SSL / TLS now available for CMX-MicroNet and CMX-TCP/IP

The SSL/TLS Add-On option is now available for CMX-MicroNet and CMX-TCP/IP TCP/IP stacks. The SSL/TLS offers a comprehensive suite of SSL/TLS security standards for embedded devices, offering support for client and/or server applications.

With growing demand for security across public and private networks in numerous industry segments including automotive, industrial, medical, energy management and more, SSL/TLS offers a full set of crypto and hash functions and also allows the designer to implement a subset of these functions for client and/or server authentification, MCU/FPGA authentification and encryption, RSA based encryption, in-memory or in-file bulk security and bootloader flash image hash verification.

SSL/TLS is designed for ease of use and eliminates the need for time-consuming roll-your-own solutions or derived libraries which compromise footprint and memory or rely on ANSI C memory heap often resulting in memory thrashing and fragmentation when used for SSL processing. SSL/TLS eliminates these problems using a self-contained internal memory manager with fine-grained sizing and tuning features to optimize platform memory allocation. Designers can further optimize flash and RAM by enabling only those features required for the specific application.

SSL/TLS Feature Summary:

- Small footprint Add-On for CMX-MicroNet and CMX-TCP/IP TCP/IP Stacks
- SSL / TLS Client and Server functionality
- Self-contained memory manager
- X.509 Certificate Processing
- Base 64 encode / decode
- Integrates with MCU security API libraries and cores
- 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
- Portable ANSI C Code
- Ported for popular tool chains
- Sample code and API documentation provided
- Support for 8-, 16- and 32-bit processors
- Hash and Crypto functions including; AES, 3DES, RC4, RSA, SHA1/2, MD2, MD4, MD5 and Trivium

In the case of SSL/TLS, some of it is supplied as source code and some is supplied as as library code.

For more information, please visit CMX Systems' website at http://www.cmx.com.