

CryptoSwift HSM

Secure Network Performance

FIPS 140-1 Level 3 Certified:
Certificate #162



2001 High Tech Product of the
year for CryptoSwift HSM



Hardware Security Module (HSM) for Physically Secure Acceleration

The CryptoSwift® HSM by Rainbow Technologies, is the ideal solution for today's business, banking, and financial environments requiring a high level of security assurance and performance when completing transactions over the Internet.

The CryptoSwift HSM is validated with the Federal Information Processing Standard (FIPS 140-1 Level 3). The CryptoSwift HSM accelerates server performance when plugged into a Web Server. It protects a Web site's digital credential by keeping the signature inside the CryptoSwift HSM's security boundary.

The CryptoSwift HSM protects a Certificate Authority's root key or an Online Certificate Status Protocol (OCSP) Server's signing key by shielding it with a tamper-active circuitry. All digital signing and verification processes are done inside the HSM for better performance and security. All keying material is encrypted before they leave the HSM for backup purposes.

With its tamper-active design, the CryptoSwift HSM's evasive measures defeat physical attacks through detection and response to ensure the integrity and confidentiality of keying information. The CryptoSwift HSM also provides secure key generation, storage, archival, cloning, and migration. In addition, strong two-factor authentication is provided for Security Officers and Operators with the CryptoSwift HSM's trusted channel, a USB port with Rainbow Technologies' iKey authentication solution.

Key Benefits:

- Provides physical security and acceleration for high-assurance Web servers, Certificate Authorities and OCSP Servers
- Tamper-active circuitry secures sensitive keying information
- On-board RSA key generation, secure key storage and backup
- True on-board Random Number Generator
- SSL acceleration rated at 200 new sessions per second
- Scalable with multiple CryptoSwift HSM boards
- Java based key and device management software
- USB-trusted channel for conveying keying information and security officer/operator authentication

For more information on CryptoSwift HSM, visit our Web site at www.rainbow.com/cryptoswifthsm/, or contact a Rainbow office nearest you.

Specification

Product Compatibility

Operating Systems

- SUN/Solaris 2.6, 7.0, 8.0
- Microsoft Windows 2000
- WinNT 4.0, Service Pack 6 required
- Linux 2.2x and 2.4.x

Web Servers

- iPlanet Web Server 4.1 or later
- Apache 1.3.19
- IIS 5.0

Electrical Interface

- PCI 2.1, 3.3 and 5 volts

APIs and Tool Kits

- PKCS#11 v2.01
- PKCS#11 v2.10
- OpenSSL 0.9.6

Protocols Supported

- SSL 2.0
- SSL 3.0

Cryptographic Functions

- Modular exponentiation functions, including DH, DSA, and RSA
- RSA Public Key with CRT key lengths: 384-bit to 2048-bit
- RSA modulus length increment: 384-bit to 2048-bit
- RSA private key with CRT performance: 4.95ms/operation at 1024-bit
- Random Number Generation: 18,000 Bytes/second

Regulatory Standards Certification

- FIPS 140-1 Level 3-Certificate No.162 Certified
- U/L 94V-0
- FCC Part 15 – Class B
- CE Compatible

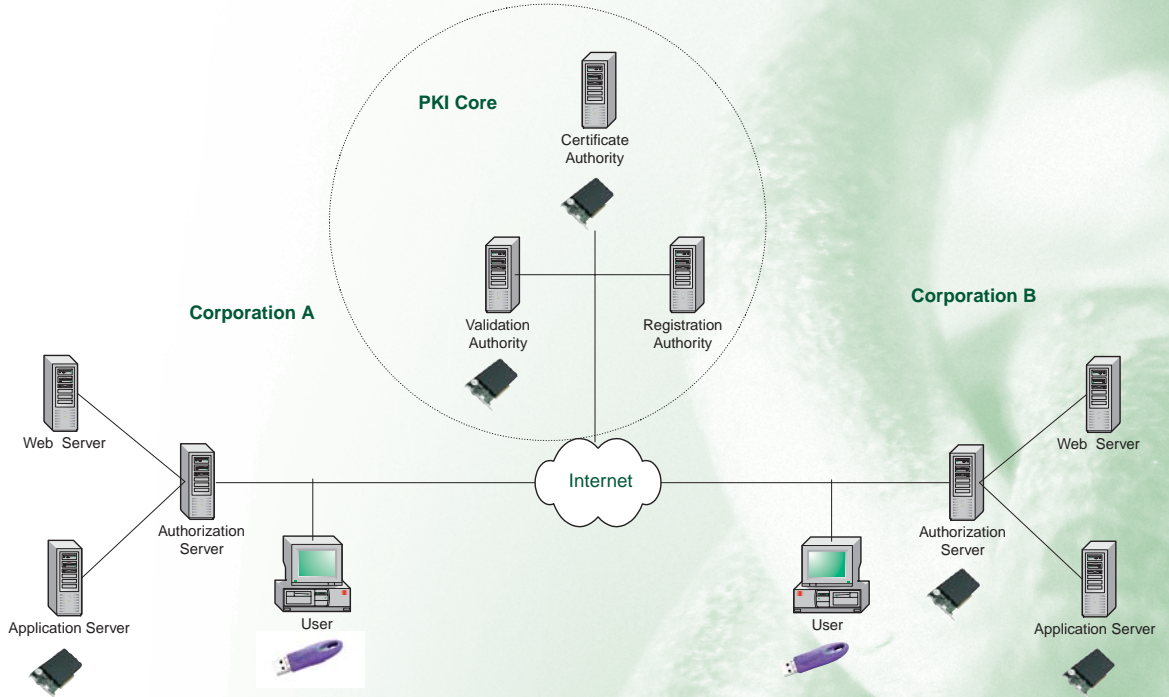
Export

- Exportable internationally for approved customers and applications



CryptoSwift HSM

PKI Applications



www.rainbow.com

Corporate: 50 Technology Drive, Irvine, CA 92618 USA
Tel: +1 949 450 7300 or +1 800 852 8569 eMail: sales@rainbow.com

Australia
Tel: +61 3 982 8322
<http://au.rainbow.com>

Brazil
Tel: +55 11 6121 6455
<http://www.rainbow.com/brasil>

China
Tel: +86 10 8851 9191
<http://cn.rainbow.com>

France
Tel: +33 1 41 43 29 00
<http://www.fr.rainbow.com>

Germany
Tel: +49 18 03 72 46 26 9
<http://www.de.rainbow.com>

Hong Kong
Tel: +852 3157 7111
<http://www.rainbow.com>

India
Tel: +91 11 26917538
<http://www.rainbowindia.co.in>

Japan
Tel: +81 3 5719 2731
<http://jp.rainbow.com>

Korea
Tel: +82 31 705 8212
<http://kr.rainbow.com>

Mexico
Tel: +52 55 5575 1441
<http://www.rainbow.com/mexico>

Singapore
Tel: +65 6274 2794
<http://www.rainbow.com>

Taiwan
Tel: +886 2 6630 9388
<http://tw.rainbow.com>

UK
Tel: +44 1932 579200
<http://www.uk.rainbow.com>

Distributors and resellers located worldwide.

Making Security Simple