Secure Sensitive Data with the BIG-IP Hardware Security Module

A hardware security module (HSM) is a secure physical device designed to generate, store, and protect digital, high-value cryptographic keys. It is a secure crypto-processor that often comes in the form of a plug-in card with built-in tamper protection. HSMs also provide critical infrastructure in support of OMB mandates for the U.S. government; PCI Audit support for financial organizations; and Safe Harbor support for electronic record keeping in healthcare. The F5® BIG-IP® system includes a FIPS cryptographic/SSL accelerator—an HSM option specifically designed for processing SSL traffic in environments that require FIPS 140-2 Level 2–compliant solutions.

Understanding HSM

Developed by the National Institute of Standards and Technology (NIST), Federal Information Processing Standards are used by United States government agencies and contractors in non-military computer systems. FIPS 140 series comprises the U.S. government computer security standards that define requirements for cryptography modules, including both hardware and software components. The current version is FIPS 140-2.

FIPS 140 enforces strong cryptographic algorithms, provides good physical security, and requires power-on self tests to ensure a device is still in compliance before operating. FIPS 140-2 evaluation is required of vendors that sell products implementing cryptography to the federal government, and the financial industry is increasingly specifying FIPS 140-2 as a procurement requirement.

The FIPS card stores the private key associated with a site certificate on a server. It is only used in the initial SSL handshake to securely exchange the SSL session key. Once the client and server establish and exchange a session key, the session key is used to encrypt application data.

F5 Solution

F5 BIG-IP devices are FIPS 140-2 Level 2–compliant. This security rating indicates that once sensitive data is imported into a BIG-IP system HSM, it incorporates cryptographic techniques to ensure the data is not extractable in a plain-text format. BIG-IP system HSMs provide tamper-evident seals to deter physical tampering; in fact, they are certified at 140-2 Level 3, which means they have a covering of hardened epoxy that, if removed, will render the card useless.

Key features

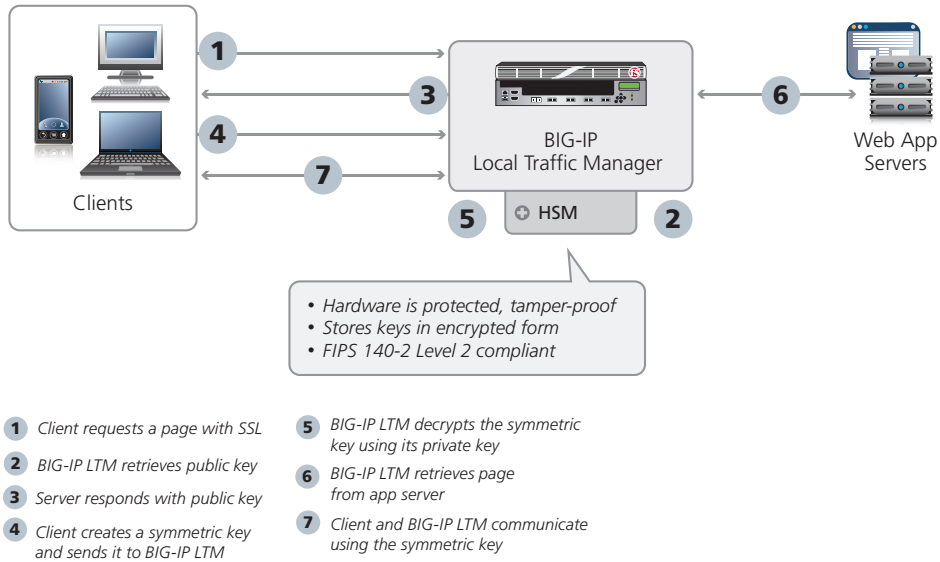
- **Strong Encryption**—Encrypts application traffic to ensure that confidential information is not disclosed
- **Stateful Firewall**—The BIG-IP system is an ICSA Labs Certified Network Firewall
- **Enhanced Security for SSL**—Stores, processes, and encrypts both keys and data
- **FIPS-Compliant**—Adheres to NIST standards specifying how to secure and encrypt sensitive data
- **Dynamic Threat Defense**—Provides a flexible means of enforcing protocol functions on both standard and emerging or custom protocols via iRules®

Key benefits

- **Unified Platform**—Enables the consolidation of SSL key management and certificate management on a single unit
- **Business Integrity**—Keeps corporate resources safe and protects the brand
- **Extensible and Adaptable**—Allows multiple application services to be managed on one device throughout the carrier network, so you can respond to new threats instantly
- **High-Performance SSL**—Processes 50,000 SSL transactions per second
- **Context Aware**—Understands user context to intelligently deliver critical applications

The BIG-IP system includes the factory-install option to add a FIPS 140-2 Level 3–certified SSL HSM in the 6900, 8900, 11000, and 11050 devices. The BIG-IP system's unique key management framework enables a highly scalable, secure infrastructure that can handle higher traffic levels, and to which organizations can easily add new services. Additionally, the FIPS cryptographic/SSL accelerator uses smart cards to authenticate administrators, grant access rights, and share administrative responsibilities, providing a flexible and secure means for enforcing key management security.

F5's FIPS-compliant application delivery platforms provide enhanced security for SSL by storing, processing, and encrypting both the keys and data in a hardware security module. In combining FIPS capabilities with application delivery services on a single device, the BIG-IP platform with FIPS-compliant HSMs provides compelling price and performance advantages, as well as protection for SSL-encrypted application traffic, while simplifying compliance management and reducing costs.



Architecture of the BIG-IP system with a hardware security module.

Learn more

For more information about BIG-IP hardware security modules, please see the following resources or search f5.com.

Web page

BIG-IP Local Traffic Manager

Datasheet

BIG-IP System Hardware Datasheet

White paper

F5 BIG-IP Platform Security

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com