FOR IMMEDIATE RELEASE

Allegro's Integrated Embedded Device Security Suite Enabled with NSA Suite B Cryptography

Allegro Delivers Standards-based Suite B Cryptography for Embedded Systems

SAN FRANCISCO, CA and BOXBOROUGH, MA – February 27, 2012 – Allegro, a leading supplier of Internet and security software for embedded systems, today at the RSA® Conference 2012 in San Francisco, CA, announced the availability of Suite B cryptography with their Integrated Embedded Device Security Suite. Suite B is a collection of unclassified NSA specified algorithms for bulk-data encryption, hashing, creating digital signatures, and key exchange to improve secure information exchange within federal, state and local governments in addition to coalition partners. Allegro's Suite B solution is specifically engineered for resource sensitive embedded environments and independently developed by US citizens meeting all Free From Foreign Influence (FFFI) requirements. Pre-integrated with RomPager Secure and RomWebClient Secure SSL/TLS server, Allegro's Suite B solution is small, fast, speeds development and reduces time to market.

What is Suite B

In 2005, the National Security Agency (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, publicly available standard for cryptography that defines algorithms and strengths for encryption, hashing, calculating digital signatures and key exchange.

Usage	Algorithm	Classification Level	
		Secret	Top Secret
Encryption	AES-GCM	128-bit key	256-bit key
Hashing	SHA-xxx	256-bit digest	384-bit digest
Digital Signatures	ECDSA	256-bit key	384-bit key
Key Exchange	ECDH	256-bit key	384-bit key

Per CNSSP-15 (Committee on National Security Systems Policy 15)

With Suite B, NSA specified only algorithms not protocols. The National Institute of Standards and Technology (NIST) and NSA have worked to integrated the use of Suite B cryptography into IETF standards. The result, specific RFCs that utilize Suite B have been adopted for several communications protocols including SSL/TLS (RFC 5430).

Suite B and Embedded Systems

Embedded systems are prolific in virtually all industries. The rapid adoption and deployment of modern communication technologies has enabled unthought-of applications. With it, comes the need for embedded device security. Any network-enabled device must be considered as a potential target for malicious intent. The important and unprecedented need for secure communications has never been higher.

Since being announced by the NSA in 2005 and subsequent adoption into IETF standards, the use of Suite B in both commercial and military applications has seen great success. Due to the underlying use of elliptical curve cryptography, Suite B has shown performance enhancements over other cryptography in both enterprise and embedded environments, which has increased the rate of adoption. Once thought to be for use in military deployments, Suite B can now be found in embedded systems for consumer electronics, financial trading systems, and enterprise networking solutions, as well.

The ultimate security level of any product is determined by the quality and proper implementation of the underlying cryptography. Allegro's Suite B solution is pre-integrated with RomPager Secure and RomWebClient Secure SSL/TLS server and client for use in resource sensitive embedded device application areas such as: Payment Card Industry (PCI), Healthcare and Health Insurance Portability and Accounting Act (HIPAA), Financial, and others.

"Network traffic from embedded devices connected to the Internet is projected to experience exponential growth in the coming years. Enabling Suite B cryptography in globally recognized communications protocols like SSL/TLS for resource sensitive embedded systems is a natural extension of Allegro's expertise" says Bob Van Andel, President of Allegro.

Allegro's Suite B solution is available now and delivered as ANSI-C source. Stop by Allegro's booth at the RSA Conference 2012, Booth #240 to discuss your embedded device security needs.

About Allegro

Allegro Software Development Corporation is a premier provider of embedded Internet solutions with an emphasis on device management and security and UPnP-DLNA networking technologies. Since 1996, Allegro has been a force in the evolution of device management solutions with its RomPager embedded web server toolkit. 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.

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