

The ESS-01 is a member of the Ellipsys portfolio of middleware solutions. The library offers symmetric cryptography support for commonly used algorithms such as AES, DES/3DES, hashing functions such as SHA-1, SHA-256 and keyed hashes such as HMAC/SHA-1. The library is targeted at embedded systems which often have limited capabilities and as such efficient implementations are mandatory. The library supports substitution of hardware and 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 throughput required.

### Key Features:

- Ciphers
  - AES
  - DES/3DES
  - KASUMI
  - 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, UMTS and LTE
  - DRM and Conditional Access
  - Government and military including Suite B
  - Medical equipment
- 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

## Overview

The ESS-01 is a member of the Ellipsys family of middleware solutions available from Elliptic. By leveraging the fully proven, efficient implementation of symmetric cryptography available from Elliptic, developers can speed time to market, meet their overall performance goals and avoid pitfalls that might open up security holes. 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, VxWorks, 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. The table below outlines the ciphers and hashes supported and the standards that the algorithms comply with.

Class	Function	Notes	Standard(s)
Symmetric Ciphers	AES DES 3DES KASUMI 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 TS 35.202 V7.0.0 (2007-06) 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
HMAC		Hash based MAC	FIPS-198
RNG/PRNG		System PRNG (/dev/urandom) ARC4	ARC4 can also be used as a cipher  SSL

Offered in highly portable source code format, the ESS-01 is available for immediate licensing.

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. These examples can be found on the Elliptic web site at the following URL:

<http://www.ellipticsemi.com/middleware-hash-demo.php>

<http://www.ellipticsemi.com/middleware-cipher-demo.php>

For more information on the library and pricing please contact Elliptic at [info@ellipticsemi.com](mailto:info@ellipticsemi.com).

Elliptic  
62 Steacie Drive, Suite 201  
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456  
Fax: +1 613 254-7260  
Email: [info@ellipticsemi.com](mailto:info@ellipticsemi.com)