Embedded Encryption Manager

Verifiable Data Encryption for Flash and Networking

HCC's Embedded Encryption Manager™ allows developers to secure embedded systems using multiple encryption or hash algorithms through a uniform interface. Using a well-defined interface shortens development time as developers can now simply drop-in the Encryption Manager and encrypt data stored on flash or transmitted across a network. Such security is necessary to block potential hackers looking for a backdoor to access embedded system data.

E-mail: info@hcc-embedded.com • Web: www.hcc-embedded.com

HCC embedded

Developed using a formal process, HCC Embedded Encryption Manager undergoes verification to ensure stability and enhanced integrity. It is delivered with a full MISRA compliance report and a test suite that includes 100% MC-DC coverage. This level of verifiable quality in the area of security and encryption stands in direct contrast with the widely used 'code-then-test' methods, which have resulted in serious security breaches, such as Heartbleed.

Encryption Manager Operation

The Encryption Manager controls all access and resource allocation for the core module and registered algorithms. Drivers are created for each algorithm to be supported; this includes HCCs range of algorithms and also allows the creation of target-optimized algorithms. These drivers are then registered with the encryption module and each application requiring an algorithm requests a handle for the specified algorithm. The handle is then used to access the encryption drivers through HCC's encryption manager API.

Key features

- All code is fully MISRA compliant
- Test suite includes 100% MC/DC coverage of the module and the algorithms
- Module can be extended with new algorithms
- All algorithms are designed to have hardware-specific optimizations
- Module includes the ability to dynamically add and verify microcontroller-specific algorithm implementations

Verified software algorithms: AES, 3DES, DSS, EDH, MD5, RSA, SHA1, SHA256

Hardware Optimization

The software includes hooks to allow hardware-specific optimization to be implemented where supported by the target controller along with the verification suite to ensure that the hardware optimizations are done correctly.

Seamless Integration with any RTOS, MCU and Toolchain

Using HCC's Advanced Embedded Framework, the HCC Embedded Encryption Manager is completely portable and algorithms are accessed by reference through the encryption Manager, freeing the application of direct references to a particular algorithm. The Encryption Manager can be used with HCC's verifiable TLS or any other application requiring access to a suite of verifiable encryption algorithms. HCC can supply all software as fully integrated source code supplied with abstractions to operate with any RTOS, development board, toolchain or MCU peripheral tested on the target system. Should any of these elements change in future projects, only the framework abstractions change leaving all interfaces to file systems and communications software unchanged – meaning working with HCC software is a long term investment.