

SafeXcel IP

In-line IPsec/MACsec Packet Engine (EIP-62)

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

Applications:

- NPU SoC
- MACsec routers
- L2 & L3 Secure Switches
- Fibre Channel Security (FC-SP)

Protocol Support:

IPsec

- ESP transform (RFC4306)
- Cipher suites: AES-GCM/GMAC (RFC4543, RFC4543)
- 128/192/256 bit cipher key
- Supports both IPv4 and IPv6

- Plaintext header bypass
 - Full ESP header processing
 - Sequence number generation/true anti-replay checking
 - Extended sequence numbering
 - Pad insertion and observation
 - ICV processing
- #### MACsec
- 802.1AE-2006 compliant

- 128/192/256 bit cipher key
- SecTAG insertion/removal
- Confidentiality offset from 1 to 64 byte
- Packet number processing
- Programmable header offset
- ICV processing
- Offset to bypass VLAN tags

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 10-80Gbit/s
- Supports wide range of applications

Support for cryptographic security has become a basic requirement for networks. In the WAN networks IPsec is used for internet protocol security, while in the LAN/MAN networks, MACsec protects LAN and Metro ethernet communications at the link-layer. Specification of new AES-GCM cipher suite for both IPsec and MACsec protocols brought the opportunity and requirement to support line rate processing in network equipment. The SafeXcel-IP In-line IPsec and MACsec frame engine (EIP-62) is one of AuthenTec's sophisticated, highly integrated security modules, designed to add line-rate IPsec and MACsec processing for gigabit-rate networking applications. Designs needing only MACsec and no IPsec support are best served with the EIP-60 core.

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.

Up to 80 Gbit/s AES-GCM based IPsec and MACsec protocol acceleration

IPsec (Internet Protocol Security) is a framework of open standards for secure communication over internet

protocol (IP) networks by using cryptographic security services. The IPsec security architecture comprises of three main components: AH (for IP header protection), ESP (for IP payload protection) and IKE (Key Agreement Protocol). While IKE protocol is typically handled by the host CPU, the data plane protocols (ESP and AH) require hardware offload to meet performance and power requirements. The ESP protocol nowadays is the most used data plane security protocol. MACsec is an IEEE 802 standard that specifies how all or part of a LAN network can be transparently secured at the link-layer. The MACsec security architecture comprises two components: an authenticated key agreement protocol defined in 802.1X-REV and a data plane protocol in 802.1AE and known as MACsec, which protects frames transmitted on the LAN using AES-GCM cipher suite.

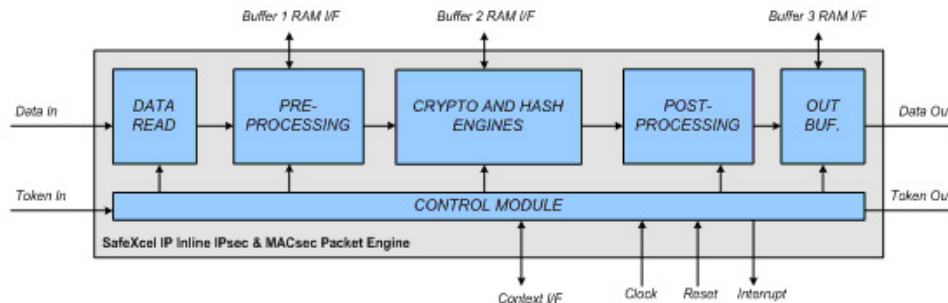
Wide Range of Applications

The EIP-62 is an In-line IPsec and MACsec packet engine designed to perform line-rate processing for IPsec ESP protocol, MACsec protocols and frame bypass/drop. The EIP-62'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. In addition, the EIP-62 can be used in various SoC architectures, even 'look-aside' architectures, to accelerate in cryptographic operations and offload them from the CPU.

The modern network equipment tend to combine in one module usage of IPsec for protecting communication to external world and MACsec to protect local network, therefore the EIP-62 is ideally positioned here as universal data plane security engine due to its dual-protocol support in single engine.

For applications that require IPsec processing to support also mature cipher suites (3DES, AES-CBC, MD5, SHA etc.) in performance range from 1 to 5 Gbit/s, AuthenTec offers the EIP-96 In-line Security packet engine that is intended to co-exist with the EIP-62 in one system providing features required interoperating with the existing IPsec equipment.

The AuthenTec QuickSec IPsec toolkit and QuickSec MACsec toolkit can be used to build your software environment with high-performance hardware offloading to the EIP-62 engine.



In-line Packet Processing

The EIP -62 implements single-pass protocol transformation using AES-GCM cipher with cipher key lengths of 128-bit, 192-bit and 256-bit. The protocol processing functions are accessed via simple per-packet commands (tokens). The IP sec ESP processing with the EIP-62 requires external system to provide and modify the IP headers, while for MACsec no additional external processing is required.

The EIP-62 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 and mask state, the EIP-62 has a simple TCM interface with wait-state capability.

Very Low Latency

The EIP-62 is designed for very low system latency. The maximum latency of a from (first byte in, first byte out) is less than 36 cycles for all frame types in all configurations of the EIP-62.

The EIP-62 implements cut-through processing for all MACsec and control/bypass frames. This reduces the external buffering to a minimum. In cut-through mode the frame length is determined autonomously by the EIP-62 using externally provided 'end of frame' signaling with the last byte of the frame.

Configurations and Options

The EIP-62 features a modular interface design, allowing flexible integration into various systems. The EIP-62 is offered in three configurations for various gate-count and performance targets. Additionally, depending on target technology (FPGA or ASIC), the EIP-62 can be delivered with special RTL modification for the most efficient implementation.

Gate count and performance

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

Table 2: Configurations and Ordering Information

Configuration	Part Number for ordering	Technology	Approximate Gate Count at optimum clock frequency (K gates)	Buffer RAM	Maximum Frequency (MHz)	Throughput for all frame sizes (including Ethernet overhead)	
						any clock frequency (bits/cycle)	max. clock frequency (Gbit/s)
EIP-62im-j	913-062005-130	TSMC 90nm	400	1 x 256 2 x 128	460	>106/97	49/45
		TSMC 65nm	450		615		65/60
		TSMC 40nm	400		800		85/78
		Xilinx Virtex 5	41k LUT + 16k FF + 56 BRAMs		120		13
		Altera Stratix II	31k ALUT + 16k FF + 224 M4K RAMs		115		12
EIP-62im-f	913-062004-130	TSMC 90nm	305	1 x 256 2 x 128	460	>89	41
		TSMC 65nm	345		615		55
		TSMC 40nm	345		800		71
		Xilinx Virtex 5	40k LUT + 14k FF + 28 BRAMs		140		12
		Altera Stratix II	30k ALUT + 14k FF + 112 M4K RAMs		115		10
EIP-62im-d	913-062003-130	TSMC 90nm	230	1 x 256 2 x 128	460	>51	23
		TSMC 65nm	255		615		31
		TSMC 40nm	255		800		41
		Xilinx Virtex 5	32k LUT + 13k FF + 16 BRAMs		140		7.1
		Altera Stratix II	24k ALUT + 13k FF + 64 M4K RAMs		115		5.8

Special Features

Crypt-Authenticate processing

- Basic operations with AES-GCM/GMAC/CTR modes
- Bypassing data in front of the crypto data
- Programmable ADD length
- ICV calculation & insertion and checking & removal
- Various IV loading methods

Frame Bypass/Drop

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

Technical

Specifications

Cryptography support

- AES-GCM/GMAC/CTR
- 128/192/256-bit cipher key

Data-path

- 128-bit wide
- Instruction set driven
- Authenticated encryption or decryption
- Plain encryption/decryption
- Frame bypass/drop

Interfaces

Input/Output Packet interface

- FIFO 128-bit

Token interface

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

Context interface

- TCM 128-bit with wait-state capability

Control bus interface

- TCM 32-bit

Local Buffer RAM

- Three instances
- Dual port (1R/1W)
- 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