CryptoSwift

eCommerce Accelerator

Handle unexpected peak loads, and deliver faster transactions to your clients.

Product Overview

Whether you are implementing an eCommerce Web site or a PKI environment, CryptoSwift™ can significantly improve your secure Web server response time and extend the life of your server investment. Rainbow Technologies' CryptoSwift accelerates the public-key cryptographic functions of SSL, TLS, SET, SSH and other widely used security protocols.

Using patent-pending technology, CryptoSwift contains a public-key processor that off-loads and speeds up the secure operations that would otherwise saturate the Web server's main processor. Running up to 600 transactions per second and processing a 1024-bit RSA transaction in less than 5 milliseconds, CryptoSwift improves server response time by up to ten times and frees your server to perform other tasks. The CryptoSwift board easily plugs into the PCI slot of your server and seamlessly installs into your secure Web server software. CryptoSwift works with the secure Web server resources you have in place allowing your infrastructure investment to last longer.

CryptoSwift's performance is available in speed configurations including 100, 200, and 600 transactions per second, matching your needs at a price you can afford. In addition, because CryptoSwift is scalable, multiple cards can provide increased performance; allowing you to handle any size peak load—for example, three cards triple the speed.

CryptoSwift Accelerates:

- SSL
- SSH
- TLS
- IPSec/IKE
- SET
- SWAN

Algorithms Supported:

- RSA
- DH
- DSS
- Modular exponentiation

Key Features

- Improves your server's response time by up to 10 times
- Seamlessly integrates with your secure server software
- Easy software installation
- Extinguishes customer wait-times
- True hardware random number generator
- Hardware secure key management capabilities
- Operates under multiple platforms
- Scalable performance with multiple CryptoSwift boards without requiring server reconfiguration
- CryptoSwift EN™, an external version is available
- CryptoSwift HSM™, a physically secure version is available
- Supported by leading cryptographic developer tool kits and secure applications

Applications

- Online Store Fronts
- Electronic Stock Trading
- Payment Gateways
- Financial Services
- Electronic Data Interchange (EDI)
- SET Merchant Servers
- Internet Service Providers
- Tax Processing
- Student Records
- Intranet Secure Servers
- Medical Records
- Travel Reservations

RAINBOW TECHNOLOGIES

Changing the way the world secures business.

http://www.rainbow.com/cryptoswift

Specifications

CryptoSwift is easy to install, and seamlessly integrates with your server software.

Product Compatibility

Device Driver O/S Compatibility
- AIX 4.3.2
- BSDi 3.0
- FreeBSD 2.1.5, 2.1.6
- Linux 2.2.5
- SUN/Solaris 2.5.1, 2.6, 7
- WinNT 4.0, 3.5.1, 3.5
- HP/UX 10.20, 11.0
- Windows 2000

Compatible Servers
- Apache Web Server
- Microsoft IIS/BackOffice
- C2Net Stronghold
- iPlanet Web Server
- Netscape Proxy Server
- Netscape Directory Server
- Netscape Enterprise Server

APIs, Tool Kits & Protocols

APIs and Tool Kits
- Consensus SSL Plus
- Cryptoki (PKCS #11) Ver.1.1, 2.0
- Entrust
- Intel CDSA
- Maithean NetPAY
- Microsoft CryptoAPI 1.0, 2.0
- OpenSSL
- RSA BSAFE; RSAref; RSA S/PAY
- SETref
- SSLeay

Protocols Supported
- SSL (Secure Sockets Layer)
- SET (Secure Electronic Transactions)
- SSH (Secure Shell)
- IPSec (IP Security)
- IKE (Internet Key Exchange)
- TLS, SWAN

CryptoSwift dramatically increases the number of clients your server can support.

Cryptographic Functions

- Modular exponentiation functions, including DH, DSA, RSA and raw modular exponentiation
- Secure data storage for private keys
- RSA Public Key w/ CRT key lengths—384-bit to 4096-bit
- RSA modulus length increments—128-bit
- RSA private key w/ CRT performance—4.95ms/operation at 1024-bit
- Random Number Generation—up to 4,096 Bytes/command
- RNG output—18,000 Bytes/sec

Regulatory Standards Certification

- U/L 94V-0 Flammability
- FCC Part 15 - Class B
- ISO - 9002 Certification
- CE Compatibility
  - -CISPR 11/22
  - -IEC 801-2, 801-3 and 801-4
  - -EN 60950

Export

- Exportable internationally for approved applications

* Performance data results are available at http://isglabs.rainbow.com

RAINBOW TECHNOLOGIES

Changing the way the world secures business.

http://www.rainbow.com/cryptoswift

50 Technology Drive, Irvine, California 92618
800.852.8569 tel. 949.450.7300 fax 949.450.7450 www.rainbow.com

France
Rainbow Technologies
122, Avenue Charles de Gaulle
92522 Neuilly sur Seine Cedex
Tel: +33 (0) 1414 32900
Fax: +33 (0) 1462 47691

Germany
Rainbow Technologies GmbH
Lise Meitner Strasse 1
85716 Unterschleissheim
Tel: +49 (0) 89 3217980
Fax: +49 (0) 89 32179850

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, China, India, The Netherlands, Russia & Taiwan. Distributors located worldwide.

000175-002 1/00