

The ESS-02 is the second member of the Ellipsys portfolio of middleware solutions. The library offers asymmetric cryptography support based upon the Public Key Cryptography Standard (PKCS) #1 reference implementation with support for both the v1.5 (IETF RFC2437) and v2.1 (IETF RFC3447) versions of the standard. Release 2.1 of the library now includes support for Elliptic Curve Cryptography (ECC) – specifically the prime field algorithms recommended by NIST and required for Suite B compliance. The library also 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:

- Supports all PKCS #1 asymmetric functions:
  - RSA Encryption and Decryption
  - RSA Key Generation
  - Signature and Verification
  - RSAES-OAEP (RSA Encryption Scheme - Optimal Asymmetric Encryption Padding)
  - ASN.1 encoding and decoding of keys and data
- Features support for prime field Elliptic Curve Cryptography
  - Supports all five of the NIST recommended prime field elliptic curves defined in NIST FIPS 186-2 (with changes) - Digital Signature Standard (DSS)
  - National Security Agency Suite B compliant 256-bits and 384-bits curves
  - Key sizes from 192 to 521 bits in lengths
  - Algorithms include EC-DSA, ECIES and Diffie-Hellman
- Library is targeted at common security protocols including:
  - VPN and e-commerce SSL
  - Wi-Fi and WiMAX
  - DRM
  - Government and military
  - Medical equipment
- Support for blocking and non-blocking modes
  - Adaptable to hardware core offload if required
- OS Agnostic
  - Written for portability
  - Target OS – Linux, Windows Mobile, VxWorks, WindRiver, iTRON
  - Licensed as C source code

## Overview

The ESS-02 is the second member of the Ellipsys family of middleware solutions available from Elliptic. By leveraging the fully proven, efficient implementation of asymmetric 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-02 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.

Release 2.1 of the ESS-02 has been enhanced to include prime field Elliptic Curve Cryptography capabilities. The library provides support for portions of ANSI X9.62 and X9.63 ECC algorithms. This includes all five of the NIST approved prime field elliptic curves ranging in size from 192 to 521 bits in length. The following capabilities are now available:

- Key Generation
- Key Removal
- Key Import and Export
- EC Digital Signature Algorithm – Signature and Verification
- ECIES – Elliptic Curve Integrated Encryption System, and
- EC-DH – Elliptic Curve Diffie-Hellman key agreement

The algorithms can be implemented entirely in software or can take advantage of hardware offload engines if they are available in the target system.

RSA Securities (<http://www.rsa.com>) worked with cryptographers and implementers in the early 1990s to create a series of Public Key Cryptography Standards (PKCS) to encourage the deployment of a public key infrastructure in the Internet and private networks. PKCS #1 in particular was a significant step forward and is used in standards ranging from SSL/TLS to WiMAX and Wi-Fi. The cross reference of the original RSA standard to the associated IETF and IEEE standards is offered in the table below:

Original RSA Standard	IETF	IEEE	Usage
PKCS #1 v1.5	RFC2437	P1363 - Draft Version 4	SSL v3.1 TLS v1.1 Wi-Fi
PKCS #1 v2.1	RFC3447	P1363-2000 P1363A-2004	WiMAX

Many proprietary designs such as smart cards, digital rights management (DRM) and secure USB key implementations leverage PKCS #1 for key generation and encryption since the reference design offers significant field experience and test suites.

The PKCS standards use ITU-T Abstract Syntax Notation One (ASN.1) to represent keys and certificates in a rigorous methodology. In PKCS #1, ASN.1 notation is used to represent the keys and data and they are often stored in structures using ASN.1. The ESS-02 library therefore includes functions to encode and decode ASN.1 keys and data to facilitate the exchange of information among different software processes.

High quality coding standards ensure customers in demanding markets such as automotive and medical applications in demanding markets such as automotive and medical applications can be comfortable in using the library. The test harness used includes test vectors used for Elliptic's semiconductor IP cores which ensures not only that the cores and software library will interoperate but that the library is tested to a uniform, rigorous quality level. Offered in binary format and optionally as source code should further optimization or porting be required, the ESS-02 is available for immediate licensing.

Sample code for the ESS-02 can be found on the Elliptic web site at the following URL:

<http://www.ellipticsemi.com/middleware-RSA-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)