

# SSLimSecure

## Embedded SSL and TLS Client and Server



**SSLimSecure** is an embedded implementation of the Secure Sockets Layer (SSL) & Transport Layer Security (TLS) protocol. **SSLimSecure** integrates the core functionality needed to implement secure HTTPS client/server components that are fully interoperable with free and commercial HTTP web browser and server implementations, and to secure any non-HTTP socket based transactions as well.

**SSLimSecure** includes support for all popular cryptography algorithms including AES and 3-DES and offers easy integration with existing web-based device management systems, embedded web servers and HTTP clients. Given its ability to scale out optional features, **SSLimSecure** is ideally suited for use in low-resource embedded environments.

**SSLimSecure** is a robust, standards based, small-footprint socket-based framework that secures data exchanged between two network applications. It includes a powerful implementation of Secure Sockets Layer (SSL) & Transport Layer Security (TLS)

protocols for embedded devices, with a comprehensive set of encryption ciphers for data privacy, cryptographic hash algorithms for message integrity checks and X.509 v3 (and older) digital certificate support for authentication.

**SSLimSecure's** SSL framework installs itself above the TCP/IP layers, and below higher-level application protocols such as HTTP or custom transaction protocols. It then uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, optionally allows the client to authenticate itself to the server, and allows both machines to establish an encrypted and tamper-proof data connection.

**SSLimSecure** powerful features include an implementation of most common versions of the SSL protocol (v2 and v3) and also the newest IETF standardized TLS v1.x. While **SSLimSecure** comes pre-packaged with a wide variety of encryption and has algorithms, its modular design allows scaling out of any cipher, thereby eliminating any memory and performance from components that are not used by the embedded application.

**SSLimSecure's** APIs allow the securing of any TCP socket-based client/server network applications via just a few API calls from the application to initiate the SSL handshake, and replacing socket calls with their secure equivalents. This enables secure management of connected embedded devices a snap, and also helps

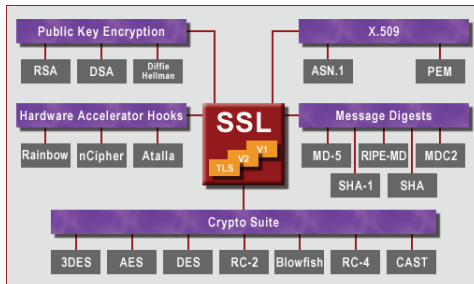


Fig 1: SSLimSecure Components

### Features

- ❖ Provides client and server support for protocols SSLv2, SSLv3, and TLSv1.
- ❖ Full featured cryptography including various flavors of AES, DES/3-DES, RC2, RC4, Blowfish, CAST.
- ❖ Message digests and public key cryptography support.
- ❖ Provides APIs for hardware acceleration support.
- ❖ Enables native Https support for WindWeb, WIND Manage and other 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!

in securing data or measurements that may have to sent back to an SSL enabled server. Further optimizations such as a using the same SSL parameter template ("context") for various SSL sessions, and customizable hardware assist functionality are also included in **SSLimSecure**.

While **SSLimSecure** can secure any socket based transaction, web-server or HTTP-client security is undoubtedly a popular use of SSL technologies. **SSLimSecure** can secure both the client and server sides of an HTTP session simultaneously in the same system, and with the use of a proxy mechanism can also achieve this without any modifications to existing HTTP server and client code.

Out of the box integration (even in the absence of proxies) is included for common embedded web-servers including shhttp, thhttpd, WindWeb and WIND Manage for Web. This allows for an easy upgrade to

### Special Features

- ❖ Includes server and client components
- ❖ Server authentication with X.509 Digital Certificates
- ❖ Support for per-connection variables
- ❖ Certificate Revocation List (CRL) support
- ❖ Memory partition support to isolate memory usage of various **SSLimSecure** modules
- ❖ Enhanced memory management & partition support
- ❖ Multi-tasking support
- ❖ SSL layer is built on top of standard OS socket interface
- ❖ Works with packet-filtering firewalls such as FireFly by blocking normal web-server port so only secure (https) connections are allowed

secure existing web-based device management frameworks.

**SSLimSecure** has been extensively validated on a variety of CPU architectures, and this minimizes development and integration efforts. **SSLimSecure** supports multi-tasking, memory partitions, & abstractions that are lean, yet fast. **SSLimSecure** enables secure transactions in embedded network applications with the fewest changes, and provides a seamless solution that is interoperable with existing web servers and web-browsers on embedded and non-embedded platforms.

### Cryptography Support

**SSLimSecure**'s included crypto library contains APIs to support most popular ciphers for encryption and hashing, and 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 footprints when **SSLimSecure** is used, and can also be used by other applications and protocols. 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

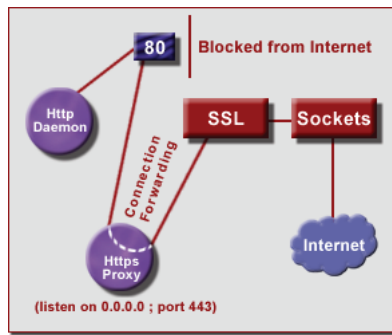


Fig 2: Securing HTTP Connections

DES/3-DES which includes 15 flavors

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

#### Message Digests

- ❖ MD5, RIPE-MD, MD-4, and MD2
- ❖ SHA (SHA-0), SHA-1, SHA-2 (256, 384, 512)
- ❖ MDC2

### Public Key Support and Digital Certificates

Public Key Cryptography is supported for RSA, DSA 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

Requirement	SSHield SSH	SSLimSecure SSL	V-IPSecure 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).

### Also Available

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

### Custom Solutions

Expertly customized implementations of SSL solutions including support for custom hardware accelerators are available through **TeamF1**'s professional services team.

### 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.

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 the embedded device 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 that can be used as templates to secure any network application.

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



© 2011 TeamF1, Inc.