

Symantec™ Shared Service Provider Public Key Infrastructure Service



Data Sheet: Authentication

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).

Symantec™ Shared Service Provider Public Key Infrastructure Service

With Symantec™ Shared Service Provider Public Key Infrastructure (SSP PKI) Service, U.S. Federal agencies are able to leverage Symantec's expertise and existing PKI platform that currently provides managed PKI services for thousands of commercial and government customers. Federal agencies benefit from Symantec'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** – Symantec 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. Shared Service Provider PKI Service fully complies with all requirements of the Federal PKI Common Policy.

- **Customizable environment** – Shared Service Provider PKI Service provides each federal agency with multiple, dedicated Certification Authorities (CAs), which enable the issuance of multiple, custom certificate types. The U.S. General Services Administration (GSA) Managed Service Offering does not offer this level of customization or flexibility.
- **Reliable and available** – Shared Service Provider PKI Service provides the reliability and availability necessary to help meet the mission-critical needs of federal agencies. Symantec's military-grade managed PKI platform supports 24 hours a day, seven days a week, 365 days a year monitoring, management, archiving, and full disaster recovery.
- **Real-time certificate management** – Shared Service Provider PKI Service includes a global, distributed certificate validation service to provide timely certificate status information.

Card management system integration

MyID® Personal Identity Verification (PIV) for Symantec™ is a comprehensive identity and card management system that, when combined with Shared Service Provider PKI Service, enables U.S. Federal Government agencies to comply with HSPD-12. MyID PIV for Symantec provides a single interface for registering, identity proofing, issuing, and maintaining PIV cards in compliance with the FIPS 201 standard. It is integrated with Shared Service Provider 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.



Data Sheet: Authentication

Symantec™ Shared Service Provider Public Key Infrastructure Service

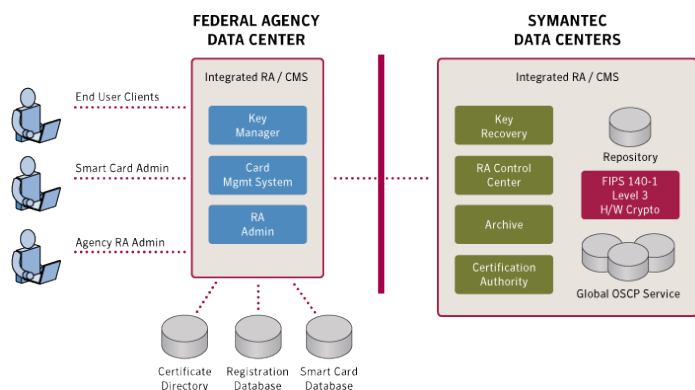


Figure 1: Symantec SSP PKI Service for HSPD-12

Features & Benefits

Feature	Benefit
Hosted certification authority (CA)	Symantec hosts and operates multiple, dedicated CAs for each federal agency, which include the following: <ul style="list-style-type: none"> FIPS 140 Level 3 hardware security modules for CA key generation and storage. Issuance of four PIV certificate types, plus CMS Signer, Domain Controller, OSCP Responder, and other certificate types as needed by U.S. Federal government agencies. Certificate Revocation List (CRL) issuance at least every 18 hours, per minimum requirements, or more often if desired.
Registration authority (RA)	Symantec provides the federal agency with the ability to: <ul style="list-style-type: none"> Remotely authenticate, approve/ reject, and revoke certificate requests from subscribers. Generate reports on certificate activity.
Key management service	Includes an integrated key management service with these capabilities: <ul style="list-style-type: none"> Generation and distribution of user-private encryption keys and certificates. Local Triple-DES encrypted storage of user-private

Feature	Benefit
	encryption keys. <ul style="list-style-type: none"> Two-man control for secure recovery of user-private encryption keys and certificates. Support for leading secure messaging solutions.
Mission-critical reliability	Delivers reliability and availability levels that help meet mission-critical needs; including 24x7x365 monitoring, management, archiving, and full disaster recovery.
Card management system support	Integration with MyID PIV for Symantec enables issuance of multiple smart card types, including PIV-interoperable smart cards, and delivers: <ul style="list-style-type: none"> An easy-to-use, Web-based interface that allows secure management of the entire lifecycle of smart cards and digital certificates. Support for various deployment models, including local printing and remote bureau printing for large volume deployments. Access to the system controlled through definable roles and smart card-based authentication.
Archive and reporting	An Oracle® database records signed audit information for all transactions. An integrated reporting tool is also included.
Online certificate status protocol (OCSP) service	Includes a distributed OCSP validation service to enable timely retrieval of certificate status.
Implementation and support services	Symantec Professional Services alleviate the burden of planning, implementing, and maintaining an in-house PKI support infrastructure. <ul style="list-style-type: none"> Includes 24x7x365 Level 2 help desk support and all required training for federal agency operations personnel.
Annual security audit	Annual WebTrust™ and SSAE 16 compliance audits are conducted by an independent, accredited third-party.
Physical and logical access security	Multiple certificate types enable security for physical and logical access to applications in intranet, extranet, and Internet scenarios.

More Information

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the



enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com