

Features

- Ciphers
 - AES
 - DES/3DES
 - SNOW 3G
 - SEED
- Modes (supported by all block ciphers)
 - ECB
 - CBC
 - CFB
 - CTR
 - OFB
- Hashes
 - MD5 and SHA-1 through SHA-512
- MACs
 - CMAC
 - HMAC
 - XCBC
- Certified under the U.S. National Institute of Standards and Technology CAVP (Cryptographic Algorithm Validation Program)
- Library is targeted at common security protocols including:
 - VPN – IPsec, SRTP and SSL
 - Wi-Fi, WiMAX, 3GPP, UMTS and LTE
 - DRM and Conditional Access
 - Government and military including Suite B
- Support for blocking and non-blocking modes
 - Adaptable to hardware core offload
- OS Agnostic
 - Written for portability
 - Target OS – Linux, Windows Mobile, VxWorks, WindRiver, iTRON
 - Licensed as C source code

The ESS-01 is part of the Ellipsys Security Architecture (ESA) which offers a comprehensive set of security software for embedded applications. The ESS-01 features a complete library of symmetric cryptography algorithms such as AES, 3DES, hashing functions SHA-1, SHA-2 and keyed hashes such as HMAC/SHA-1.

The library supports substitution of hardware for software modules to permit designers to choose when hardware offload is required or to use an all software solution if the computational abilities of the processor are sufficient for the required throughput. Release 3.1 of the library offers additional algorithms, reduced stack size and enhanced portability.

General Description

The ESS-01 is a part of the Ellipsys Security Architecture offered by Elliptic. By leveraging the fully proven, efficient implementation of symmetric cryptography available in the ESA, developers can speed time to market, meet their overall performance goals and avoid pitfalls that might open up security holes.

Release 3.1 of the library offers additional symmetric algorithms, reduced stack size and enhanced portability. Elliptic will continue to support customers who have licensed Ellipsys Release 2.1 for one year from the release date of Ellipsys 3.1.

Class	Function	Notes	Standard(s)	
Symmetric Ciphers	AES DES 3DES SEED CAMELLIA CAST5 SNOW 3G	Ciphers are implemented with ECB interfaces only. Wrappers are required to achieve chaining modes UEA2	FIPS-197 FIPS 46-2 FIPS 46-3 TTAS.KO-12.0004/R1 (SEED) RFC 3713 (Camellia) RFC 2144 (CAST5) TS 35.201 V7.0.0 (2007-06)	
	CBC CFB OFB CTR	Basic Chaining Modes		
	XTS	XTS (XEX) modes	IEEE 1619	
	Key Wrap	NIST Key Wrap	NIST – November 2001 RFC 3394	
	CMAC	NIST CMAC	SP-800-38B	
	XCBC	XCBC MAC Support 1 and 3 key mode	1 Key FFC 3566	
	CCM GCM	Encryption and authentication mode	SP-800-38C SP-800-38D	
	One-Way Hash Functions	MD5 SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SNOW 3G	Hash algorithms provide hash only UIA2	RFC 1321 FIPS-180-3 TS 35.201 V7.0.0 (2007-06)
		HMAC	Hash based MAC	FIPS-198
		RNG/PRNG	System PRNG (/dev/urandom) ARC4	ARC4 can also be used as a cipher

General Description cont'

The ESS-01 is designed as a portable library capable of targeting any of the embedded environments in common use today ranging from Linux, Windows Mobile, VwWorks, iTRON and WindRiver.

The library is also designed to support hardware offload when available as many microcontroller and NPUs now have embedded crypto cores which can greatly accelerate cryptographic throughput.

Coding Standards and Examples

Elliptic coding standards were developed to ensure customers in demanding markets such as automotive and medical applications can be comfortable in using the library. The test harness used includes FIPS test vectors used for Elliptic's semiconductor IP cores which ensures that the cores and software library will interoperate. Testing is also under the rigorous testing conducted by a third party testing laboratory which is required for certification per the NIST CAVP validation.

Two sample implementations are offered on Elliptic's web site. One sample illustrates how a hash algorithm such as SHA-1 and the other for a cryptographic function such as AES.

Ellipsys Security Architecture

The Ellipsys Security Architecture pictured below consists of five distinct products encompassing symmetric and asymmetric cryptography primitives, secure boot, Linux IPsec and DTCP stack.

The architecture offers a well defined, uniform API blending industry standard PKCS#11 with Ellipsys extensions in support of third party applications software. Customers can configure Ellipsys and choose between hardware and software security primitives and can implement platform security elements such as secure boot and key management.

When used with Elliptic hardware, a wide variety of use models are available supporting single crypto cores all the way up to sophisticated packet processing engines.

The Ellipsys Security Architecture can also be adapted to hardware offload in off the shelf processors with board support packages (BSPs) written either by Elliptic or by customers themselves.

Ellipsys is written to be highly portable and is licensed in C source code. The Ellipsys Security Architecture is illustrated below.

Ordering Information

- Offered in highly portable source code format, the ESS-01 is available for immediate licensing.
- There are two licensing options for the ESS-01. They are listed in the table below:

Order Code	Functionality
ESS-01-AES	AES cipher only (all modes)
ESS-01	All ciphers and hashes listed above

