



SafeXcel™ IP Inline MACsec Frame Engine (EIP-60)

EIP-60: Intellectual Property (IP)

Family of security engines for In-line processing of MACsec frames and AES-GCM based authenticated encryption/decryption at line rate up to 80 Gbit/s.

SPECIFICATIONS

Applications:

- NPU SoC
- MACsec routers
- L2 & L3 Secure Switches

Protocol support:

MACsec

- 802.1AE-2006 compliant
- SecTAG insertion/removal
- Confidentiality offset: 0, 30, and 50 bytes
- ICV calculation/insertion and checking/removal
- Packet number generation and checking

MACsec Extended Features

- Offset to bypass VLAN tags
- Confidentiality offsets from 1 to 64-byte

Crypt-Authenticate processing

- Basic operations with AES-GCM/GMAC/CTR modes

- Bypassing data in front of the crypto data
- ICV calculation & insertion and checking & removal
- Various IV loading methods

Cut-Through Processing

- Enormously reduces latency
- Processing can start before the complete frame is received

Benefits:

- Silicon-proven IP Design
- Lowest possible latency
- Line rate throughput across all packet sizes
- Multiple speed grades available with throughput from 10 to 80 Gbit/s
- Supports wide range of applications
- Worldclass support
- Available now

Support for cryptographic security has become a basic requirement for networks. In a LAN/MAN network, MACsec can provide the required level of security for protecting LAN and Metro Ethernet communications at the link-layer. The SafeXcel IP Inline MACsec Frame Engine (EIP-60) is one of AuthenTec's sophisticated, highly-integrated security modules, designed to add line-rate MACsec processing for networking applications.

Ease of Integration and World-class Support

Years of experience in designing silicon security products made AuthenTec the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly product interfaces. AuthenTec's global presence and expertise in security IP design enables us to provide our customers with 24/7 world-class support that is unmatched in the industry - supporting your design-in process and ensuring the success of your project.

MACsec protecting the LAN

MACsec is an IEEE 802 standard that specifies how all or part of a LAN network can be transparently secured at the link-layer. MAC Security provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. The MACsec security architecture comprises two main components — an authenticated key agreement protocol defined in 802.1X-REV, and a data plane protocol, which protects frames transmitted on the LAN.

The data plane protocol is defined in 802.1AE and is known as MACsec. MACsec defines the frame format for data encapsulation, encryption, and authentication. MACsec adds a security tag in the frame that allows the receiver of the frame to verify the authenticity, integrity, and the timeliness of the frame.

Wide Range of Applications

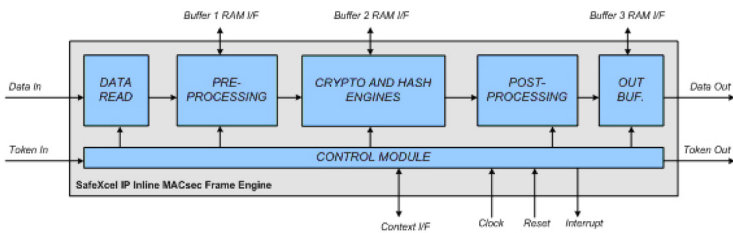
The EIP-60 is an Inline MACsec Frame Engine designed to perform line-rate processing for MACsec protocol (including extended

MACsec features), AES-GCM-based authenticated encryption/decryption and frame bypass/drop. The EIP-60's simple token-based control interface makes the engine suited for communications processors and other general-purpose processors that require maximum data plane offload to dedicated security hardware. The EIP-60 accommodates designs that already include Packet Classifiers (such as NPUs) as well as designs that require bulk crypto processing without any flow processing. In addition, the EIP-60 can be used in various SoC architectures, even 'look-aside' architectures, to accelerate cryptographic operations and offload them from the CPU.

In systems where no packet classification hardware is available, AuthenTec also offers the EIP-160 Flow-Through MACsec Frame Engine that completes the EIP-60 with flow pre- and post-processors. Pre-integration with AuthenTec's QuickSec for MACsec makes it to be the only complete MACsec solution on the market offered from a single vendor.

Inline Packet Processing

The EIP-60 implements various data manipulation instructions, including data insertion, data removal, data replacement and data retrieval, along with crypto and authentication operations. The high-level processing functions are accessed via simple per-packet commands (tokens). The EIP-60 comes with FIFO-like interfaces for both frame data and token, allowing easy integration within a frame processing pipeline. To access security context structures that hold key, IVs and packet number state, the EIP-60 has a simple TCM interface with wait-state capability.



High-Performance Architecture

In order to achieve Gigabit rate throughputs, the EIP-60 uses a sophisticated multi-stage processing pipeline, which includes security context pre-fetching and optimal update. This allows the engine to achieve line rate across all packet sizes. The core can be provided at various clock speed and throughput points (contact AuthenTec for the most appropriate configuration for your system).

Configurations and Options

The EIP-60 features a modular interface design, allowing flexible integration into various systems. The EIP-60 is offered in three configurations for various gate-count and performance targets. Additionally, depending on target technology (FPGA or ASIC), the EIP-60 can be delivered with special RTL modification for the most efficient implementation. For more options, such as support for other bus interfaces or alternate configurations of the encryption and authentication algorithms, please contact AuthenTec.

For applications that require 256-bit AES support and/or IPsec functionality, AuthenTec offers the EIP-97g Inline IPsec & MACsec Engine that delivers the same MACsec functionality plus IPsec ESP transform and 192/256-bit key for both protocols.

Gatecount and Performance

The EIP-60 gate count values listed below are NAND equivalents and indicative for generic cell libraries:

Configuration	Technology	Gate-count (kGates)	Buffer RAM	Maximum frequency (MHz)	Throughput ¹ (Gbit/s)
EIP-60c	TCMS 90 nm	301	1 x 256 Byte	540	57
	TCMS 65 nm	336		720	76
	Xilinx Virtex 5	38k LUT + 12k FF + 40 BRAM	2 x 128 Byte	140	14.8
	Altera Stratix II	29k ALUT + 12k FF + 160 M4K RAMs		125	13
EIP-60b	TCMS 90 nm	261	1 x 256 Byte	540	48
	TCMS 65 nm	291		720	64
	Xilinx Virtex 5	31k LUT + 11k FF + 28 BRAM	2 x 128 Byte	140	12.5
	Altera Stratix II	24k ALUT + 11k FF + 112 M4K RAMs		125	11
EIP-60a	TCMS 90 nm	194	1 x 256 Byte	550	28
	TCMS 65 nm	216		740	37
	Xilinx Virtex 5	23k LUT + 11k FF + 16 BRAM	2 x 128 Byte	138	7.0
	Altera Stratix II	17k ALUT + 10k FF + 64 M4K RAMs		125	6.3

¹This is a line rate throughput for all possible frame sizes including inter-frame gap, pre-amble and frame check sequence.

HEADQUARTERS

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, FL 32901 USA
+1-321-308-1300

WORLDWIDE REPRESENTATIVES NETWORK
A complete listing of AuthenTec's network of representatives is available at our web site.

For more information about Embedded Security Solutions:
embedded@authentec.com

www.authentec.com

TECHNICAL SPECIFICATIONS

Frame Bypass/Drop

- Bypassing frames
- Dropping frames (with and without fetching the frame)

Technical Specifications

Cryptography support

- AES-GCM
- AES-GMAC
- AES-CTR
- 128-bit cipher key

Data-path

- 128-bit wide
- Instruction set driven
- Cryptographic and non-cryptographic data processing
- Authenticated encryption or decryption
- Plain encryption/decryption
- Frame bypass
- Frame drop

Interfaces

Input/Output Packet interface

- FIFO 128-bit

Token interface

- Input FIFO 32-bit
- Output FIFO 32-bit

Context Interface

- TCM 32-bit

Local Buffer RAM

- Three instances
- Dual port (IR/IW)
- TCM 128-bit

Interrupt output

Deliverables

RTL source code

- Synthesizable Verilog
- Generic Memory models

Verification environment

- RTL test bench
- Simulation script
- Test & Result vectors

Synthesis Script Documentation

- Data Sheet
- Hardware Reference and Programmers Manual
- Operations Manual
- Integration Manual
- Verification Specification