



SSLimSecure

for pSOS+

Secure Socket Layer

SSLimSecure is a robust, standards based, small-footprint Secure Sockets Layer (SSL) & Transport Layer Security (TLS) implementation for pSOSystem® 2.x and 3.x. SSLimSecure integrates the core functionality needed to implement secure client/server components. Its unique, advanced features include complete support for popular cryptography algorithms, APIs for hardware acceleration, easy integration with existing web-based device management systems, and enhanced memory management. Given its ability

to scale out optional features, SSLimSecure is ideally suited for use in low-resource embedded environments.

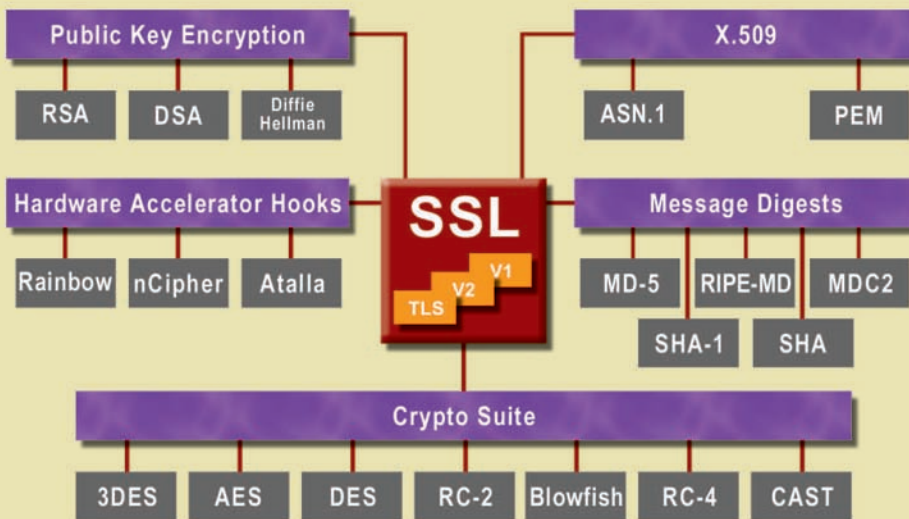
Cryptography Support

SSLimSecure's included crypto library contains implementations of most popular encryption and hashing algorithms. It also includes support for hardware accelerators and a framework for elliptic curves. The crypto functionality is completely modular, allowing for scaling out of unused ciphers for deeply scaled down memory

Features

- ❖ Provides client and server support for protocols SSLv2, SSLv3, TLSv1.
- ❖ Full featured cryptography including various flavors of AES, DES/3-DES, RC2, RC4, Blowfish, CAST, with FIPS certified algorithms available.
- ❖ Message digests and public key cryptography support.
- ❖ Provides APIs for hardware acceleration support.
- ❖ Enables native https support for GoAhead® and other popular embedded web servers.
- ❖ Includes digital envelope routines, base64 encoding and a framework for elliptic curves.
- ❖ Vulnerability countermeasures against timing based attacks.
- ❖ Support for CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/XScale
- ❖ Royalty-free!

SSLimSecure Components



pSOSystem Edition Features

- ❖ Designed exclusively for pSOS+
- ❖ Requires no special pSOS+ source modifications
- ❖ Integrated with pSOS+ and pRISM+ build & install methodology
- ❖ Common Crypto framework (Krypto-Lite) usable by other security protocols
- ❖ Enhanced memory management & regions support
- ❖ Multi-tasking support
- ❖ SSL layer is built on top of standard pNA socket interface
- ❖ Integrated with netutils library of pNA
- ❖ Native support for pSOSystem 2.x and 3.x

footprints when SSLimSecure is used, and can also be used by other applications and protocols, such as other members of TeamF1's SSecure family of products. Specifically the following cryptographic modules are included:

Encryption

- ❖ AES (Advanced Encryption standard or Rijndael)
- ❖ Fast crypt
- ❖ RC4
- ❖ RC2 which includes 4 modes — ecb, cbc, cfb, and ofb
- ❖ Blowfish which includes 4 modes — ecb, cbc, cfb, and ofb
- ❖ Eric A. Young's implementation of DES/3-DES which includes 15 flavors

Also Available

- ❖ **SSHield**
Secure Shell
- ❖ **V-IPSec IPsec & IKE**
Network Layer Security
- ❖ **FireFly**
IP-Filtering Firewall
- ❖ **ClassHopper**
Alternate Queuing Disciplines

Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized implementations of SSL solutions including support for custom hardware accelerators.

Customization Flexibility

- ❖ Available in full-source format
- ❖ Configurable choice of ciphers and authentication methods
- ❖ Overridable PRNG functionality
- ❖ Configuration loader
- ❖ Customizable hardware assist functionality
- ❖ Unwanted components can be scaled out

Built for pSOSystem

The pSOS edition of **SSLimSecure** is a drop-in component for pSOSystem 2.x and 3.x. It has been extensively validated on a variety of CPU architectures, and this minimizes development and integration efforts. **SSLimSecure** is especially optimized for pSOS+ with support for multi-tasking, memory regions, & abstractions that are lean, yet fast. **SSLimSecure** enables secure transactions in embedded network applications with the fewest changes.

- 1, 2, and 3 key (3-DES) versions of ecb, cbc, cfb, ofb
- pcbc
- generic cfb and ofb
- DESx in cbc mode

Message Digests

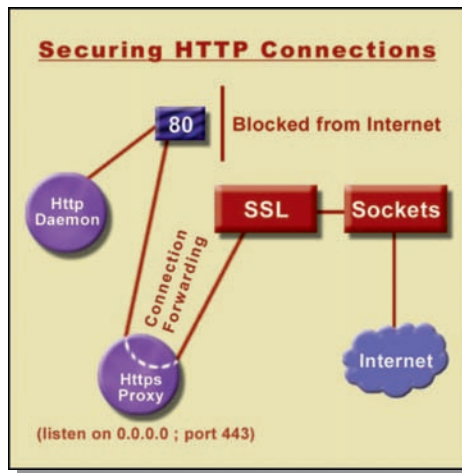
- ❖ MD5, RIPE-MD, MD-4, and MD2
- ❖ SHA (SHA-0) and SHA-1
- ❖ MDC2

Public Key Support and Digital Certificates

Public Key Cryptography is supported for RSA, DSA (FIPS 186-2 certified), and Diffie-Hellman with no limit on the number of bits. X.509 certificates are supported with encoding into and decoding from binary ASN1 and a PEM based ASCII-binary encoding which supports encryption with a private key. Enhanced CRL (Certificate Revocation List) support is also included.

Secure Web Communications

Because SSL is built into all major browsers, securing an embedded web server and having it respond to https requests is a convenient way of accessing secure data from an embedded system. **SSLimSecure**



enables any web server running on pSOS+ including the Go Ahead webserver, and several other third-party web servers to respond to https requests. Further, the client component of **SSLimSecure** can be used for secure downloads from any SSL-enabled web servers on the network. **SSLimSecure** also comes packaged with several web-based and non-web-based reference applications including proxy-https, that can be used as templates to secure any network application.

Requirement	SSHield SSH	SSLimSecure SSL	V-IPSec IPsec / IKE
Area of Security	Application	Transport/Session	Network
OSI Model Layer	L7	L4 / L5	L3
Secures legacy applications without modifications	✓	✗	✓
Typical area of usage	Management	Mgmt/Control	Data Path
Secures UDP (voice, NFS etc.)	✗	✗	✓
Standardized authentication mechanisms	✓	✓	✗
Extensible with authentication protocols	✓	✗	✓*
Supports User Authentication	✓	✓	Add-on
Suitable for sophisticated security policies	★★★	★	★★
Cross-platform interoperability	★★★	★★★	★★
Compatible with NAT & Firewalls	✓	✓	Limited
VPN capabilities	★	★★★	★★★
Per-connection/user end-to-end traffic flow confidentiality	✓	✓	✗
Protection against DoS attacks and traffic analysis	★★	★★★	★★★
Ease of provisioning	★★★	★★★	★★
Fine grained programmatic control	★★	★★★	★★★

* Protocol does not provide standard interface for extending authentication mechanisms.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

This product includes cryptographic software from the OpenSSL cryptographic library written by Eric Young (eay@cryptsoft.com) and Tim J. Hudson (tjh@cryptsoft.com).

Email: sales@TeamF1.com
 Web: www.TeamF1.com
 Ph: 510-505-9931 ext. 5
 Fax: (510) 505-9941



© 2002-2004 TeamF1, Inc.