FOR IMMEDIATE RELEASE

Allegro Software Announces Integrated Embedded Device Security

FIPS Approved Cryptography for Embedded Systems

SAN FRANCISCO, CA and BOXBOROUGH, MA – February 25, 2012 – At the RSA® Conference 2013 in San Francisco, CA, Allegro, a leading supplier of Internet software for embedded devices, today announced the addition of Allegro Cryptography Engine, ACE™, to the RomPager® suite of embedded internet toolkits. Specifically engineered for the rigors of embedded computing, ACE makes embedding standards-based security protocols into resource sensitive embedded systems such as military, energy and healthcare embedded applications fast, easy and reliable while decreasing time to market.

FIPS 140-2

Billions of embedded systems are quietly working behind the scenes of almost all modern technologies, from automobiles and factory floors, healthcare networks and new medical devices, defense and energy markets to space exploration missions. Increasingly, these critical embedded systems are built from commercial products, and often incorporate standards-based network connectivity. Early networked desktop PCs and servers were unprepared to address the new security implications of network connectivity. The same is true for many of today's embedded systems which presents a significant new security concern that must be addressed immediately and systematically. Many industries, especially post 9-11, now have a heightened awareness that embedded systems and larger enterprise systems with embedded devices are vulnerable to all types of Internet attacks. Within the government, the National Institute of Standards and Technology (NIST) and National Security Agency (NSA) have taken steps to ensure security and compatibility between communicating computers by defining Federal Information Processing Standards (FIPS). Working together they have 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. In addition to the government systems market, the FIPS 140-2 standards have been adopted by the financial (Check21, etc.), energy (Smart Grid) and healthcare (HIPAA, HITECH, etc.) industries to safe-guard their data.

ACE and Embedded Device Security

The Allegro Cryptography Engine (ACE) is a cryptographic library module specifically engineered to meet the critical needs of embedded computing systems and designed to meet the requirements needed for FIPS 140-2 validation. The module provides embedded systems developers with a common software interface to enable bulk encryption and decryption, message digests, digital signature creation and validation, and key generation and exchange. In 2005, the NSA defined a set of cryptographic algorithms that when used together, are the preferred method for assuring the security and integrity of information passed over public networks such as the Internet. Today, Suite B is globally recognized as an advanced standard for cryptography that defines algorithms and strengths for encryption, hashing, calculating digital signatures and key exchange. ACE includes a platform independent, implementation of the NSA Suite B defined 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 site. An implementation that includes the ACE module is in process for FIPS 140-2 validation and is listed on the NIST CVMP site.

"The next-generation of network-enabled embedded systems must meet the need for high encryption standards to ensure data privacy" says Bob Van Andel, President of Allegro. "The availability of Allegro's ACE FIPS toolkit significantly reduces development, integration and testing time, while giving our customers the security they need." ACE is delivered as ANSI-C source toolkit and will be available in Q2-2013. Stop by Allegro's booth at the RSA Conference 2013, Booth #239 to discuss embedded device security and your product designs.

About Allegro

Allegro Software Development Corporation is a premier provider of embedded Internet solutions 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