Cypherbridge® Systems uSSL™ Security Stack

Overview

The Cypherbridge Systems uSSL security stack implements a standards based solution to achieve chip-to-chip and chip-to-server interoperability across wired and wireless networks.

With the advent of the connected device era, classic SSL/TLS is just the beginning. uSSL is the ideal solution for a wide-variety of security applications for industrial, point-of-sale, instrumentation and metering, machine-to-machine, and standalone systems where a small-footprint, standards based solution is called for.

An application specific subset of uSSL security features can be tailored to support simple client authentication, RSA based encryption, in-memory or in-file bulk security, boot loader flash image hash verification, and a wide range of application specific requirements.

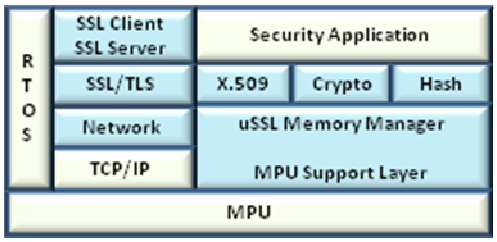

Figure 1: uSSL block diagram

Product Integrity

MCU platforms are pervasive, and it has become vital to provide a comprehensive security solution that can keep pace with the so-called internet of devices. Embedded products including the boot-loader, firmware and programmable logic, are vulnerable to reverse engineering, unauthorized use, and remote access and communication security risks.

System quality may become compromised in industrial and consumer applications, not due to classic *product reliability*, but instead due to *product integrity*. This has led to new requirements in product planning and development to integrate security features in MCU based designs. By including standards based security features, these risks can be greatly reduced to increase product integrity, improve field support and system availability, enhance interoperability, and increase product lifecycle ROI.

Accelerate Time-to-Market

Time-consuming proprietary solutions and desktop SSL derived libraries pose significant compromises when it comes to footprint and memory, typically relying on ANSI C memory heap which can result in memory thrashing and fragmentation when used for SSL processing. This can lead to problems in device-level applications where performance, duration and reliability is paramount.

With its designed-for-chip source code, the uSSL memory management layer optimizes dynamic memory allocation, avoiding roll-your-own desktop SSL compromises. uSSL is thread-neutral, and can be integrated with RTOS task and embedded heap APIs.

User configurable for specific features, uSSL achieves industry leading small footprint for small to medium memory models where flash and RAM must be carefully balanced.

uSSL design wins have achieved system and information integrity on multiple MCU families including payment card applications. Accelerate your application time-to-market with uSSL.

Features

- ✓ *SSL 3.0/TLS 1.0 server and client protocol support*
- ✓ *Supported crypto and hash functions include: RSA, PKCSv1.5, DES, 3DES, AES, RC4, SHA1, SHA2, MD2, MD4, MD5, RNG*
- ✓ *X.509 certificate processing for signing and authentication*
- ✓ *Memory management layer with dynamic buffer trace*
- ✓ *MCU platform support layer*
- ✓ *Network interface layer to 3rd party RTOS and TCP/IP stack*
- ✓ *Available projects for tool chains including IAR, GCC, Code Composer Studio*
- ✓ *Interoperates with Windows RSACryptoService Provider and Linux Apache SSL*
- ✓ *Complete self-test functions and sample application code*
- ✓ *Utilities including PKI key generator import to uSSL*
- ✓ *Portable ANSI-C small RAM and ROM footprint targeted to low-power 16 and 32 bit microcontrollers*
- ✓ *Royalty-free source code license*

For Pricing and Availability Contact:

Cypherbridge Systems, LLC
7040 Avenida Encinas #104211 Carlsbad, CA 92011
www.cypherbridge.com
sales@cypherbridge.com
Tel: (760) 814-1575

About Cypherbridge Systems:

Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.

CSL-uSSL-0917.1