

The IEEE has ratified the 802.1AE Media Access Control Security (MACsec) standard which offers connectionless user data confidentiality, frame data integrity, and data origin authenticity for LANs, metropolitan optical networks and other applications. The MACsec security design consists of two elements - a key agreement protocol specified in 802.1af/802.1X-REV, and a data plane protocol which protects frames traversing the network. The data plane protocol defines the frame format for data encapsulation, encryption, and authenticity using the high performance authenticating cipher GCM-AES. Elliptic's LLP-04 is based on its silicon proven GCM-AES core with support for 802.1af/802.1X-REV offered through Elliptic's Ellipsis Middleware.

### Key Features:

- Bandwidth up to 45 Gbps full duplex at 375 MHz core clock
- Small internal memory required for classification and security association storage
  - Scalable support for multiple Secure Associations and Connectivity Associations
- Flow-through 802.1AE PDU Processing Engine with FIFO fast path interfaces
- Separate LMI interface to control plane
- Gate count of 800K ASIC gates

### Applications:

- Ethernet Switches
- Metropolitan Ethernet
- Routers

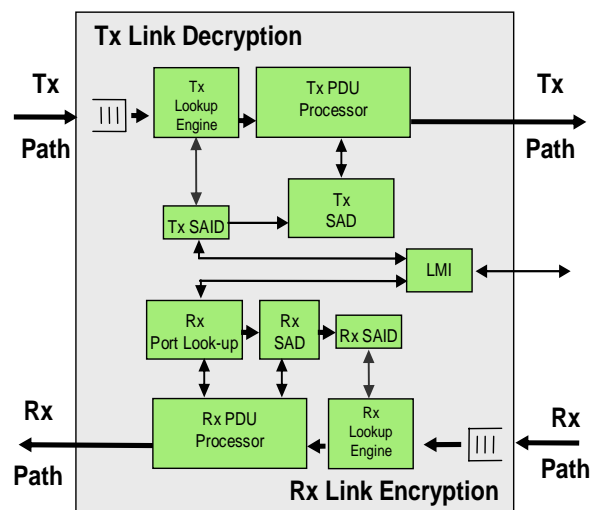


Figure 1 LLP-04 Pin Diagram

## General Description

The IEEE 802.1AE protocol would take a significant amount of CPU processing and is usually implemented in a dedicated hardware security engine. Elliptic's 802.1AE protocol offload engine supports the complete MACsec frame processing function and can be integrated with the system MAC to maximize system throughput. Full 802.1AE security processing is performed on each frame, including SA lookup, Tx encapsulation, Rx decapsulation, error checking and implementation of the GCM-AES self-authenticating cipher.

The architecture provides an inline, flow-through data path with FIFO interfaces for easy integration into high-speed architectures. It also provides a Link Management Interface (LMI) for managing SecY contexts. It is built on Elliptic's scalable, pipelined GCM-AES architecture, and thus can scale to very high data rates beyond 40 Gbps. Each instance of the engine can be configured to handle Rx-only, Tx-only or combined Rx/Tx traffic. The design supports processing a single complete frame at a time.. Solutions requiring interleaved frame segments are also available (contact Elliptic for details).

802.1AE specifies the transforms required to authenticate and optionally encrypt datalink layer frames as illustrated in Figure 2.

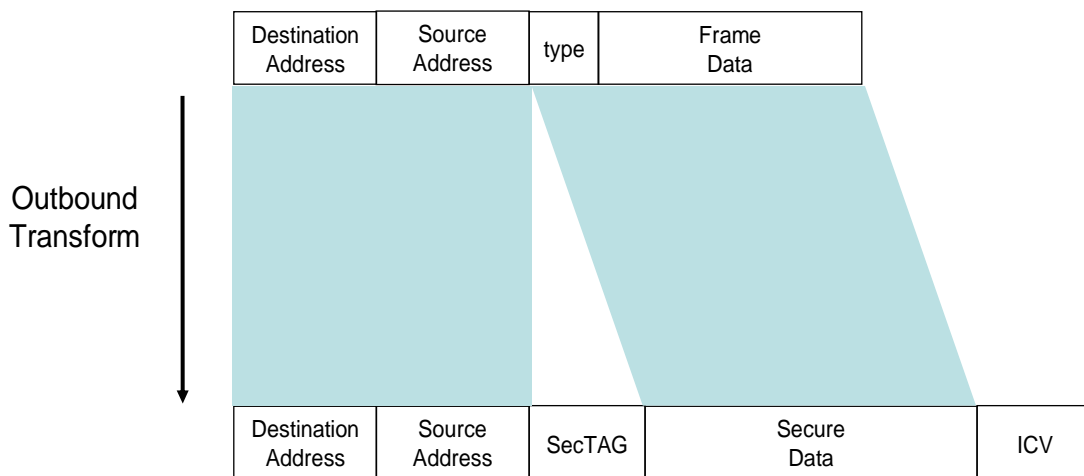
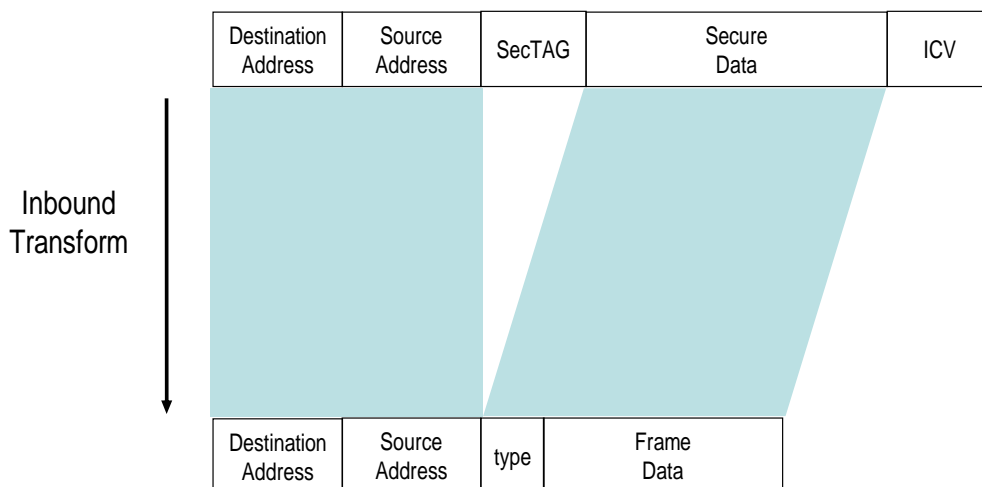


Figure 2 Transmit MACsec frame transform

The SecTAG consists of 8 or 16 octets that include (among other things) the four octet Packet Number (PN) and an optional eight octet Secure Channel Identifier (SCI). The PN provides anti-replay protection, while the SCI identifies which key is to be used for cases



**Figure 3 Receive MACsec frame transform**

where a single switch participates in multiple secure associations. The data is (optionally) encrypted with a 128-bit AES key associated with the link through the Secure Association using the GCM-AES algorithm. MACsec supports authentication-only and authenticated confidential services.

The inbound or receive transform restores the original frame for switching or processing by higher layers. This transform is shown in Figure 3.

The 802.1AE engine offloads the following protocol-level processing:

- Header parsing and generation/extraction of SecTAG, PN, SL, SCI, etc. (as required)
- Confidentiality Offset processing
- PDU validation (Ethertype, ES, SCB, SC, SL, E, C, Version, lengths, etc.)
- SA lookup using SCI
- Anti-replay checking (Packet Number)
- GCM (authenticated encryption) and GMAC (authentication-only) processing

The engine can also be configured with different GCM-AES cores to allow it to map to applications in the 2 to 20 Gbps range.

## Ellipsys Middleware

A solution for 802.1af/802.1X-REV – the management layer protocol for 802.1AE is available. It has been developed using Elliptic's Ellipsys Security Middleware. Licensed as fully proven, NIST-certified C source code, the library offers algorithms for symmetric and asymmetric cryptography including AES, SHA, RSA and ECC capabilities.

## Hardware Deliverables

The LLP-04 is available in soft IP form, either as a HDL Source or a Netlist. The deliverables available are:

### HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

### Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation 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 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)