successful and on-schedule HSPD-12 deployment.

Regarding major milestones for the HSPD-12 deployment schedule, two significant policy directions are taken in FIPS 201:

- d) to segregate all identity proofing, registration, issuance, maintenance, and privacy standards and control objectives from all technology and card specifications; and
- e) to require implementation by October, 2005 only of the processes that satisfy the identity proofing, registration, issuance, maintenance, and privacy standards and control objectives.

Certainly, these policy decisions allow more time (up to an extra year under current OMB guidelines) for the technology standards to be debated and finalized and for vendors to develop products that meet the standards. More importantly perhaps, the decisions allow time for departments and agencies to focus on the processes that support identity proofing, registration, card issuance, maintenance, and privacy. Managers need time to understand and manage the risks inherent in those processes so they can ultimately assure the quality and security of their personal identity verification system. Once agency standards are in place for quality and security of these processes, business and technical managers will be in an excellent position to evaluate and select technologies to implement those standards.

#### Personal Identity Verification (PIV)

The set of identity proofing, issuance and maintenance processes required by October 2005 is referred to in FIPS 201 as PIV-I. The technical and interoperability standards that follow are called PIV-II. FIPS 201 includes another reason to focus attention on getting the PIV-I processes right. The smart card and other IT systems supporting HSPD-12 must be accredited like all other federal IT systems by the agency authorizing official. This role is usually performed by the agency Chief Information Officer (CIO) or a designated senior management official. However, for the PIV-I processes, an additional validation is required:

- f) The identity proofing, registration, issuance and maintenance processes must be accredited by the department or agency<sup>5</sup> as satisfying the requirements of the Standard and approved in writing by the head of the federal department or agency.

Written approval by the agency head attesting to the trustworthiness of an Agency's PIV system will add immense value later when agency systems begin to interconnect and decisions are made about granting access based on credentials from other agencies.

5 The requirement for accreditation by the agency Inspector General was withdrawn on February 29, 2005.

Accrediting a process, or a set of processes, is unlike accrediting an IT system comprised of hardware and software. A new methodology is required. NIST provides this methodology in Special Publication (SP) 800-79, “Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.” The Standard and SP 800-79 call for the development and use of continuous auditing or monitoring practices to protect the security and privacy of PIV data, processes, and systems. The relationship of PIV-I components is illustrated in Figure 1.

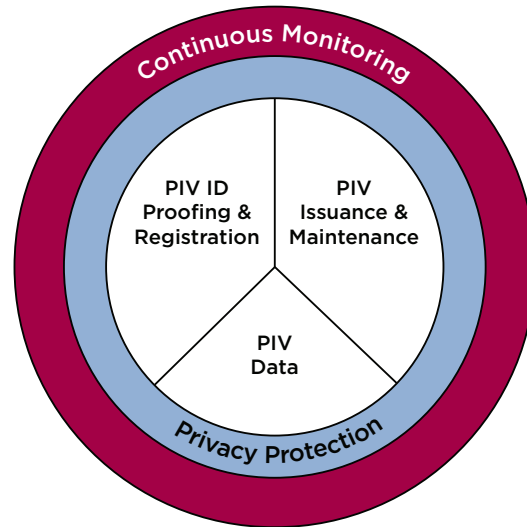


Figure 1: PIV-I Components

One federal standard adopted in FIPS 201 with only minor modifications is the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FPKI Common Policy). This is the Certificate Policy for Public Key Infrastructures (PKI) that issue digital certificates to federal employees and contractors. Authored by Federal PKI policy makers, this Certificate Policy (CP) includes requirements for applicant identity proofing, registration, secure certificate issuance, and life-cycle maintenance. Digital certificates are commonly used to authenticate the bearer to an application, as well as for data and message integrity and encryption. FIPS 201 specifies digital certificates that comply with the FPKI Common Policy for a variety of authentication purposes.

The FIPS 201 identity proofing and credential issuance standards closely follow Federal PKI policies, which in turn were derived from industry standard PKI policies, practices, and specifications<sup>6</sup> that were developed and authored in large part by VeriSign.

#### FIPS 201 and the Shared Service Provider (SSP) Program

Recognizing the PKI industry’s experience in operating, maintaining, and monitoring large PKI systems, the government created the Shared Service Provider (SSP) program to provide digital certificate issuance to agencies under the FPKI Common Policy. VeriSign was the first commercial PKI provider to be certified as an SSP. FIPS 201 recognizes digital certificates from only two sources, an SSP or an agency PKI that is cross-certified with the Federal Bridge Certification Authority (FBCA). After December 31, 2005, the FBCA will no longer accept applications for cross-certification from federal agency PKIs.

<sup>6</sup> Internet-related specifications are documented as Internet Engineering Task Force (IETF) Requests for Comments (RFC).

## + Planning for and Deploying HSPD-12 Solutions

The previous section of this paper outlined why the initial emphasis of HSPD-12 is on identity proofing, registration, credential issuance, maintenance, and privacy, and on meeting and monitoring the control objectives associated with these tasks. This section describes each of these processes in some detail, and explains why partnering with VeriSign is the ideal choice for achieving HSPD-12 compliance. If you are an agency manager, you can readily determine the importance of this stage of HSPD-12 solution development by using the newspaper test. In other words, would you like to read in the newspaper that your agency had allowed a valid PIV credential to be issued to a suspected terrorist? On the other hand, if your agency's smart card failed to integrate properly with a legacy mainframe application, would it even make the newspaper?

### Control Objectives

The control objectives given in HSPD-12 and expanded in FIPS 201 are critical to meeting the security, efficiency, fraud prevention, and privacy protection goals of HSPD-12 and must be maintained throughout the life-cycle of PIV-I and PIV-II deployments. The control objectives can be summarized as follows:

**Use of Roles in Registration and Issuance** - The processes of authorizing an applicant, registering the data, and issuing the credential must be performed by persons occupying different roles. This provides additional quality checks during the credential issuance process. This separation of duties helps to ensure that no one person acting alone can issue a credential to an unauthorized person.

**Use of Original Identity Source Documents** - Identity documents from the I-9<sup>7</sup> list, that have established, verifiable methods of confirming their validity, are required. Proper custody throughout the credentialing process of the documents or copies presented for identity proofing is needed to ensure accurate credential issuance and to maintain the privacy of personal information.

**Use of Background Investigations** - Credentialing officials must have the means to verify that the right amount of investigation has been carried out on the right individual before a credential is issued. The agency, the Office of Personnel Management, and OMB must determine the minimum level of investigation that must be performed before a credential is issued. This is particularly important when the credential is issued pending the completion of a full required background investigation.

**Use of Credentials Resistant to Tampering and Forgery** - The use of smart cards as PIV credentials allows for extensive use of cryptography, especially PKI cryptography, to prevent fraudulent uses of the card. All of the data on the card, and most card operations, can be mathematically verified using PKI.

**Reliance on Rapid Credential Revocation** - Agencies must have the ability to swiftly and effectively revoke a credential issued in error or when there has been a change of condition. That means rapid electronic authentication must include verification of the credential and its current revocation status.

**Certification and Accreditation** - Formal certification and accreditation (C&A) is used to test and verify the identity proofing and registration processes, all IT systems used to support PIV, and even to test the reliability of PIV card issuers. A thorough certification test and report gives agency managers a clear picture of the risks present in the processes and systems and a plan for managing those risks.

<sup>7</sup> Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.

VeriSign is the world leader in PKI. VeriSign consultants have extensive experience developing and testing identity proofing and registration systems to ensure separation of duties and preservation of audit trail data. The VeriSign SSP service for digital certificates includes global Online Certificate Status Protocol (OCSP) access for 24 x 7 real-time validity checking. VeriSign consultants have broad experience performing C&A on IT systems throughout the government. VeriSign's experience validating PKI implementations puts VeriSign at the forefront of the industry in its ability to execute for the government on the assessment and certification of PIV-I processes.

#### Interoperability and Access Control Benefits

The goal of HSPD-12 to improve efficiency by using interoperable credentials across the government calls for new ways of thinking about access control policies for facilities and systems. The promise is increased productivity of workers who can access information resources from work locations other than their normal duty station. However, achieving this goal requires overcoming barriers of trust, beginning with the credential issuance process. In planning to meet PIV-I standards, an agency program manager might ask, "How would I want another agency to prove the quality and security of their credential system to me?"

The answer will likely include publicly available security policies, privacy policies, certification reports, independent audit reports, Inspector General reviews, and agency management statements. Making security policies publicly available is not just a requirement of FISMA,<sup>8</sup> it is also a requirement for privacy policies and Federal PKI Certificate Policies, and an effective way to promote trust among current and potential users.

Early in the HSPD-12 planning process is a good time to do a complete review of agency authentication and access control policies, both physical and logical, to ensure readiness for HSPD-12 requirements. VeriSign can assist in creating or rewriting policies with the view in mind that they will be publicly disclosed upon completion.

#### Authentication and Federated Identity Strategies

VeriSign also understands there are opportunities to leverage HSPD-12 efforts to gain significant advantages in current and future IT operations. FIPS 201 places new demands on identity management and drives integration with PKI. Preparing for these steps provides a good opportunity to review and upgrade the agency authentication strategy. This strategy defines the technical and security requirements for agency authentication services by assurance level from highest to lowest. It also defines where given technologies will be supported, including the provision of reader equipment if necessary. As facility and physical access authentication is driven more to integrate with Internet technologies such as OCSP and LDAP<sup>9</sup>, the physical access applications must be included in the authentication strategy as well.

<sup>8</sup> FISMA Section 3544(e)

<sup>9</sup> Lightweight Directory Access Protocol (v3), RFC 2251.

In a related program, the President's E-Government E-Authentication Initiative calls for a standards-based authentication architecture to help increase the number of government services that can be delivered electronically while driving down the cost of implementing each new service. The additional goal of reducing the number of electronic credentials citizens and businesses need to access government services parallels the goal of the single PIV credential for all federal employees and contractors. Agency experience with implementing one will reinforce the other. This is especially true for the PKI implementations within PIV and E-Authentication systems.

In order to transition "as promptly as possible" to more secure authentication to federally controlled facilities and information systems it is necessary to identify and prioritize the systems in question. VeriSign consultants are experienced at identifying and categorizing systems and transactions, performing e-authentication risk assessments, and updating agency policies to comply with new regulations. VeriSign consultants can help get the most out of required investments in PKI by developing migration paths for critical agency applications that can save money by using the existing PKI for strong authentication.

As agency managers look ahead to the long-term benefits of HSPD-12 as well as the near-term demands of the E-Authentication Initiative, the concept of federated identity arises. Federated identity is the sharing of identification data with external organizations for the purpose of accessing facilities or information. A federated identity strategy defines how an organization will collect, process, store, distribute, and protect all of the data used in a federated identity system. Development of a federated identity strategy and system, like E-Authentication and PIV credentials, is closely linked to the agency's overall identity management strategy. Decisions made for PIV and E-Authentication compliance will affect the choices available for federated identity services and are best made in concert. Again, seeking good advice from a qualified and committed partner will go a long way toward developing effective strategies that build on each other.

#### + About the Author

David Sulser, CISSP, CISM

David Sulser is a Principal Consultant with VeriSign's Public Sector Consulting Group. He has 20 years experience working with technology, public policy, and legal issues in the telecommunications and information technology industries. Mr. Sulser has been instrumental in developing policies, procedures and technical frameworks that have brought federal customers to the forefront of regulatory compliance while raising the performance level and effectiveness of agency security operations. He can be reached at [dsulser@verisign.com](mailto:dsulser@verisign.com).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. All other trademarks are the properties of their respective owners.

00021428 11-08-05