

# Cryptographic Development Kits

**ISC cryptographic toolkits are used in a wide variety of mission-critical military, intelligence, financial, and industrial applications. ISC support personnel can assist with the rapid integration of confidentiality and authentication schemes into any type of application.**

## OVERVIEW

ISC CDKs are cost-effective, flexible collections of linkable modules that permit developers to easily incorporate conventional and public key cryptographic technology into their applications. These commercially supported libraries reduce the cost of developing security-enabled applications employing encryption, digital signatures, message authentication, and standard credential management functions.

ISC CDKs include implementations of all standard cryptographic algorithms, including:

- **symmetric ciphers:** AES, TDES/DES, RC2, RC4, CAST-128, Skipjack, *etc.*
- **message authentication codes:** SHA-1, SHA-256/384/512, MD2, MD5, RIPEMD-160, HMAC, *etc.*
- **public key systems:** RSA, discrete log based systems (e.g., ElGamal), and ECC
- **signature schemes:** RSA, DSA, ECDSA
- **key agreement/key exchange protocols:** Diffie-Hellman, ECDH, ECMQV, KEA, *etc.*
- **PDU handling:** creation and parsing of ASN.1 encoded certificates, certificate chains, S/MIME CMS, PKCS#12 and #15 PDUs, *etc.*

ISC CDKs comply with all relevant Federal Information Processing Standards (FIPS) as well as with ANSI, IEEE, ISO, IETF, and PKCS Standards (details on reverse side.)

Whether developing software for internal use or OEM products for resale, ISC provides the trusted security tools and expertise needed to rapidly complete and deliver critical projects.

## TECHNICAL SUPPORT

ISC provides e-mail and telephone support to rapidly resolve any issues developers may have with scheme implementation or library integration. Developers won't waste time hoping for a response on a mailing list.

## RAPID DEVELOPMENT

ISC CDKs allow developers and integrators to build cryptographic functions into a wide range of solutions intended for internal corporate use or resale. The CDK APIs are well documented and easy to use, allowing developers to quickly build security-enabled applications in any development environment.

Each CDK includes a sample test project complete with commented source code illustrating the use of functions in the library and containing (mainly NIST-supplied) known vector tests for all supplied FIPS-approved algorithms. This test suite can be recompiled and executed in order to verify the proper operation of the cryptographic engine on the target platform.

With ISC CDKs and ISC support services security-enabling your software application shouldn't impact its delivery schedule.

## CONSULTING SERVICES

Taking advantage of ISC's expertise can provide you with a distinct competitive advantage. Not only can we help ensure that security in your application is implemented correctly and represents 'best practices' in the field, but you also gain the cachet of using the same cryptographic libraries upon which many U.S. military and intelligence agencies depend.

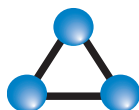
ISC offers consulting and integration services. If you are unsure of the optimal combination of cryptographic algorithms to use in an application or device, confused by HIPAA or other state and/or Federal security requirements, or in need of programming assistance or a pre-release security review, ISC's technical staff is available for consultations on-site, by telephone, and via e-mail.

## ELLIPTIC CURVES

NSA Suite B curves and protocols are fully supported, as are most NIST, ANSI, and Brainpool curves. State-of-the-art ECDH and ECDSA implementations, along with support for ECC X.509 certificates, S/MIME ECC CMS, and ECC TLS afford your applications with immediate compliance with NSA's recommendations for the protection of sensitive and classified information up to the SECRET level.

## ADDITIONAL DETAILS

- NSA Suite B support fully complies with NSA's *Suite B Implementer's Guide to NIST SP800-56A*
- X.509v3 certificate and CRL handling (RFC2459, RFC3279, RFC5280, RFC5480, NIST SP 800-15)
- S/MIME v3 CMS functions for PDU creation and parsing (RFC3278, RFC3370, RFC3394, RFC3565, RFC3851, RFC5652)
- PKCS#7/8/10/12 PDU creation and parsing
- key derivation functions for PKCS#5 PBE and various ANSI and PKCS#1/3/5/8 (RFC2313-2315) padding, encoding, and decoding functions
- AES key wrapping (RFC3394)
- pseudo-random number generation, primality testing, and routines for low-level modular exponentiation and other high-precision arithmetic operations (in rings of integers and finite fields and on elliptic curves)
- SSL/TLS client support
- Windows device driver support



**Information Security**  
CORPORATION

+1 847 405-0500  
sales@infosecorp.com  
<http://www.infosecorp.com>

# Cryptographic Development Kits

## LICENSING TERMS

A low-cost, fixed-fee, "Get Started" package includes a CDK library for one target platform and a two-seat developer license. Additional developer seats and platforms may be purchased at reduced cost.

Runtime fees, to be negotiated prior to the distribution of your application, depend on algorithm requirements and the number of anticipated users, but not on the type of application to be distributed.

Contact ISC for additional licensing information, standard licensing agreements and fee schedules.

## PLATFORM AVAILABILITY

ISC CDKs are available on:

- Windows NT/2000/XP/2003/Vista/2008/7 (i86)
- Windows Mobile (ARM)
- Windows Embedded (i86)
- Mac OS X (PowerPC and i86)
- iPhone (ARM)
- Solaris 8,9,10 (SPARC and i86)
- HP-UX 10.x/11.0 (PA-RISC and IA64)
- IBM AIX 4, 5, 6 (PowerPC)
- RHEL, SUSE, and other Linux distros (i86 and IA64)
- SGI IRIX 6.x (MIPS)
- Compaq Tru64 (Alpha)
- OpenVMS/AXP (Alpha)
- Cray UNICOS, and others

The high performance C++ code (with or without assembly language optimizations) can be readily ported to additional platforms upon request while maintaining FIPS 140-2 compliance.

On Windows, CDKs are available as DLLs, static libraries, and COM objects. UNIX libraries using a variety of different linkage conventions can be provided. Java applications are supported via JNI.

## STANDARDS COMPLIANCE

The cryptographic primitives that can be included in a custom CDK comply with the following Federal and industry standards:

Algorithms Supported	Relevant Standards and Other References	NIST Certificate
RSA	FIPS 186-3; ANSI X9.31-1998; RFC2437 (PKCS#1v2.0), RFC3447 (PKCS#1v2.1)	VA
DSA	FIPS 186-3; ANSI X9.30-1997	#65
ECDSA	FIPS 186-3; ANSI X9.62-1998; IEEE 1363-2000	VA
DH	RFC2631; ANSI X9.42-1998; IEEE 1363-2000	
ECDH / ECMQV	ANSI X9.63; IEEE 1363-2000; NIST SP-800-56A	
AES	FIPS 197; NIST SP-800-38A; NIST SP-800-38C; NIST SP-800-38B; CNSS Policy No. 15; RFC3565	#9
DES	FIPS 46-3; ANSI X3.92	#171
TDES	FIPS 46-3; ANSI X9.52-1998; NIST SP-800-38A; NIST SP 800-20; NIST SP 800-67	#115
DESX	(analysis by J. Kilian and P. Rogaway)	
Skipjack/EES	FIPS 185; NIST/NSA specification	#9
RC2	RFC3217; RFC2268	
RC4	RFC2246 (SSL/TLS); "Arcfour" internet-draft	
SHA-1	FIPS 180-3; ANSI X9.30 Part 2; ISO/IEC 10118-3:1998	#100
SHA-224/256/384/512	FIPS 180-3; RFC3874	
HMAC-SHA-1	FIPS 198-1; RFC2104; ANSI X9.71	#100, VA
HMAC-MD5	RFC2104; ANSI X9.71	
MD2 / MD5	RFC1319; RFC1321	
PRNG	FIPS 186-2 Appendix 3.1; FIPS 140-2 Annex C; NIST SP 800-90; NIST SP 800-22	
Password Generation	FIPS 181	

## FIPS 140 INFORMATION

CDK 7.0 is FIPS 140-2 compliant and was awarded FIPS 140-1 Validation Certificate No. 347. All algorithms in the above list that have been awarded NIST Algorithm Certificates, as well as those marked VA for "vendor affirmed", are approved for use in FIPS compliant applications. The module is. Contact ISC for details.



## EXPORT INFORMATION

Applications utilizing ISC CDKs may, with proper notification to the BIS, be freely exported to all but a handful of embargoed countries and denied parties under License Exception ENC:

ECCN 5D002; CCATS: G026249.

While ISC can provide guidance, you should consult your own legal representatives prior to exporting a security-enabled application to ensure compliance with Federal Law.