SEGGER veröffentlicht Kryptographiebibliothek emCrypt

Hilden, Deutschland – 24. Dezember 2017 –

SEGGER hat heute angekündigt, dass ab sofort die neue Softwarebibliothek emCrypt verfügbar ist. emCrypt ist eine Softwarebibliothek für Kryptographie mit hoher Verarbeitungsgeschwindigkeit, die vollständig in C geschrieben wurde. Sie kann einfach auf optimale Code-Größe oder höhere Verarbeitungsgeschwindigkeit eingestellt werden. Für verschiedene populäre MCU-Familien wie STM32, Kinetis, EFM32 und LPC18S/43S sind Hardware-Beschleuniger verfügbar.

emCrypt is extrem flexibel und beinhaltet alle wichtigen Block Ciphers, Hashes, MACs und digitale Signaturalgorithmen, die notwendig sind, um die steigenden Anforderungen an die Kryptographie moderner Embedded Systeme und des stetig wachsenden IoT Universums zu erfüllen.

Von Grund auf konzipiert für die Nutzung in Systemen mit eingeschränkter Speicherverfügbarkeit, nutzt emCrypt so wenig Speicher wie möglich in RAM und ROM und belastet die CPU so wenig wie möglich. Die Softwarebibliothek kann sowohl auf Microcontrollern als auch auf größeren Systemen mit viel Speicher wie Tablets oder PCs eingesetzt werden

Testanwendungen und Beispielcode werden gleich mitgeliefert und vereinfachen den Einstieg. Hilfsprogramme für Windows und Linux sind als Download frei verfügbar.

Die Algorithmen von emCrypt haben sich bereits seit Jahren in SEGGER Produkten, wie emSecure, emSSL, emSSH, dem Secure E-Mail-Client, der Dropbox-Unterstützung sowie in zahlreichen Kundenapplikationen bewährt. Diese Algorithmen sind nun für jede Applikation auf 16-, 32-, oder 64-Bit Prozessoren unter einfachen nicht-GPL, nicht-viralen Lizenzbedingungen erhältlich.

„Heutige Embedded Systems erfordern ausgefeilte Sicherheits- und Kryptographie-Software. Diese selbst zu schreiben ist keine Option, Open Source Lösungen sind entweder nicht verfügbar, nicht geeignet für Embedded Systems oder unbrauchbar wegen der viralen Lizenz (GPL). Ich denke, emCrypt ist durch die NIST Prüfung und die hoch effiziente Implementierung auch für exotische Algorithmen die beste Lösung für Anwendungen, die Kryptographie benötigen, auch für Systeme außerhalb des Embedded Computing," sagt Rolf Segger, Gründer von SEGGER Microcontroller.

Das Produkt wird in zwei Versionen angeboten. Auf der einen Seite als Base version mit den populärsten Algorithmen und als PRO Paket mit allen Algorithmen, die üblicherweise verwendet werden. Alle Algorithmen werden gegen Testvektoren geprüft. Die meisten Algorithmen sind zusätzlich NIST validiert.

Die Bibliothek beinhaltet Block Ciphers wie AES und DES, Hashes wie SHA-1 und alle SHA-2 / SHA-3 Varianten, MACs wie HMAC, CMAC, GMAC, KMAC, Public Key Verschlüsselung (RSAES-OAEP), Key Agreement (DH, ECDH, X25519), Key Derivation (HKDF, KDF1, KDF2), und digitale Signaturen (RSASSA-PSS, RSASSA-PKCS1, ECDSA, Ed25519).

Für weitere Informationen zu emCrypt und der Performance, besuchen Sie bitte: https://www.segger.com/emcrypt.html

Mehr Information zu emSSH steht unter: https://www.segger.com/emssh.html

Mehr Information zu emSSL steht unter: https://www.segger.com/emssl.html

Mehr Information zu emSecure steht unter: https://www.segger.com/emlib-

emsecure.html

###

Über SEGGER

SEGGER Microcontroller ist Hersteller einer umfassenden Palette an Software, Hardware und Entwicklungswerkzeugen für Embedded Systems. Das Unternehmen bietet Unterstützung für den kompletten Entwicklungsprozess mit preiswerten, hoch-qualitativen, flexiblen und schnell einsetzbaren Werkzeugen und Komponenten. Um der rasanten Entwicklung im Bereich IoT gerecht zu werden, bietet SEGGER Lösungen ebenso für sichere Kommunikation wie für Daten- und Produktsicherheit.
SEGGER wurde 1997 gegründet, ist in privater Hand und wächst stetig. Das Hauptquartier ist in Deutschland bei Düsseldorf. Mit einem Büro nahe Boston in den USA und Distributoren auf allen Kontinenten bietet SEGGER das gesamte Produktsprektrum weltweit an. Für weitere Informationen besuchen Sie bitte: https://www.segger.com

Kontakt:

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

Herausgegeben im Auftrag von:

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