Cypherbridge® Systems uSSL™ SDK

Cypherbridge®
Trusted, Safe and Secure

Overview

The uSSL SDK is compact ANSI C software development kit that implements TLS server and client operations. The uSSL SDK is designed for small and medium memory models where CPU and memory resources are carefully allocated and balanced. It is portable to a wide range of processors and platforms from embedded MCU to MPU.

IETF protocol standards TLS 1.3 1.2, 1.1, 1.0 and SSL 3.0 are fully implemented for secure network protocol handshake message processing, cryptographic operations, and extensions handlers.

SDKPac

The Cypherbridge SDKPac Framework integrates uSSL TLS, X.509 Credentials Manager, and uCrypt™ library, and Platform.

The SDKPac Credentials Manager includes off-line utilities and run-time APIs to configure RSA and ECDSA certificates and private keys. Credentials can be dynamically loaded to perform sign and verify operations for TLS handshake.

The uCrypt™ library full features cryptographic and math library includes symmetric block and stream ciphers, AEAD, hash and HMAC, HKDF, along with a wide range of X.509 PKI PKCS operations. This fully supports the TLS standard cipher suites including TLS 1.3. Platform dependent hardware crypto offload is available.

The SDKPac Platform kit includes platform dependent interfaces to CPU, I/O, MCU HAL, flash memory, along with integrated dynamic memory pool manager for zero heap. Platform kits are available for a wide range of IoT platforms, RTOS, TCP/IP, and networks including Ethernet, WiFi, and LTE.

Embedded Client

The uSSL embedded client implements TLS secure connection to private, public and hybrid cloud services, including Azure IoT, AWS, and OpenSSL hosted services.

Embedded Server

The uSSL embedded server implements TLS secure connection to browser or proprietary applications. This implements a framework to build proprietary embedded services that are secured and interoperable.

dHTTP Server

SDKPac adds full function dHTTPS web server. TLS secure, it includes HTTP 1.1 POST GET CGI ENV SSI CSS and client javascript with sample forms. Extended features include file transfer upload and download, client login and authentication, cookies and AJAX. Content management includes ROM content compiler and platform file system support.

Platform Portability

The uSSL ANSI C99 SDK is highly portable and supported on a wide range of development kits, RTOS, TCP/IP stacks and toolchains.

Applications and Industry Sectors

uSSL is RFC standards based and fully interoperable. Applications include industrial control, telemetry, energy systems, geo-location tracking, medical device applications, network equipment, and many more.

Securing the Internet of Things

Secure new product designs to meet current and emerging IoT industry practice and regulatory requirements. In addition to new product designs, the proven flexible SDKPac uSSL framework is designed to integrate, modernize, and secure existing product lines.

Features

- ✓ *RFC8446 TLS 1.3*
- ✓ *RFC5246 TLS 1.x*
- ✓ *Configurable ECDSA and RSA host keys using Credentials Manager*
- ✓ *Configurable crypto includes ECDH, SuiteB AES128-256 CTR AEAD GCM SHA256-SHA512 CHACHAPOLY1305*
- ✓ *Low footprint zero threaded library for RTOS and embedded TCP/IP stacks*

Applications

- ✓ *Smart Meter*
- ✓ *IoT Gateway*
- ✓ *SCADA Telemetry*
- ✓ *Geo-location*
- ✓ *Industrial Control*
- ✓ *PLC and RTU*
- ✓ *Network appliances*
- ✓ *Data Center equipment*
- ✓ *EVSE Charging Stations*

SDKPac Options

- ✓ dHTTP
- ✓ uMQTT
- ✓ uSMTP
- ✓ uRADIUS
- ✓ uMODBUS
- ✓ MBAPS Modbus TLS Secure

For Pricing and Availability Contact:

Cypherbridge Systems LLC
7040 Avenida Encinas #104211 Carlsbad, CA 92011
www.cypherbridge.com
sales@cypherbridge.com
Tel: +1 (760) 814-1575

About Cypherbridge Systems:

Established in 2005, delivering a broad range of secure connectivity protocols and solutions including

- *IoT Device SDKs and Toolkits*
- *Product and System Integration*
- *Full Stack Cloud Computing*