

SharkSSL

SharkSSL delivers an extremely compact Secure Socket Layer/Transport Security (SSL/TLS) stack. It's designed from the ground up to ensure completely secure communication and management of remote embedded devices and dedicated applications.

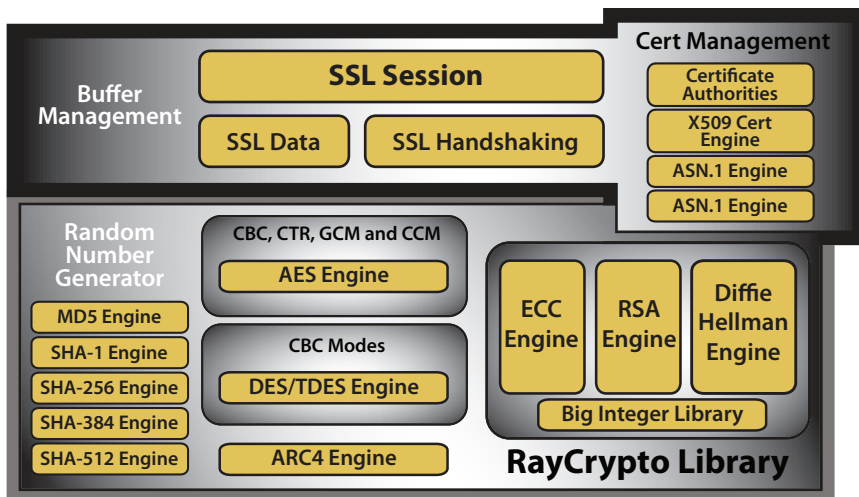
Using a transport-agnostic API, SharkSSL supports virtually any embedded device from 8- to 64-bit microcontrollers while maintaining the optimal security and performance needed for reliable communications in the most stringent IoT and M2M applications.

SharkSSL incorporates:

- Elliptic Curve technology & Suite B
- Crypto Libraries for processors that provide limited or no acceleration support

Enterprise level security < 20kb

SharkSSL is the world's smallest and best-performing SSL v3.0/TLS v1.0/1.1/1.2 solution. With many compile-time options, SharkSSL can be fine-tuned to require an extremely small footprint. For example, on ColdFire®, SharkSSL occupies less than 20-kB total footprint using the "CAU" cryptography acceleration coprocessor unit.

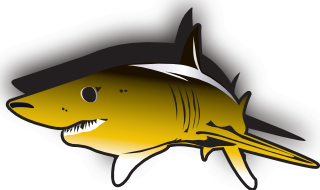


SharkSSL Features

SharkSSL is designed to ease the development of secure IoT and network applications.

- Embedded M2M Client Framework
 - Communicates with backend M2M web server
 - Supports secure, persistent, real-time protocol.
 - Small footprint M2M client to server link easily fits into the internal memory of small MCUs
- Embedded WebSocket Client Library
 - C source code WebSocket Client Library
 - Eases M2M by applying the RFC 6455 "WebSocket protocol"
- Minnow Server (Embedded Web Socket Server)
 - Embedded WebSocket server
 - Enables small MCUs without external memory to act as real-time web server
- Embedded SMTP Library
 - SMTP C source code library
 - SMTP authentication compliant (RFC 4954)
 - Secure SMTP/SMTPLS compliant
 - STARTTLS compliant (RFC 3207)
 - Supports server authentication with Certificate Authorities Validation
 - Supports client certificate for client authentication

Fig. 1: SharkSSL incorporates RayCrypto, a bundle of cryptographic libraries supporting every authentication and encryption algorithm you are likely to need.



SharkSSL



Embedded Tools GmbH Fon: +49 251 98729-0
Willy-Brandt-Weg 33 Fax: +49 251 98729-20
48155 Münster www.embedded-tools.de

Supports hardware encryption

SharkSSL excels on any processor while including the off-the-shelf optimized precision to take full advantage of coprocessor encryption acceleration. Available with source code, SharkSSL achieves unmatched throughput on all popular processors.



Optimized C & assembly libraries

SharkSSL, with its proprietary C- and assembly-optimized big integer library, delivers record-breaking performance on processors without specialized hardware-acceleration encryption engines as well as those with only partial hardware acceleration.

“While keeping code size to a minimum, SharkSSL is capable of performing a private RSA operation 60 percent faster than the competitors’ solutions.”

Supported Leading Encryption Standards:

- AES (including GCM and CCM)
- SHA256/384/512
- 3DES
- ARC4
- SHA1
- MD5
- Poly1305
- ChaCha20

Licensing

SharkSSL is a Commercial Proprietary solution containing no open source. Proprietary Security solutions provide an inherent protective barrier because the source code is not freely downloadable or accessible for malicious experimentation and is not susceptible to anonymous contributions.

License grants are available to verifiable, commercial or academic organizations creating a system of check and balance at the first level of access.

- 90 days of Support & Maintenance (included)
- General commercial licensing is available on a perpetual or term basis with no run-time royalties or volume restrictions.

Supports RTOS, HLOS or Bare Metal

SharkSSL supports multi-threaded applications. Real-time Operating System (RTOS) support includes:

- INTEGRITY™
- MQX™
- SMX™
- ThreadX™
- VxWorks™
- EBSnet™
- rtplatform
- uCLinux™
- Linux
- Windows™
- No-OS (Bare Metal)*

**Shark SSL is not reliant on the provision of an operating system, and is equally effective when applied to bare-metal configurations.*

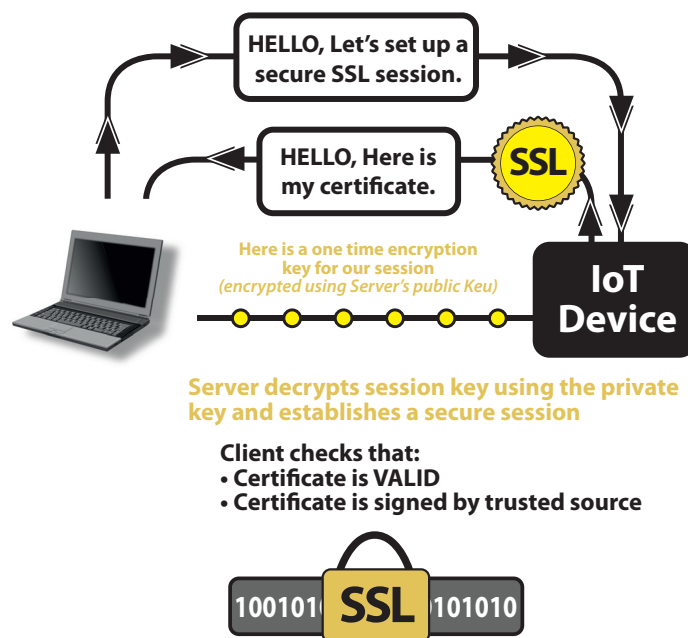


Fig. 2: In addition to providing encryption, SharkSSL also provides trust management. It tells you if you can trust the peer side you are connected to.

About Real Time Logic

Real Time Logic is a leader in embedded web server and security products for remote management and control. We offer high-performance, reliable web applications with enterprise-level security on compact, lower-power devices.



Headquarter Real Time Logic LLC 14 Monarch Bay Plaza, #108 - Monarch Beach, CA 92629 USA
phone +1 949-388-1314 fax +1 949-272-3781 www.realtimelogic.com ginfo@realtimelogic.com



Embedded Tools GmbH
Willy-Brandt-Weg 33
48155 Münster
Fon: +49 251 98729-0
Fax: +49 251 98729-20
www.embedded-tools.de