Cypherbridge Systems

Embedded Systems Solutions
Our Commitment is Total Customer Satisfaction

(760) 840-0629
www.cypherbridge.com
info@cypherbridge.com

CYPHERBRIDGE SYSTEMS ANNOUNCES uSSL SDK SUPPORT FOR ARM CORTEX-M3

Cypherbridge Systems announces support for the uSSL Software Development Kit on ARM© Cortex-M3™ platforms. The uSSL SDK implements a complete suite of SSL/TLS security standards, achieving chip-to-server interoperability across wired and wireless networks with Windows and Linux enterprise systems.

Combining industry-leading MIPS, low-power, and connectivity, ARM Cortex-M3 powered MCUs are taking the industry by storm, bringing 32-bit performance to 8 and 16 bit price points. Available in fully-integrated SOC solutions from industry leaders including Texas Instruments, ST Microelectronics, and Atmel, these MCUs are designed into networking and telecom, automotive and industrial, consumer appliances, medical and many more applications.

uSSL is the ideal solution for a wide-variety of security applications for ubiquitous computing, connected devices, machine-to-machine, and standalone systems where a small-footprint, standards based solution is called for. Increasingly, projects are using a subset of the uSSL security suite to support simple client authentication, RSA based encryption, in-memory or in-file bulk security, boot loader flash image hash verification, MCU/FPGA authentication and encryption, and a wide range of application specific requirements. uSSL is designed to be easy to configure for applications ranging from classic end-to-end SSL, to single component embedded security solutions.

Time-consuming roll-your-own 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.

uSSL avoids these problems using a self-contained internal memory manager with fine-grained sizing and tuning features to optimize platform memory allocation. Highly configurable to enable only the specific features needed, 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, including PCI compliance, on multiple MCU families. Accelerate your application time-to-market with uSSL. For pricing and availability, visit our website today, or call for detailed product and pricing information, and let us know how we can serve your application specific requirements using our embedded stack solutions, including the uKernel RTOS with real-time diagnostics monitor, small footprint TCP/IP, and HDMI and GPS SDKs.

PRODUCT FEATURES AND BENEFITS

Features

- ✓ *SSL/TLS server and client protocol support*
- ✓ *TCP/IP network socket adaptation layer*
- ✓ *Supported crypto and hash functions include RSA, 3DES, AES, RC4, SHA1, SHA2, MD2, MD4, MD5, Trivium*
- ✓ *X.509 certificate processing*
- ✓ *Base64 encode/decode*
- ✓ *Portable ANSI C*
- ✓ *Operates on 8, 16, and 32 bit, microcontrollers*
- ✓ *Small RAM and ROM footprint*
- ✓ *Self-contained memory manager*
- ✓ *API documentation and sample code making easy to use for both experienced and first-time crypto integrators*
- ✓ *Can be integrated with MCU security API libraries and cores*
- ✓ *Tool support including CodeSorcery, CCE, Keil*

Applications

- ✓ *Industrial information security, privacy, and compliance*
- ✓ *Payment Card Industry, Point-of-Sale Terminals*
- ✓ *Machine-to-Machine wired and wireless application security*
- ✓ *In-Memory and in-File Bulk storage encryption*
- ✓ *RSA asymmetric keying*
- ✓ *Signing and verification*
- ✓ *File hashing and integrity checks for secure firmware boot loading and field upgrades*
- ✓ *MCU/FPGA authentication and encryption using Diffie-Hellman key exchange and symmetric cipher*
- ✓ *Public Key Infrastructure, device and server authentication*