



## DATA SHEET

# VeriSign® HSPD-12 Solutions

## KEY FEATURES

### *Simplified Management*

A common and easy-to-use Web-based interface allows organizations to securely enroll card holders and manage the entire lifecycle of cards and digital certificates without completing an integration project. Typically an organization would need to complete and support an integration effort to enable seamless communication between its PKI and CMS solutions.

### *Multiple Issuing Models*

Various deployment models are supported: bureau for large volume deployments, batch for groups of users, individual for face-to-face service, and self-service.

### *Numerous Roles and Card Policies*

Access to the system is controlled through definable roles and an unlimited number of card policies.

### *Supports Contact and Contactless Cards*

Manage proprietary cryptographic cards, Java cards, iClass and MIFARE interfaces.

### *Range of Technology Vendors*

Support for multiple vendors of FIPS-201 compliant Smart Cards, IDMS, Middleware, Biometric Capture Devices, Validation Solutions, and Physical Access Systems.

Homeland Security Presidential Directive 12 (HSPD-12) mandates that all US Federal Government employees and contractors be issued a standard and reliable form of identification. HSPD-12 called for a new standard for issuing, maintaining, and electronically validating personal identity cards. Federal Information Processing Standard 201 (FIPS 201) was developed by the National Institute of Standards and Technology (NIST). FIPS 201 defines acceptable standards both for the type and appearance of credentials and for the processes of registration, identity-proofing and issuance of Personal Identity Verification (PIV) cards for government employees and contractors. FIPS 201 provides a phased approach to meeting the new process, system integration, and government-wide interoperability standards.

The path to full HSPD-12 compliance is different for each agency, due to existing organizational structures and embedded technologies. Two major components of any organization's plan for HSPD-12 compliance are the implementation of Shared Service Provider (SSP) Public Key Infrastructure (PKI) and a card management system (CMS). Other components of a complete solution will include identity management system redesign, the deployment of issuance stations, and a host of new procedures, training programs, system integration and software development, to name a few.

Through years of experience delivering highly secure credentials to government and industry customers VeriSign's engineering and delivery teams observed the complexity associated with smart card deployments. More specifically, the integration of several technologies that are used to produce a credential is complex. With its understanding of the intricacies of smart card projects VeriSign decided to provide two of the core technologies as one integrated solution, VeriSign SSP PKI and Card Management System. VeriSign's integrated solution removes the need to integrate two of the most important components of a FIPS 201 solution, and as a result significantly reduces the cost to deploy a compliant solution.



Where it all comes together.™

**KEY BENEFITS**

*Reduced Complexity and Ease of Deployment*

VeriSign's solution reduces the complexity of any overall HSPD-12 solution by providing a completely integrated "out of the box" solution to Certificate and Card Management.

*Compliance*

VeriSign has received its certifications for both the Card Management System and SSP PKI. The CMS certification package leveraged the VeriSign SSP PKI, and was uniquely tested with fully compliant certificates.

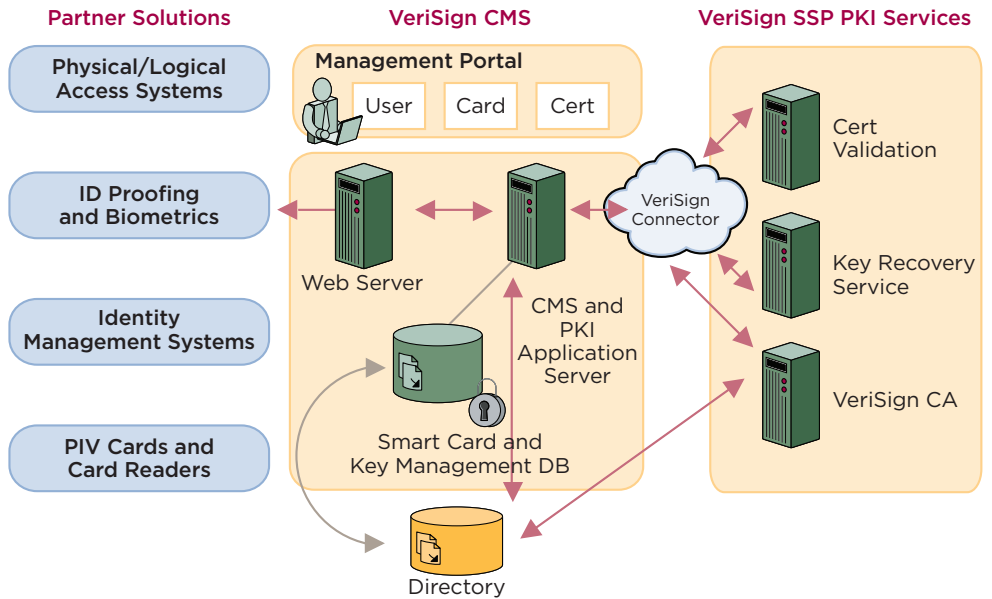
*Ease of Use*

Credential administrators have only one system for issuing, revoking, and managing all users' credentials for both physical and logical access.

*Full Audit Trail and Flexible Reporting*

All system activity is logged into a security audit database. Multiple reports can be defined, produced, viewed and printed using the integrated reporting tool.

VeriSign's Integrated HSPD-12 Solution is depicted below:



More About the VeriSign Solution:

**+ VeriSign® Card Management System for PIV**

The VeriSign® Card Management System is a comprehensive and easy-to-use suite of management tools specifically designed for smart card deployments, supporting a wide choice of smart card types, workflows, and deployment options for securing enterprises and government agencies. It includes a fully featured card management system, addressing the entire smart card credential life cycle, from card and credential issuance to replacement and cancellation, as well as managing smart badging and applets. Together with VeriSign's Two Factor Authentication Services organizations are able to deploy a integrated credential management solution that addresses the complexities of physical and logical access.

**+ VeriSign® Shared Service Provider PKI**

VeriSign was the first commercial vendor certified as a Shared Service Provider (SSP) by the Federal Identity Credentialing Committee (FICC). The VeriSign SSP PKI service fully complies with the requirements of the Federal PKI Common Policy Framework and NIST FIPS-201 and provides the following capabilities:

- Certification Authority (CA)
- Registration Authority (RA)
- Key Management
- Repository
- Archive
- Integrated OCSP Responder Functionality
- Out of the Box Integration With The VeriSign Card Management System (CMS)



The VeriSign SSP PKI services are hosted in VeriSign's highly secured data center in Mountain View, CA with all transactions mirrored over a dedicated secured link to a backup disaster recovery data center in Dulles, VA. VeriSign SSP services will be operated 24x7x365 with availability in excess of 99.9%. All SSP PKI transactions are electronically audited and archived. VeriSign provides all the services necessary to establish and maintain the SSP PKI service including 7x24 level 2 help desk support and all required training for VeriSign, partner or federal agency operations personnel. The VeriSign SSP Certification Authority has been certified and accredited by the GSA and will also undergo an annual external audit (WebTrust) as required by federal policy and the VeriSign SSP Certification Practices Statement (CPS).

### + The VeriSign Difference

Many service providers offer point solutions for HSPD-12 compliance, but few match VeriSign's comprehensive solution suite and expertise. VeriSign helps enable organizations to utilize a single integrated platform for all their authentication needs. VeriSign's HSPD-12 Solutions can reduce the cost of deployment by leveraging an organizations existing infrastructure while moving the complexity of security and scalability to VeriSign. Based on guidelines developed by Initiative for Open Authentication (OATH), the open reference architecture provides a common interface for managing all types of credentials from multiple vendors. VeriSign HSPD-12 Solutions combine exceptional security knowledge and experience, best-of-breed open solutions, and VeriSign's history of stability and trust to deliver security compliance solutions that are both effective and optimize the use of existing in-house resources, technologies, and processes.

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

©2007 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.

01-29-2007