

The WiMAX forum has introduced a security profile for mobile WiMAX based on the IEEE 802.16e-2005 standard. The profile implements a single AES-CCM algorithm to lower silicon cost and overall system complexity. The LLP-03 is derived from the silicon proven LLP-02 and is available for immediate licensing. Like the LLP-02, the core offers an inline processing engine which captures traffic, security associations and control words through a single FIFO and operates on them per the reference standard. This greatly simplifies the implementation of complex security functions required for WiMAX.

### Key Features:

- Inline symmetric cryptographic functions (compliant to the WiMAX mobile profile 802.16e-2005 PDU processing)
- AES-CCM to the NIST SP 800-38C specification with 128 bit keys
  - Support for insertion and extraction of packet number
- NULL encryption mode support to flow through selected PDUs without performing any security processing.
- Gate count of 44K ASIC gates with standard throughput option
  - Cipher option for increased throughput also available

### Applications:

- WiMAX SoCs in base station and subscriber applications

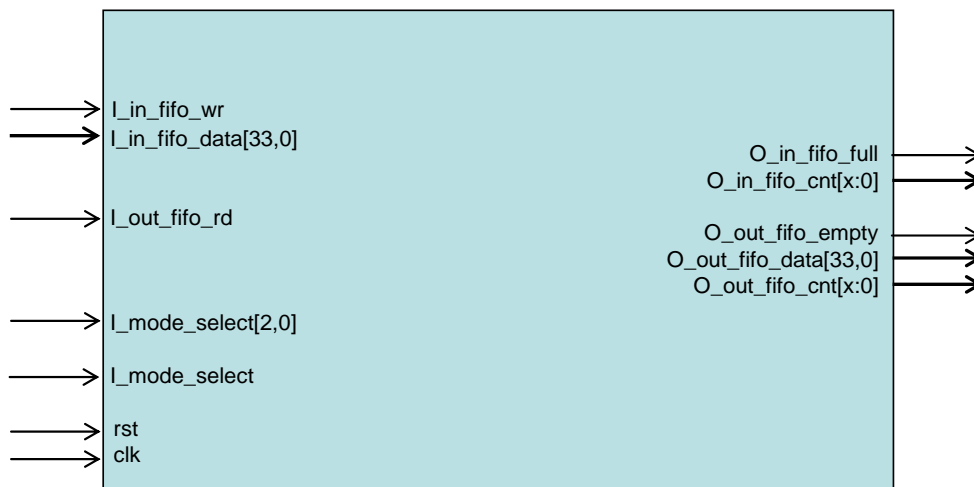
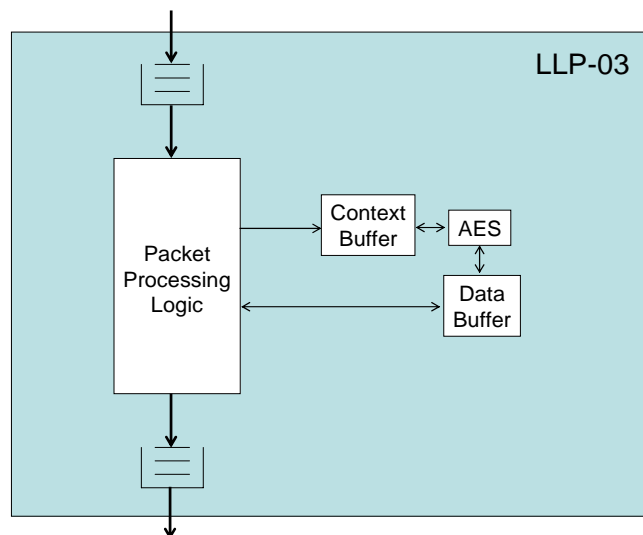


Figure 1 LLP-03 Pin Diagram

## General Description

The LLP-03 offers a complete, drop-in solution to the link layer security requirement for the 802.16/WiMAX Forum mobile profile. It is a subset to the IEEE 802.16e-2005 standard. The LLP-03 accepts interleaved security associate (SA) and PDU data through a common FIFO, interprets the command sequence, establishes the context for the appropriate cipher block then does either the encryption or decryption operation required. The LLP-03 can therefore be inserted seamlessly into the upper layer of the MAC.

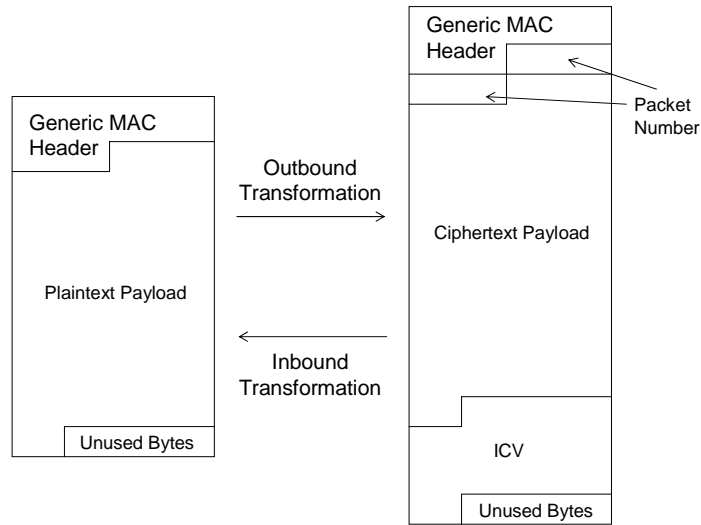
The mobile profile of the WiMAX specification specifies AES as the only cipher with 128 bit key size and support for CCM (Counter mode with CBC Message authentication). The block diagram below illustrates the internal construction of the core.



**Figure 2 Block diagram for the LLP-02**

The FIFOs in and out of the core are 34 bits wide. 32 bits are used for data and 2 bits for control. Control words indicate the type of data presented to or received from the FIFO, i.e. the control bits select whether the associated data word contains PDU data, SA data, or control information to/from the core. Any PDU in the stream may be tagged with the NULL encryption mode and will pass transparently through the core without application of the cryptographic functions. This feature can also be useful for debug during integration and application development.

As the specified cryptographic function is implemented, the PDU is transformed based upon the mode selected. A sample transformation is outlined in the diagram shown in Figure 3 below.



**Figure 3 PDU Transform – AES-CCM**

## Core Memory

The LLP-03 requires two internal memories or register files. There is context memory for the AES core, a context memory and a data buffer. The following table specifies these requirements:

Memory	Size	Type
AES Context	72 x32	Dual Port SRAM
Data Buffer	48 x 32	Dual Port SRAM

**Table 1 Memory Requirements**

As mentioned earlier, the input and output FIFOs are build time configurable by Elliptic. The standard configuration is implemented as 24 words deep – each word being 34 bits.

## Ellipsys Middleware for PKM

Elliptic offers PKM software to simplify and speed time to market. The PKM protocol is used for certificate-based authorization of the subscriber station and to perform transfer of keys between the base station and the subscriber station. The subscriber station provides its certificate to the base station, thus revealing its identity and public key to the base station. The base station returns an authorization key to the subscriber station, protected by the subscriber station public key using the RSA algorithm. The subscriber station can then decrypt the authorization key using its private key. The authorization key is then used to derive symmetric keys used in the LLP-03 for PDU traffic. The Ellipsys PKM software offers a library of the RSA authentication, encryption and decryption

functions for PKM. Ellipsys software is available either as a library or as source code if required.

## Hardware Deliverables

The LLP-03 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

### Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

### HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes either as a bit file or optionally on the EVAL-01 or EVAL-02 evaluation systems. For more information on pricing and the complete User's Manual, please contact:

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)