SEGGER releases cryptographic library emCrypt

Hilden, Germany – 24th April 2017 –

SEGGER today announced immediate availability of its new emCrypt cryptographic algorithm library. emCrypt is a complete software library of cryptographic algorithms, written entirely in C, with high performance. It can easily be fine-tuned to favor smaller or faster code. Hardware acceleration for various popular MCU families such as STM32, Kinetis, EFM32 and LPC18S/43S is available.

emCrypt is extremely versatile, including all relevant block ciphers, hashes, MACs, and digital signatures required to meet the demanding cryptographic needs of modern embedded devices and the ever expanding IoT universe.

Having been designed from the ground up for use in memory-constrained embedded systems, emCrypt uses minimal resources in respect of memory footprint (RAM/ROM) as well as CPU utilization. It can be used on MCUs as well as on larger systems with lots of memory, as well as on tablets and PCs.

Test applications and example code come with the product and make it very easy to use. Executables for Windows and Linux are available as utilities for download free of charge.

The algorithms in emCrypt have been been proven for years in SEGGER products such as emSecure, emSSL, emSSH, Secure email client, Dropbox access as well as numerous customer applications, and are now available for use in any application on 16/32 or 64-bit processors, under simple non-GPL, non-viral licensing terms.

“Today's embedded systems need sophisticated security and encryption software. Writing these from scratch is not an option, open source solutions are either not available, not suitable for embedded systems or not usable due to viral licensing (GPL). I believe that emCrypt with its NIST proven and highly efficient implementation of even exotic algorithms is the best solution for applications - not limited to the Embedded Computing space - needing cryptographic algorithms,” says Rolf Segger, founder of SEGGER Microcontroller.

The product is available in two flavors, as affordable Base version with the most common cryptographic algorithms and as PRO package with all algorithms which are currently in wider use. All algorithms are tested against test vectors, most algorithms are also NIST validated.

The library includes block ciphers such as AES and DES, Hashes such as SHA-1 and all SHA-2 / SHA-3 variants, MACs such as HMAC, CMAC, GMAC, KMAC, public key encryption (RSAES-OAEP), key agreement (DH, ECDH, X25519), key derivation (HKDF, KDF1, KDF2), and digital signatures (RSASSA-PSS, RSASSA-PKCS1, ECDSA, Ed25519).

To access more information on emCrypt and its performance go to: https://www.segger.com/emcrypt.html

More information on emSSH is available at: https://www.segger.com/emssh.html

More information on emSSL is available at: https://www.segger.com/emssl.html

More information on emSecure is available at: https://www.segger.com/emlib-emsecure.html

###

About SEGGER

SEGGER Microcontroller is a full-range supplier of software, hardware and development tools for embedded systems. The company offers support throughout the whole development process with affordable, high quality, flexible and easy-to-use tools and components. SEGGER offers solutions for secure communication as well as data and product security, meeting the needs of the rapidly evolving IoT. SEGGER was founded in 1997, is privately held, and is growing steadily. Headquartered in Germany with a US office in the Boston area and distributors in all continents, SEGGER offers its full product range worldwide. For additional information, visit: https://www.segger.com

Contact information:

Dirk Akemann
Marketing Manager
Tel: +49-2103-2878-0
E-mail: info@segger.com

Issued on behalf of:

SEGGER Microcontroller GmbH & Co. KG
In den Weiden 11
40721 Hilden
Germany
www.segger.com

SEGGER Microcontroller Systems LLC
106 Front Street
Winchendon, MA 01475
United States of America
www.segger-us.com