FOR IMMEDIATE RELEASE

Allegro Software Announces FIPS Embedded Device Security

FIPS Validated Cryptography Library for Embedded Systems

BOXBOROUGH, MA – December 16, 2013 – Allegro Software Development Corporation, a leading supplier of Internet component software for embedded devices, today announced that it has earned FIPS 140-2 level 2 validation for the Allegro Cryptography Engine, ACE™. Specifically engineered for the rigors of embedded computing, ACE enables manufacturers to add standards-based cryptography to resource sensitive embedded systems quickly, easily and reliably while decreasing time to market. ACE is ideally suited for use in embedded transportation, military, energy, healthcare and communications applications where strong validated cryptography is a requirement.

FIPS 140-2

Early embedded systems were unprepared to address the new security implications of network connectivity. Many industries now have a heightened awareness that embedded systems and larger enterprise systems that include embedded devices are vulnerable to a whole new realm of Internet attacks. The National Institute of Standards and Technology (NIST) has taken steps to ensure security and compatibility between communicating computers by defining Federal Information Processing Standards (FIPS). They specifically identified a set of guidelines (FIPS 140-2) for cryptographic-based security systems to protect sensitive information in computer and telecommunication systems, whether desktop or embedded, and asserted the requirement that vendors must comply to these standards to sell and support the government or its contractors. The application and testing process to earn FIPS 140-2 validation is rigorous and non-trivial, but for companies selling security products to the federal government, their contractors or allies overseas, formal FIPS validations are a prerequisite to eligibility for government contracts.

ACE and FIPS 140-2 Validation

The 140-2 FIPS (Federal Information Processing Standards) are used to accredit cryptographic "modules" that drive secure software or hardware implementations, and most federal agencies and contractors working on sensitive government projects are prohibited from buying products containing security software that is not officially FIPS-validated. Allegro applied for and received FIPS 140-2 level 2 validation for the Allegro Cryptography Engine. ACE is one of the smallest, fastest, and most comprehensive FIPS 140-2 validated software modules on the market. ACE was specifically engineered to meet the critical needs of embedded computing systems and purposely designed to meet the requirements for FIPS 140-2 validation. With a common software interface, embedded systems developers can easily perform bulk encryption and decryption, message digests, digital signature creation and validation, and key generation and exchange. ACE additionally includes a platform independent implementation of the NSA defined Suite B suite of cryptographic algorithms, as well as other FIPS approved algorithms. The FIPS approved cryptographic algorithms included in ACE have been validated and are listed on the NIST CAVP sites along with the final validation designation on the NIST CVMP site.

"Data privacy is a significant issue for the billions of network-enabled embedded systems that inhabit the Internet" says Bob Van Andel, President of Allegro. "Allegro's ACE toolkit significantly reduces risk, development effort, integration and testing time while giving our customers FIPS-validated security solutions engineered for use in embedded systems." ACE is delivered as an ANSI-C source code toolkit and is available now. For additional information on ACE, visit our website: http://www.allegrosoft.com/ace.

Reference

NIST CAVP Sites:

http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html
http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsaval.html

NIST CVMP Site:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

About Allegro

Allegro Software Development Corporation is a premier provider of embedded Internet components with an emphasis on device management, embedded device security and UPnP-DLNA networking technologies. Since 1996, Allegro has been a force in the evolution of secure device management solutions with its RomPager embedded web server and RomPager Secure toolkits. Also an active contributor to UPnP and DLNA initiatives, Allegro supplies a range of UPnP and DLNA toolkits that offer portability, easy integration and full compliance with UPnP and DLNA specifications. Allegro is headquartered in Boxborough, MA and can be found on the web at http://www.allegrosoft.com.

Contacts:

Loren Shade
VP Marketing
Allegro Software Development Corporation
978-264-6600
loren@allegrosoft.com

Larry LaCasse
VP Business Development
Allegro Software Development Corporation
978-264-6600
larrylc@allegrosoft.com