Allegro Cryptography Engine ACE™

Advanced Edition Embedded FIPS Cryptography

ACE Benefits

- Decrease time to market by leveraging field-proven embedded security solutions
- Highly portable via field-proven abstraction layer
- FIPS-approved algorithms
- Full Power-On Self-Test support
- Independently developed by US citizens to meet Free From Foreign Influence (FFFI) requirements
- GPL free
- Simple development model
- Small RAM/ROM footprint
- ANSI-C source distribution
- Compilation switches for size and speed trade-offs

The Allegro Cryptography Engine (ACE) is a platform-independent, high performance, resource-sensitive, FIPS cryptography engine certified by NIST and specifically engineered for the rigors of embedded computing. ACE enables OEM manufacturers to add sophisticated encryption technology to their designs and dramatically speed the development cycle. ACE is designed to meet the criteria necessary for FIPS 140-2 validation.

Embedded systems appear in virtually all industries, with the capability to communicate independently. The rapid adoption and deployment of modern communication technologies is enabling new applications in healthcare, military applications, energy management, consumer devices, and many other areas. With these capabilities comes the need for embedded device security. Any network-enabled device must be considered as a potential target for malicious intent. Encryption of sensitive data while in motion or at rest is a key component to thwarting malicious attacks and reducing risk.

Allegro Cryptography Engine (ACE)

ACE is a cryptographic library module for embedded computing systems that provides software implementations of FIPS-approved algorithms for the calculation of message digests, digital signature creation and verification, bulk encryption and decryption, key generation, and key exchange. Used standalone or pre-integrated with other Allegro toolkits, ACE provides government validated implementations of sophisticated encryption algorithms for use in embedded systems.

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 standard for cryptography that defines algorithms and strengths for encryption, hashing, calculating digital signatures, and key exchange. ACE includes a platform independent validated implementation of the NSA Suite B-defined suite of cryptographic algorithms, as well as validated implementations of other FIPS-approved cryptography algorithms. ACE is delivered as ANSI C source.

ACE can be used standalone or pre-integrated with Allegro's suite of embedded device security protocols such as TLS and SSH in addition to the full RomPager AE suite of Internet software for embedded devices that include Web Services using HTTP, XML, and SOAP.

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts
01719

+1 (978) 264-6600
www.allegrosoft.com

Allegro

Rich Algorithm Support

ACE (FIPS Mode)

Digital Signature Algorithms

- RSA (FIPS 186-3) Key lengths: 2048, 3072
- DSA (FIPS 186-3) Key lengths: 1024, 2048, 3072
- ECDSA (FIPS 186-3) Curves: NIST P-192, P-224, P-256, P-384, P-521

Symmetric Keys

- AES Key lengths: 128, 192, 256
- AES-GCM Key lengths: 128, 192, 256
- AES-CCM Key lengths: 128, 192, 256
- AES-XTS Key lengths: 128, 256
- TripleDES

Hash Functions

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Message Authentication

- HMAC-SHA-1
- HMAC-SHA-224
- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512
- AES-GMAC Keylengths: 128, 192, 256
- AES-CMAC Keylengths: 128, 192, 256

Key Agreement

- DH (NIST SP 800-56A)
- ECDH Curves: NIST P-192, P-224, P-256, P-384, P-521

Random Number Generator

- DRBG (NIST SP 800-90A)

ACE (Non-FIPS Mode)

All of the above in addition to the following:

Digital Signature Algorithms

- RSA: arbitrary key lengths 512 to 3072
- DSA: arbitrary key lengths 512 to 3072

Symmetric Keys

- DES
- RC4

Hash Functions

- MD2
- MD4
- MD5

Message Authentication

- HMAC-MD5

Allegro

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts 01719

Phone: +1 (978) 264-6600
Fax: +1 (978) 266-2839
www.allegrosoft.com