ALLEGRO CRYPTOGRAPHY ENGINE - ACE™

FIPS 140 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 complete Allego EdgeAgent suite, ACE provides government validated implementations of sophisticated encryption algorithms for use in your application.

ACE BENEFITS

- Improve time to market by leveraging field-proven embedded solutions
- Highly portable with a field-proven abstraction layer
- NIST Validation of FIPS 140 algorithms
- Full Power-On Self-Test support
- CNSA cryptography
- GPL-Free code protects your intellectual property
- Simple development model
- Independently developed by US citizens to meet Free From Foreign Influence (FFFI) requirements
- Small RAM/ROM footprint
- ANSI-C source code (C99) distribution
- Support for hardware cryptographic acceleration
- Compilation switches for size and speed trade-offs
- Pre-integrated with Allegro's advanced device management and communication toolkits

FIPS VALIDATION INCLUDING CNSA CRYPTOGRAPHY

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

In 2018, the NSA replaced Suite B algorithms with the Commercial National Security Algorithm Suite (CNSA 1.0). The NSA widely promotes this set of cryptographic algorithms, which serve as the cryptographic base to protect National Security Systems information up to the Top Secret level. In September 2022, the NSA announced CNSA 2.0, which incorporates the first set of recommendations to support post-quantum cryptography.

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 CNSA 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 CNSA algorithms so your product can securely link hosts together in civilian applications as well as government based deployments.

PRE-INTEGRATED SOLUTIONS

The Allegro EdgeAgent 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 EdgeAgent product toolkits deliver 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 Inter face(CLI)
- Exchange XML, SOAP, or JSON messaging with enterprise or cloud based computing and storage resources

SECURING DATA AT REST

Before offloading data to cloud based applications, any sensitive information stored by IoT devices face 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 EdgeAgent and ACE product suites provide 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 validated cryptography.

SPEED DEVELOPMENT EFFORTS

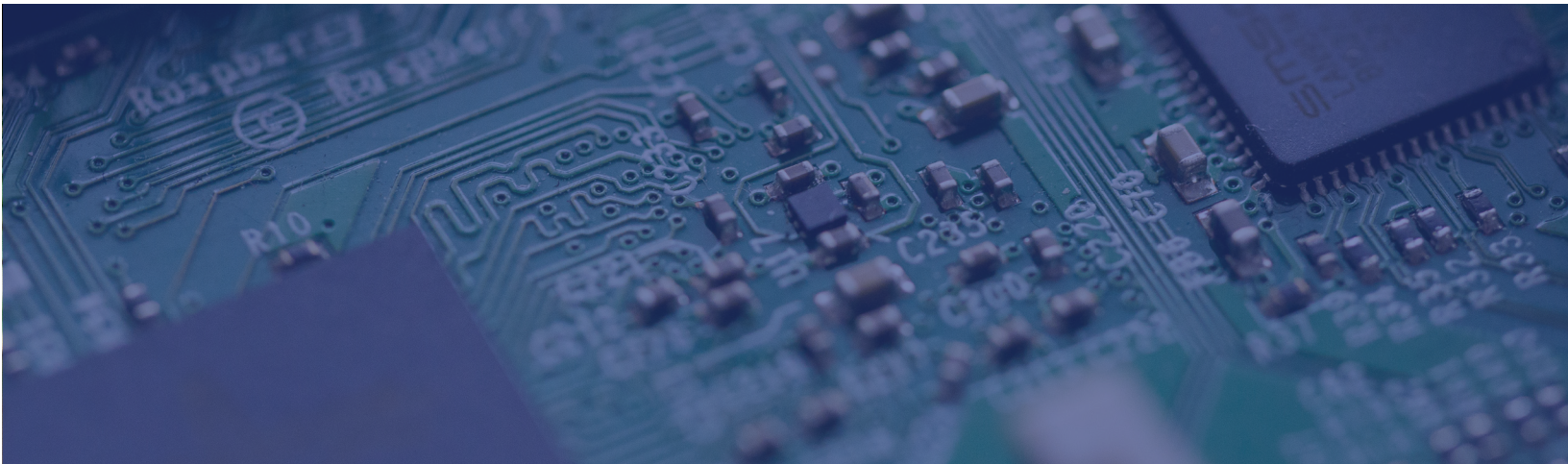
ACE is a ready-made, pre-optimized and exhaustively tested cryptography solution that frees your in-house development team to focus on product differentiation: the functionality that makes your project unique and adds value to your target customer. ACE gives your development team the freedom to develop 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 product suite, is CPU architecture and platform independent. ACE relies on our fieldproven abstraction layer and can be utilized in the most resource sensitive environments, including those without an RTOS.

GPL-FREE CODE

ACE is delivered as ANSI C source (C99) 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.



Rich Algorithm Support

ACE (FIPS MODE)

Digital Signature Algorithms

- RSA (FIPS 186-4) Key lengths: 1024 (verification only), 2048, 3072, 4096 (generation and verification)
  Padding Modes: ANSI X9.31, PSS
- ECDSA (FIPS 186-4) Curves: NIST P-224, P-256, P-384, P-521 (generation and verification), NIST P-192 (verification only)

Symmetric

- AES Key lengths: 128, 192, 256 Modes: ECB, CBC, CTR, CFB1, CFB8, CFB128, OFB, FF1 (format preserving encryption)
- AES-GCM Key lengths: 128, 192, 256
- AES-CCM Key lengths: 128, 192, 256
- AES-XTS Key lengths: 128, 256

Hash Funnctions

- SHA-1
- SHA2-224
- SHA2-256
- SHA2-384
- SHA2-512
- SHA3-224
- SHA3-256
- SHA3-384
- SHA3-512
- SHAKE-128
- SHAKE-256

Key Wrapping

- AES Key lengths: 128, 192, 256 Modes: KW, KWP
- AES-ECB with HMAC Key lengths: 128, 192, 256

Message Authentication

- HMAC-SHA-1
- HMAC-SHA2-224, HMAC-SHA3-224
- HMAC-SHA2-256, HMAC-SHA3-256
- HMAC-SHA2-384, HMAC-SHA3-384
- HMAC-SHA2-512, HMAC-SHA3-512
- AES-GMAC Key lengths: 128, 192, 256
- AES-CMAC Key lengths: 128, 192, 256

Key Agreement

- KAS-IFC-SSC: MODP 2048, 3072
- KAS-FFC-SSC: MODP 2048, 3072
- KAS-ECC-SSC: NIST P-224, P-256, P-384, P-521

Key Derivation

- Password-Based Key Derivation Function 2 (PBKDF2)
- TLS Key Derivation Functions:TLS v1.2, v1.3
- SSH Key Derivation Function: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512
- HMAC Key Derivation Function (HKDF): SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512

Random Number Generator

- DRBG (NIST SP 800-90A): SHA2-224, SHA2-256, SHA2-384, SHA2-512

ACE (Non-FIPS Mode)

All of the above in addition to the following:

Hash Functions

- MD2, MD4, MD5

Key Wrapping

- PKCS#8, PKCS#1.5 RSA, RSA with 1024 bit keys

Key Generation

- ECDSA with Curve P-192

Message Authentication

- HMAC-MD5, Poly1305

Digital Signatures

- RSA 1024-bit, SHA1, RC2, RC4, ChaCha20/Poly1305, DES, 3DES, DSA, RSA with PKCS #1.5

Since 1996, Allegro has been providing superior products to the embedded industry. Many companies have discovered the advantages of connecting devices to the Internet and working with Allegro to meet their networking needs. Allegro customers include many of the leading developers of computer systems and networking equipment 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 the Allegro 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 275 million deployed devices worldwide, Allegro delivers robust and field proven Internet software for your embedded device. Visit **www.allegrosoft.com** or scan the QR code to learn more.