

CryptoSwift HSM/WS

Physically Secure Accelerator



Hardware Security Module (HSM) for Physically Secure Acceleration

CryptoSwift HSM/WS™ by iVEA, is the ideal solution for today's business, banking, and financial environments requiring a high level of assurance when completing secure transactions over the Internet.

Designed to be compliant with the Federal Information Processing Standard (FIPS 140-1 Level 3), the CryptoSwift HSM/WS provides secure acceleration for public-key encryption associated with establishing a Secure Sockets Layer (SSL) connection between a Web server and browser. SSL is the most common security protocol used by organizations that must protect their customers' sensitive information while conducting a secure transaction like the transfer of money.

When establishing an SSL connection, the Web browser encrypts the session key with the Web server's public key. Only the Web server has the corresponding private key to unlock the encrypted session key, which is used for all the data communication between the Web server and the Web Browser later on. The private key is exposed in the Web server's memory in clear text when the Web server and Web browser are establishing a secure session. The exposure of the private key yields it potentially vulnerable to cyber-theft by hackers. The CryptoSwift HSM/WS provides physical security for the private key with on-board secure key storage and key generation. As a PCI card that can easily be installed on a Web server, the card has a tamper-resistant shield that protects the private key within a tamper-active circuitry that locks out any potential hackers.

The CryptoSwift HSM/WS also provides SSL acceleration, increasing throughput and speeding up the delivery of Web pages while lowering CPU utilization and freeing up the server to perform other tasks.

Key Benefits:

- Provides physical security for high-assurance web servers
- Tamper-proof casing secures sensitive keying information
- On-board RSA key generation and key storage.
- True on-board Random Number Generator
- SSL acceleration rated at 200 new sessions per second
- Free one year Web server certificate

For more information on CryptoSwift HSM, visit our Web site at www.ivea.com, or contact an iVEA office nearest you.



www.ivea.com

Specifications

Product Compatibility

Operating Systems

- SUN/Solaris 2.6, 7.0
- WinNT 4.0

Web Servers

- iPlanet Web Server 4.1 or later

APIs and Tool Kits

- PKCS#11 v2.01

Protocols Supported

- SSL 2.0
- SSL 3.0

Export

- Exportable internationally for approved applications

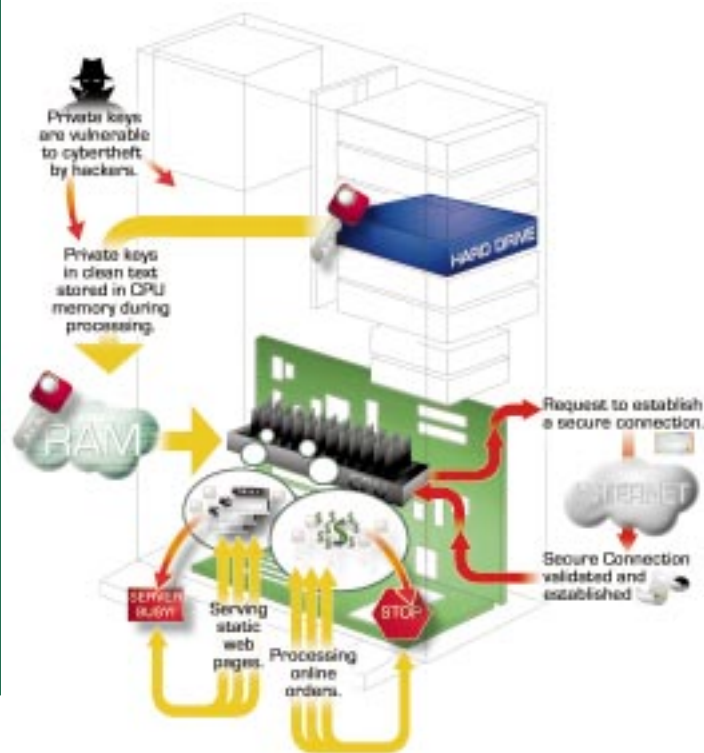
Cryptographic Functions

- Modular exponentiation functions: RSA
- RSA – 1024 and 2048-bit

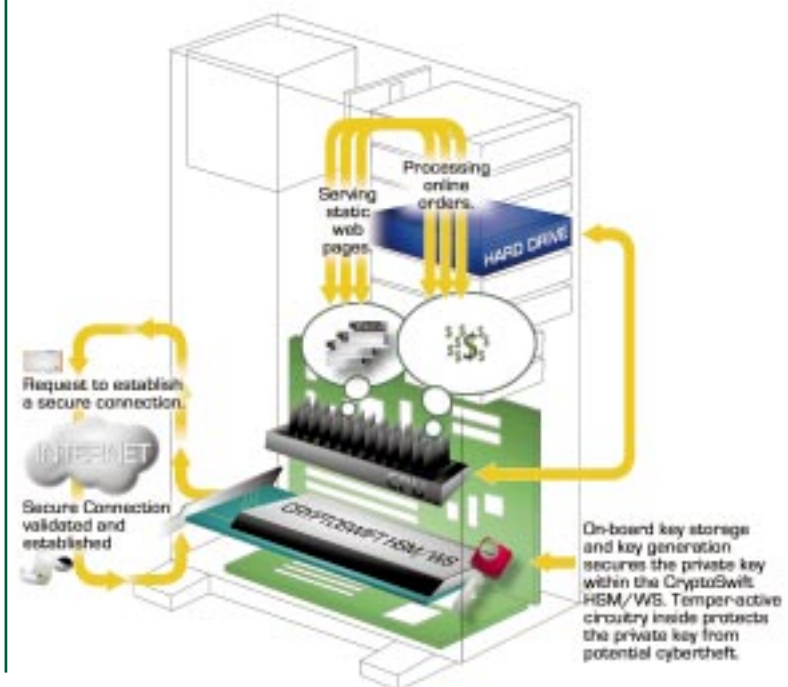
Regulatory Standards Certification

- U/L 94V-0 - EN61000-3-3
- FCC Part 15 – Class B - EN61000-4-2
- CE Compatibility - EN61000-4-3
 - CISPR 11/22 - EN61000-4-4
 - EN55022 – Class B - EN60950
 - Conducted Emissions - EN50082-1
 - EN55022 – Class B - ENV50204
 - Radiated Emissions - ENV50140
 - EN61000-3-2 – Class D

Secure Web Server **without** CryptoSwift HSM/WS



Secure Web Server **with** CryptoSwift HSM/WS



www.ivea.com

Corporate Headquarters

8 Hughes, Irvine, California 92618

toll free 877.274.4832 tel 949.206.7000 fax 949.206.7050

United Kingdom

Rainbow Technologies Ltd
4 The Forum, Hanworth Lane
Chertsey, Surrey KT16 9JX
Tel: +44 (0) 1932 579200
Fax: +44 (0) 1932 570743

Additional offices in the United States, Australia, Brazil,
China, India, Japan, The Netherlands, and Taiwan. Distributors
located worldwide.