INSIDE SECURE HIGH-PERFORMANCE VAULTIC SECURITY MODULES RECEIVE FIPS CERTIFICATION

VaultIC 420, 440 and 460 Deliver the Most Comprehensive Collection of FIPS140-2 Level 3 Certified Cryptographic Algorithms and Services in the Industry

AIX-EN-PROVENCE, France, September 18, 2012 – INSIDE Secure, a leader in semiconductor solutions for secure transactions and digital identity, today announced that three members of its high-performance VaultIC™ family of hardware security modules have been awarded FIPS140-2 Security Level 3 (2011) certification. With this achievement, the high-performance VaultIC 420, 440 and 460 security modules are now able to provide the most comprehensive collection of FIPS-certified cryptographic algorithms and security services in the industry, allowing manufacturers of USB authentication tokens and a variety of embedded authentication, secure network communications, fiscal printer, smart metering, and secure data storage applications to use a single security solution to address all their global markets.

"Having FIPS certification gives us a major advantage over the competition in this market because it is an important requirement for any manufacturer using cryptography to provide security in products they sell to the U.S. government, and it has also become recognized as an important benchmark of security quality by the financial and health-care industries, as well as by other governments and industries around the world," said Christian Fleutelot, general manager and executive vice president Digital Security for INSIDE Secure. "With the large number of key cryptographic algorithms and services supported by these high-performance VaultIC modules, manufacturers can now more quickly and easily bring FIPS-certified products to market."

The VaultIC 420, 440 and 460 security modules include high-performance implementations of the most advanced cryptographic standards, including AES, 3DES-EDE and 3DES-EEE, PKCS#1 v2.1 RSAES-OAEP and RSAES-PKCS1 v1.5. Digital signature services include PKCS#1 v2.1 RSASSA-PSS and RSASSA-PKCS1 v1.5, FIPS 186-2 DSA and ECDSA and ANSI X9.62 over ECC. Message authentication codes include ISO/IEC 9797-1 MAC with DES/3DES, NIST SP 800-38B AES CMAC and FIPS 198 HMAC with SHA1 to 512. ISO/IEC 9798-2, FIPS 196 and Microsoft Card Minidriver strong challenge-response authentication is provided, as well as Global Platform v2.2 (SCP02 secure channel using 3DES and SCP03 using AES) secure communication channel with MAC and encryption. A variety of secure file management features are also included.

This broad range of embedded security firmware makes it easy to implement a fully user-defined non-volatile storage of sensitive or secret data; set up identity-based authentication with user, administrator and manufacturer roles; perform authentication, digital signature, encryption/decryption and other advanced cryptographic operations using keys and data from the file system; and provide secure communication channels to satisfy customer requirements around the world.

The VaultIC 420, 440 and 460 security modules share a common tamper-resistant hardware platform, including a high-performance 8-/16-bit secure RISC CPU, hardware random number generator, hardware 3DES crypto-accelerator, hardware AES crypto-accelerator and hardware 32-bit public key crypto-accelerator. The chips feature 32, 64 and 128 Kbyte EEPROM capacities, respectively, and a real-time clock, and include a full speed certified, CCID-compliant USB 2.0 interface, high-speed slave serial peripheral interface (SPI), inter-integrated circuit (I2C) interface, ISO/IEC 7816 standard UART and 10 GPIOs for the greatest flexibility in connecting the VaultIC to applications. Available in industry standard SOIC and QFN packages, these VaultIC tamper resistant modules offer the fast, easy integration of advanced security into any product.

About VaultIC Security Modules

INSIDE VaultIC security modules replace complex and expensive proprietary systems with a low cost, easy-to-integrate, higher security and proven solution. A single low-cost chip combines a powerful, secure microcontroller, secure storage for encryption keys, digital certificates and other sensitive data, hardware crypto accelerators, multiple interfaces and advanced security firmware to protect a broad range of products against counterfeiting, cloning or identity theft.

The embedded security firmware makes it easy to implement fully user-defined non-volatile storage of sensitive or secret data; set up identity-based authentication with user, administrator and manufacturer roles; perform authentication, digital signature, encryption/decryption, on-chip public key pair generation and other advanced cryptographic operations using keys and data from the file system; and provide secure communication channels using 3DES or AES.

INSIDE's VaultIC Starter Kit provides an easy path to mastering the cryptographic and secure data storage features of the VaultIC security modules, and includes PKCS#11 and CSP mini driver libraries.

About INSIDE Secure

INSIDE Secure (NYSE Euronext Paris FR0010291245 – INSD.PA), is a leading designer, developer and supplier of semiconductors, embedded software and platforms for secure transactions and digital security. INSIDE mobile NFC, secure payment and digital security products provide security for a wide range of information processing, storage and transmission applications. The company's customers are found in a wide range of markets including mobile payment, identification documents, access control, transit, electronic device manufacturing, pay television and mobile service operators.

For more information, visit www.insidesecure.com.

# # #

***For INSIDE Secure**:*
Patrick Corman
Corman Communications, LLC
+1 (650) 326-9648
patrick@cormancom.com

Geraldine Sauniere
Marcom Director INSIDE Secure
gsauniere@insidefr.com
+33 (0) 4 42 39 33 01

INSIDE Secure:
Juliette dos Santos
Andrew Lloyd & Associates
+33 (0) 1 56 54 07 00
juliette@ala.com