emSecure-ECDSA: Cutting-edge alternative algorithm for SEGGER's digital signature suite

Hilden, Germany – October 13th, 2015

With emSecure-ECDSA, SEGGER is adding a new powerful product to its digital signature suite. The emSecure software package now offers two different schemes for the generation and verification of digital signatures – RSA and ECDSA. This widens customer options when using emSecure to protect against firmware hacking and hardware cloning.

emSecure is a software solution to authenticate digital assets. It can be used to secure products at no per unit cost against hacking and cloning and has to date been offered with RSA signatures by default.

While RSA has proven robust for decades, ECDSA (Elliptic Curve Digital Signature Algorithm) is a relatively modern algorithm and a FIPS and IEEE standard since 2000.

Each digital signature variant has its own advantages. With the emSecure product family now offering two schemes for signature generation, the user has the choice which option better fits his requirements.

ECDSA provides the same level of security as RSA with shorter key lengths. A 256-bit ECDSA key is equivalent to a 2048-bit RSA key. Shorter keys not only save space - the underlying calculations of the algorithms may be completed faster. This especially applies to signature generation, which is about seven times faster compared to RSA and makes it possible to sign data even on small microprocessors very efficiently in time and energy expended.

emSecure-ECDSA has been created to fit a wide range of requirements in terms of size, speed, and level of security. It uses about 10 kByte of ROM and no static RAM. Signature verification can be done within 160 ms, with less than 2.5 kByte on the stack, measured on a Cortex-M and using the P-256 curve.

More information on emSecure-ECDSA can be found here: https://www.segger.com/emlib-emsecure-ecdsa.html

About emSecure

emSecure is an RSA and ECDSA-based software solution to authenticate digital assets. It is used to prevent firmware hacking and to secure products against cloning at no per unit cost. The software package allows creation and verification of digital signatures. Based on asymmetric encryption algorithms with two keys, emSecure signatures cannot be forged by reverse engineering of the firmware. In addition to the integrity check, a digital signature assures the authenticity of the provider of the signed data. emSecure secures firmware updates distributed to embedded devices and authenticates licenses, serial numbers, and other sensitive data.

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

###

About SEGGER

SEGGER Microcontroller develops and distributes hardware and software development tools as well as software components for embedded systems. An "embedded system" is one in which a microprocessor and associated components are incorporated into a device helping to accomplish difficult and complex tasks in products such as cell phones, medical instruments, instrument clusters, measurement instruments, satellite radios, digital cameras etc.

SEGGER was founded in 1997, is privately held, and is growing steadily. Based in Hilden with distributors in all continents and a local office in Massachusetts, SEGGER offers its full product range worldwide.

SEGGER software products include: embOS (RTOS), emWin (GUI), emFile (File System), emUSB (USB host and device stack) and embOS/IP (TCP/IP stack). With emSecure, a unique software to generate and verify digital signatures, and the TLS-solution emSSL, SEGGER is also offering software for the growing field of data and product security.

With the experience in programming efficiently on embedded systems, SEGGER created highly integrated, cost-effective programming and development tools, such as the Flasher (stand-alone flash programmer) and the industry leading J-Link/J-Trace emulator.

SEGGER cuts software development time for embedded applications by offering affordable, high quality, flexible and easy-to-use tools and software components allowing developers to focus on their applications. Find out more at 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