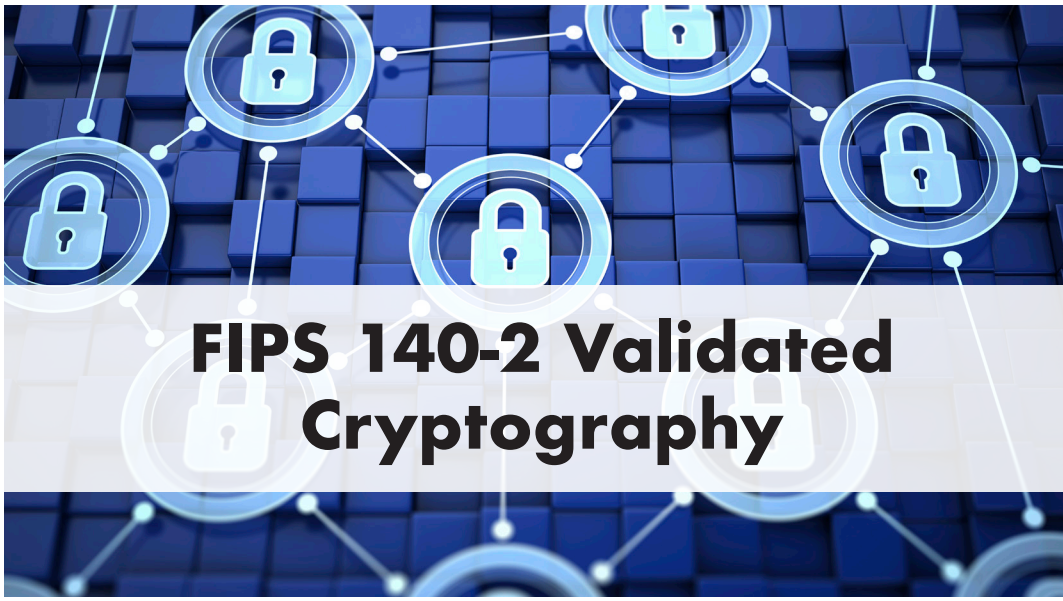
Allegro Cryptography Engine ACE™

ACE Benefits

- Improve time to market by leveraging field-proven embedded solutions
- Highly portable via field-proven abstraction layer
- NIST Validation of FIPS 140-2 algorithms
- Full Power-On Self-Test support
- NSA Suite B cryptography
- GPL-Free code protects your intellectual property
- Independently developed by US citizens to meet Free From Foreign Influence (FFFI) requirements
- Simple development model
- Small RAM/ROM footprint
- ANSI-C source code distribution
- Support for hardware acceleration
- Compilation switches for size and speed trade-offs
- Pre-integrated with the Allegro EdgeAgent Suite

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts
01719

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



FIPS 140-2 Validated Cryptography

The rapid adoption and deployment of modern communication technologies is enabling new applications in healthcare, military applications, energy management, and consumer devices that are often referred to as the Internet of Things (IoT). With the inherent threats that come with connectivity, manufacturers are putting pressure on developers to deploy strong security, authentication, and encryption technologies to mitigate the risk of potential vulnerabilities in their designs.

Allegro Cryptography Engine (ACE)

ACE is a core cryptography engine that provides developers with the resources to employ a "defense in depth" strategy with multiple layers of security services. ACE is a platform-independent, high performance, resource-sensitive, cryptography engine validated by NIST and specifically engineered for the rigors of embedded computing. With ACE, manufacturers can add standards-based cryptography to resource sensitive embedded systems quickly, easily, and reliably while decreasing time to market.

When deployed in your application, ACE is a cryptographic library module 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
- Key exchange

Used standalone or pre-integrated with the Allegro EdgeAgent Suite, ACE provides government validated implementations of sophisticated encryption algorithms for use in your application.

Allegro

FIPS Validation Including Suite B

The ACE implementions of FIPS 140-2 algorithms have been validated by NIST on multiple platforms since 2013. ACE allows your device to meet the criteria necessary for FIPS 140-2 validation.

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, the Suite B algorithms are globally recognized as an advanced standard for cryptography used 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 140-2 cryptography algorithms.

Pre-Integrated Solutions

The Allegro EdgeConnect Suite is pre-integrated with the ACE cryptography module, enabling manufacturers to add standards-based cryptography to resource-sensitive environments easily and reliably. The Allegro EdgeConnect IoT Suite delivers field-proven standards-based protocol components to:

- Securely serve Web pages, images or applets via TLS
- Manage security certificates
- Securely retrieve files from resources on the Web via TLS
- Quickly create a secure and robust Command Line Interface(CLI)
- Exchange XML, SOAP, and JSON messaging with enterprise or cloud-based computing and storage resources

Speed Development Efforts

ACE is a ready-made, pre-optimized and exhaustively tested cryptography solution that frees your in-house development team to focus on product differentiation: the functionality that makes your project unique and adds value to your target customer. ACE gives your development team the freedom to develop proprietary systems while giving the ability to use commercially available software components of your choice.

Platform Independent

ACE, in addition to the entire Allegro EdgeAgent Suite, is CPU-architecture and platform independent. ACE relies on our field-proven abstraction layer and can be utilized in the most resource sensitive environments, including those without an RTOS.

Securing Data In Motion

Many IoT applications collect and correlate valuable sensitive information at the edge of the Internet and routinely transmit it to servers in the cloud securely. TLS and DTLS are seen as the "defacto" standard for keeping data secure when communicating with servers in the cloud. Allegro's RomSTL, embedded TLS and DTLS toolkit, tightly integrates FIPS validated cryptography with a standards based, embedded implementation of TLS/DTLS to keep your data secure while in motion. RomSTL can additionally make use of ACE's support of Suite B algorithms with TLS and DTLS.

Secure Shell (SSH) encrypts communications between hosts over an insecure network and is another method employed for securing data in motion. Allegro's RomSShell is a fast, full featured SSH client/server solution designed for resource sensitive environments. RomSShell is pre-integrated with ACE and includes support for NSA Suite B algorithms so your product can securely link hosts in civilian applications as well as government based deployments.

Securing Data At Rest

Before offloading data to cloud based applications, any sensitive information stored by IoT devices faces numerous threats and risks of unintentional exposure. Adding data encryption to the transmission process has been the traditional method for reducing this risk. However, simply encrypting data transmissions doesn't fully address many of the threats aimed at recovering small segments of data or potentially an entire collection of data stored on an IoT device. The Allegro EdgeSecure Suite provides IoT design engineers the ability to proactively address the threat surface created when storing sensitive data on persistent media. Rather than encrypting data at a volume or drive level where exposing a single set of keys potentially compromises a significant amount of sensitive data, Allegro's secure data-at-rest solution encrypts information at the file level and makes use of FIPS 140-2 validated cryptography.

GPL-Free Code

ACE is delivered as ANSI C source code. The total cost of ownership for ACE is less expensive than "free" open source code, especially when considering maintenance engineering, testing and support costs are taken into consideration. ACE contains no GPL code, and you can be confident your intellectual property won't accidently become public domain due to "GPL contamination", one of the risks of using open source software.

Allegro

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts 01719

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

Rich Algorithm Support

ACE (FIPS Mode)

Digital Signature Algorithms

- RSA (FIPS 186-4) Key lengths: 2048, 3072
  Padding Modes: ANSI X9.31, PKCS #1v1.5, PSS
- DSA (FIPS 186-4) Key lengths: 2048, 3072
- ECDSA (FIPS 186-4) Curves: NIST P-224, P-256, P-384, P-521

Symmetric Keys

- AES Key lengths: 128, 192, 256
  Modes: ECB, CBC, CTR, CFB1, CFB8, CFB128, OFB, CCM
- AES-GCM Key lengths: 128, 192, 256
- AES-XTS Key lengths: 128, 256
- TripleDES
  Modes: ECB, CBC, CFB1, CFB8, CFB64, OFB

Hash Functions

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512
- SHA3-224
- SHA3-256
- SHA3-384
- SHA3-512

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-224, P-256, P-384, P-521

Key Derivation

- Password-Based Key Derivation Function 2 (PBKDF2)
- TLS Key Derivation Functions

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: key lengths 1024, 2048, 3072
- DSA: key lengths 1024, 2048, 3072

Symmetric Keys

- DES
- RC4

Hash Functions

- MD2
- MD4
- MD5

Message Authentication

- HMAC-MD5

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts 01719

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

Allegro Software

Since 1996, Allegro has been providing superior products to the embedded industry. Many companies have discovered the advantages of creating devices that are active members of the Internet of Things (IoT) and work with Allegro to meet their networking connectivity needs. Allegro customers include many of the leading developers of computer systems, networking equipment and IoT devices such as Arris, Baxter Healthcare, Bose, Brocade Networks, Cisco, D-Link, General Dynamics, Harman International, HP, IBM, Kronos, Microsoft, Motorola, Nielsen, OpenTV, ResMed, Siemens, Sumitomo, Xerox and Yamaha. These customers, and others, have found that Allegro's connectivity and security toolkits are well suited for embedding in devices like printers, routers, automobiles, medical equipment, UPS systems, enterprise phone systems, set-top boxes and networked digital media products. With over 300 design wins and over 250 million deployed devices worldwide, Allegro delivers robust and field proven Internet software for your embedded device. Visit our website to learn more:

www.allegrosoft.com

SCAN TO

LEARN MORE

Allegro

Allegro Software Development Corporation
1740 Massachusetts Avenue
Boxborough, Massachusetts 01719

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