Allegro Software Expands FIPS 140-2 Support For IoT Applications Needing Validated Cryptography in Military, Medical and Federal Environments

FIPS 140-2 validated cryptography specifically engineered for Military, Medical and Federal IoT applications

BOXBOROUGH, MA August 1, 2017 – Allegro Software, a leading supplier of Internet component software for the Internet of Things (IoT), today announced it has earned FIPS 140-2 level 1 validation on four additional platforms with the Allegro Cryptography Engine, ACE™ from the U.S. government's National Institute of Standards and Technology (NIST). This marks the culmination of Allegro's largest validation effort to date with the U.S. government. Specifically engineered for the rigors of resource constrained IoT computing environments, ACE enables manufacturers to leverage standards-based cryptography in IoT environments with ease. ACE is ideally suited for use in embedded systems and IoT applications in the military, energy, medical and communications industries.

ACE AND FIPS 140-2 VALIDATION

Since the passage of the Federal Information Security Management Act (FISMA), Federal agencies and contractors have a mandate to maintain greater control over data and information systems as a whole. U.S. Federal agencies that use cryptographic-based systems to protect sensitive information in military, medical, telecommunications, IoT applications and other IT-related products must use FIPS 140-2 validated modules to meet these security requirements. FIPS 140-2 validation is also required by national agencies in Canada and is recognized in Europe and Australia.

ACE is one of the smallest, fastest, and most comprehensive FIPS 140-2 validated software modules on the market for IoT applications. Specifically engineered for the critical cryptographic computing needs of IoT applications, ACE is easily used, highly portable, and uniquely configurable to operate in the toughest resource sensitive environments. With a rich software API, IoT developers can easily perform bulk encryption and decryption, message digests, digital signature creation and validation, along with key generation and exchange. ACE also includes a platform independent implementation of NSA defined Suite B cryptographic algorithms as well as other FIPS approved algorithms. The FIPS approved algorithms are listed on the NIST CAVP sites along with the final validation designation on the NIST CVMP site.

To further aid developers implementing IoT security, ACE is pre-integrated with the full suite of Allegro AE IoT connectivity and security toolkits including RomSTL (TLS 1.2), RomCert (SCEP and OCSP), RomSShell AE (SSH), RomPager AE (web server) and RomWebClient AE (web client).

IoT SECURITY AND HARDWARE CRYPTOGRAPHIC ACCELERATION

IoT applications are engineered from the ground up for resource sensitive execution environments. Typically, the primary driving factor in these applications aims to deliver the highest value IoT product at the lowest cost. Unfortunately, implementing cryptographic security protocols in any environment is resource intensive in CPU, RAM and ROM which IoT devices often find difficult to support. To help address these needs, silicon manufacturers augment their chipsets with specifically engineered cryptographic engines to off-load resource intensive cryptographic calculations. Two of Allegro's most recent FIPS 140-2 validated ACE modules have the flexibility to utilize on-board cryptographic acceleration when available. This greatly increases throughput while reducing the demand for CPU, RAM and ROM. These validations have been configured to support the on-board cryptographic acceleration from Intel (AES-NI) in addition to hardware based entropy to meet the latest NIST Implementation Guidance for FIPS modules.

"The need is critical for advanced security in IoT devices," says Bob Van Andel, President of Allegro. "With the culmination of Allegro's latest validations, IoT developers have access to the most essential component of seven key elements needed for proactive IoT security – highly portable, reliable, FIPS 140-2 validated cryptography." ACE is delivered as an ANSI-C source code toolkit and is available now. To learn more about the "7 Key Elements for Proactive IoT Security" visit our website: https://www.allegrosoft.com/secure-iot . For additional information on Allegro Software and the full suite of Allegro AE IoT connectivity and security toolkits, visit our website: https://www.allegrosoft.com/iot-device-cybersecurity .

ABOUT ALLEGRO

Allegro Software Development Corporation is a premier provider of embedded Internet software components with an emphasis on industry-leading device management, embedded device security, UPnP-DLNA networking, and the Internet of Things. Since 1996, Allegro has been on the forefront of leading the evolution of secure device management solutions with its RomPager embedded web server and security 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.

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