emSecure-ECDSA: Leistungsfähiger alternativer Algorithmus für SEGGERs Digital Signature Suite

Hilden, 13. Oktober 2015

Mit emSecure-ECDSA fügt SEGGER seiner Digital Signature Suite ein leistungsfähiges neues Produkt hinzu. Das Softwarepaket emSecure bietet nun zwei unterschiedliche Algorithmen zur Erstellung und Verifikation digitaler Signaturen – RSA und ECDSA. Dies erweitert die Optionen der Kunden beim Schutz gegen Firmware-Hacking und Hardware-Cloning mit emSecure.

emSecure ist eine Software-Lösung zur Authentifizierung digitaler Assets. Sie kann ohne Stückkosten zur Sicherung von Produkten gegen Hacking und Cloning eingesetzt werden und ist bislang standardmäßig mit RSA-basierter Signatur ausgeliefert worden.

Während RSA seine Zuverlässigkeit bereits über Jahrzehnte unter Beweis gestellt hat, ist ECDSA (Elliptic Curve Digital Signature Algorithm) ein vergleichsweise neuer Algorithmus und seit dem Jahr 2000 FIPS und IEEE-Standard.

Beide Varianten für die Signatur-Erstellung haben ihre jeweiligen Vorteile. Mit dem Angebot zweier alternativer Mechanismen können Nutzer jetzt selbst die Entscheidung treffen, welche Option ihren Präferenzen und Anforderungen besser entspricht.

ECDSA bietet bei kürzerer Schlüssellänge den gleichen Grad an Sicherheit. Ein 256-Bit ECDSA-Schlüssel ist einem 2.048-Bit RSA-Schlüssel vergleichbar. Kürzere Schlüssellängen sparen nicht nur Speicherplatz, die Kalkulation der dahinter liegenden Algorithmen ist auch schneller abgeschlossen. Dies gilt insbesondere für die Generierung der Schlüssel: Sie funktioniert etwa sieben Mal schneller und ermöglicht es daher, Daten selbst auf kleinen Mikroprozessoren sehr effizient mit Blick auf Zeit- und Energiebedarf zu signieren.

emSecure-ECDSA ist für eine breite Palette von Anforderungen an den Speichbedarf, Geschwindigkeit und Sicherheitsgrad ausgelegt. Es benötigt ungefähr 10 KByte ROM und hat keinen statischen RAM-Bedarf. Die Verifizierung einer Signatur kann innerhalb von 160 Millisekunden erfolgen, mit weniger als 2,5 KByte auf dem Stack – diese Werte wurden für einen Cortex-M ermittelt unter Nutzung der P-256 Kurve.

Weitere Informationen zu emSecure-ECDSA finden sich hier:
https://www.segger.com/emlib-emsecure-ecdsa.html

Über emSecure

emSecure ist eine RSA- und ECDSA-basierte Software zur Authentifizierung digitaler Assets. Es wird zum Schutz vor Firmware-Hacking und gegen Klonen eingesetzt. Das Software-Paket ermöglicht die Generierung und Verifizierung digitaler Signaturen. Diese basieren auf asymmetrischer Verschlüsselung mittels eines Schlüsselpaares und können daher selbst durch Reverse Engineering der Firmware nicht rekonstruiert werden. Zusätzlich zum Integritäts-Check stellen

digitale Signaturen die Authentizität des Absenders der Daten sicher. emSecure sichert Firmware-Updates für embedded Devices und authentifiziert Lizenzen, Seriennummern oder andere sensible Daten.

Weitere Informationen zu emSecure sind hier verfügbar:
https://www.segger.com/emlib-emsecure.html

###

Über SEGGER

SEGGER Microcontroller entwickelt und vertreibt Hardware- und Software-Entwicklungswerkzeuge sowie Software-Komponenten für Embedded-Systeme. Ein „Embedded-System" integriert einen Mikrocontroller/Mikroprozessor und entsprechende Komponenten in einem Gerät bzw. Produkt, um komplexe Aufgaben zu erledigen. Typische Produkte sind Mobiltelefone, medizinische Geräte, Kombi-Instrumente, Messgeräte, elektronische Haushaltsgeräte, digitale Kameras, etc.

SEGGER wurde 1997 gegründet. Das privat geführte Unternehmen verzeichnet ein kontinuierliches Wachstum. Mit Firmensitz in Hilden, globalen Distributoren und einer Niederlassung in Massachusetts ist SEGGER weltweit tätig.

Die Software-Produkte von SEGGER umfassen: embOS (RTOS), emWin (GUI), emFile (File System), emUSB (USB Host und Device Stack) sowie embOS/IP (TCP/IP Stack). Mit emSecure, einer einzigartigen Software für das Erstellen und Nutzen von digitalen Signaturen, sowie der TLS-Lösung emSSL bietet SEGGER außerdem Software für den wachsenden Bereich der Daten- und Hardware-Sicherheit, auch im IoT-Umfeld.

Basierend auf umfangreicher Erfahrung mit der effizienten Programmierung von Embedded- Systemen entwickelte SEGGER hochintegrierte, kosteneffiziente Programmierungs- und Entwicklungs-Werkzeuge, wie einen Flasher (Stand-alone Flash-Programmer) sowie den industrieweit führenden J-Link/J-Trace Debug Probes.

SEGGER reduziert mit seinen kostengünstigen, hochwertigen, flexiblen und einfach einzusetzenden Tools bzw. Software-Komponenten die System-Entwicklungszeit für Embedded-Anwendungen. Damit können sich Entwickler verstärkt um ihre eigentliche Applikation kümmern. Weiter Informationen findet man unter: 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
Deutschland
www.segger.com

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