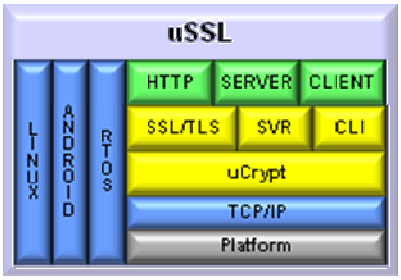
Cypherbridge® Systems uSSL™ Security SDK

Overview

The Cypherbridge Systems uSSL SDK delivers the optimal solution for chip-to-chip and chip-to-server connected device security. Standards based and interoperable across wired and wireless networks, uSSL interfaces to Linux and Windows based back office systems

uSSL is the ideal solution for a wide-variety of vertical applications in industrial, smart grid, energy management systems, SCADA telemetry, payment terminals, instrumentation and metering and M2M, where a small-footprint, standards based solution is called for.

uSSL security features can be optimized for application specific requirements to support 2WAY X509 client authentication and hardware acceleration.



Electronic Data Privacy

The era of the internet of things and big data brings with it new concerns. uSSL meets industry standards, regulatory requirements, and emerging regional policies for electronic data privacy and integrity to protect against surveillance and cybercrime.

Product Integrity

Systems can be compromised not due to *reliability*, but instead due to *data integrity*.

This has led to new product planning requirements to integrate standards based security features in MCU based designs. Risks can be greatly reduced to increase data integrity, reduce field support costs, increase system availability for higher product lifecycle ROI.

Accelerate Time-to-Market

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

With its designed-for-chip source code, uSSL avoids roll-your-own desktop SSL compromises. uSSL includes an integrated memory manager for a zero-heap solution. The uSSL ANSI C thread-free library is designed for portability and can be integrated with a wide range of MCU, RTOS and TCP.

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

Cloud Device Kit

The Cypherbridge CDK option leverages the uSSL SDK to provide direct-to-cloud data center secure synchronization and replication. It is targeted for SCADA, smart meters, energy gateways, EVSE, and any vertical application where data sets are managed across multiple devices and back end business systems.

Features

- ✓ *IETF standard SSL 3.0/TLS 1.2 protocols*
- ✓ *Embedded server and client*
- ✓ *Supported crypto and hash functions include: RSA, DSS PKCSv1.5, OAEP, DES, 3DES, AES, RC4, SHA1, SHA2, MD2, MD4, MD5, RNG*
- ✓ *X.509 certificate processing for signing and authentication*
- ✓ *Integrated memory manager*
- ✓ *MCU platform support layer. Integrated with most popular RTOS and TCP/IP stacks*
- ✓ *Available on FreeRTOS/lwIP*
- ✓ *Available projects for tool chains including IAR, GCC, Code Composer Studio*
- ✓ *Complete self-test functions and sample client and server applications*
- ✓ *Portable ANSI-C small RAM and ROM footprint for MCUs*
- ✓ *Royalty-free source code license*

Options

- ✓ *Certbuilder X.509 toolkit to generate, manage and embed certificates*
- ✓ *Cloud Device Kit cloud file system scalable sync and replication*

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-131115.1