



DATA SHEET



## VeriSign® Shared Service Provider Public Key Infrastructure Service

Homeland Security Presidential Directive 12 (HSPD-12), authorized in August 2004, mandates that all U.S. Federal Government employees and contractors be issued a secure and reliable form of identification. HSPD-12 directs the development of a standard for issuing, maintaining, and electronically validating personal identity credentials. In response, the National Institute of Standards and Technology (NIST) developed Federal Information Processing Standard 201 (FIPS 201), which defines the requirements for complying with HSPD-12. The FIPS 201 standard defines both the technical standards for a Personal Identity Verification (PIV) card, and the processes for registration, identity-proofing, and issuance of PIV cards for US Federal Government employees and contractors.

Although the path to full HSPD-12 compliance is different for each U.S. Federal agency, implementation of two major components are common to any organization's solution for HSPD-12 compliance—a *Shared Service Provider Public Key Infrastructure* (SSP PKI) and a *Card Management System* (CMS).

### + VeriSign SSP PKI Service

With VeriSign SSP PKI Service, U.S. Federal agencies are able to leverage VeriSign's expertise and existing PKI platform that currently provides managed PKI services for thousands of commercial and government customers. Federal agencies benefit from VeriSign's significant investment in its PKI infrastructure while retaining complete control over certificate lifecycle management, including issuance, renewal, and revocation.

#### *Key Differentiators*

- **First-To-Market** – VeriSign was the first vendor certified by the Federal Identity Credentialing Committee (FICC) and the first to receive FIPS 201 certification as a Shared Service Provider. VeriSign SSP PKI Service fully complies with all requirements of the Federal PKI Common Policy.
- **Customizable Environment** – VeriSign SSP PKI Service provides each federal agency with multiple, dedicated Certification Authorities (CAs), which enable the issuance of multiple, custom certificate types. The GSA Managed Service Offering does not offer this level of customization or flexibility.

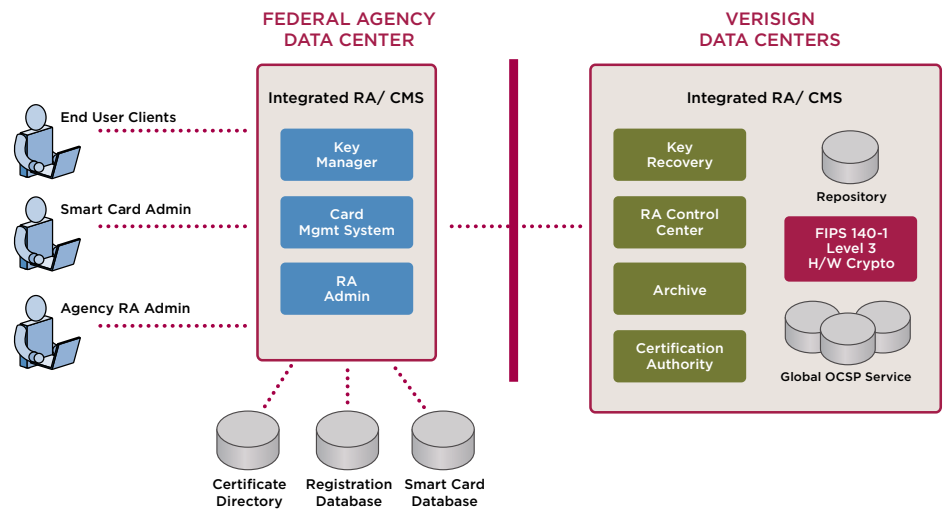


- **Reliable and Available** – VeriSign SSP PKI Service provides the reliability and availability necessary to help meet the mission-critical needs of federal agencies. VeriSign’s military-grade managed PKI platform supports 24x7x365 monitoring, management, archiving, and full disaster recovery.
- **Real-time Certificate Management** – VeriSign SSP PKI Service includes a global, distributed certificate validation service to provide timely certificate status information.

**+ Card Management System Integration**

MyID PIV for VeriSign is a comprehensive identity and card management system that, when combined with VeriSign SSP PKI Service, enables U.S. Federal Government agencies to comply with HSPD-12. MyID PIV for VeriSign provides a single interface for registering, identity proofing, issuing, and maintaining PIV cards in compliance with the FIPS 201 standard. It is integrated with VeriSign SSP PKI Service to enable federal agencies to deploy an integrated credential management solution for issuance of PIV cards that support both physical and logical access.

Figure 1: VeriSign SSP PKI Service for HSPD-12



## + Features & Benefits

<b>Hosted Certification Authority (CA)</b>	VeriSign hosts and operates multiple, dedicated CAs for each federal agency, which include the following: <ul style="list-style-type: none"><li>• FIPS 140 Level 3 hardware security modules for CA key generation and storage.</li><li>• Issuance of four PIV certificate types, plus CMS Signer, Domain Controller, OCSP Responder, and other certificate types as needed by U.S. Federal government agencies.</li><li>• Certificate Revocation List (CRL) issuance at least every 18 hours, per minimum requirements, or more often if desired.</li></ul>
<b>Registration Authority (RA)</b>	VeriSign provides the federal agency with the ability to: <ul style="list-style-type: none"><li>• Remotely authenticate, approve/ reject, and revoke certificate requests from subscribers.</li><li>• Generate reports on certificate activity.</li></ul>
<b>Key Management Service</b>	Includes an integrated key management service with these capabilities: <ul style="list-style-type: none"><li>• Generation and distribution of user-private encryption keys and certificates.</li><li>• Local 3-DES encrypted storage of user-private encryption keys.</li><li>• Two-man control for secure recovery of user-private encryption keys and certificates.</li><li>• Support for leading secure messaging solutions.</li></ul>
<b>Mission-Critical Reliability</b>	Delivers reliability and availability levels that help meet mission-critical needs; including 24x7x365 monitoring, management, archiving, and full disaster recovery.
<b>Card Management System Support</b>	Integration with MyID PIV for VeriSign enables issuance of multiple smart card types, including PIV-interoperable smart cards, and delivers: <ul style="list-style-type: none"><li>• An easy-to-use, Web-based interface that allows secure management of the entire lifecycle of smart cards and digital certificates.</li><li>• Support for various deployment models, including local printing and remote bureau printing for large volume deployments.</li><li>• Access to the system controlled through definable roles and smart card-based authentication.</li></ul>
<b>Archive &amp; Reporting</b>	An Oracle database records signed audit information for all transactions. An integrated reporting tool is also included.
<b>Online Certificate Status Protocol (OCSP) Service</b>	Includes a distributed OCSP validation service to enable timely retrieval of certificate status.
<b>Implementation and Support Services</b>	VeriSign Professional Services alleviate the burden of planning, implementing, and maintaining an in-house PKI support infrastructure. <ul style="list-style-type: none"><li>• Includes 24x7x365 Level 2 help desk support and all required training for federal agency operations personnel.</li></ul>
<b>Annual Security Audit</b>	Annual WebTrust and SAS-70 compliance audits are conducted by an independent, accredited third-party.
<b>Physical and Logical Access Security</b>	Multiple certificate types enable security for physical and logical access to applications in intranet, extranet, and Internet scenarios.

## + Learn More

For more information about VeriSign SSP PKI Service, please call 650-426-5310 or visit: [www.verisign.com/authentication](http://www.verisign.com/authentication)

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