

### EIP-96: Intellectual Property (IP)

family of security engines for In-line processing of IPsec, MACsec, SRTP, and acceleration of SSL/TLS/DTLS protocols

#### SPECIFICATIONS

##### Applications:

- NPU SoC
- L2 & L3 Secure Switches
- WiMAX and WiFi

##### Protocol Support:

###### IPsec

- IPsec ESP and AH packet transforms
- Support for latest IPsec RFCs (RFC-3566, 430x, 4434, 4543, 4868)
- Extended Sequence Number Support
- Replay protection
- Full header and trailer processing
- Mutable-bit handling for AH
- IPv4 /IPv6 support (RFC-4301) & header updates
- Performance >3 Gbps at 333 MHz

###### MACsec

- Header insertion and removal (IEEE Std. 802.1AE-2006)
- Integrity only and integrity & confidentiality modes
- Confidentiality offset

###### SRTP

- SRTP packet transforms (RFC-3711)
- Variable offset of header length per packet

###### SSL/TLS/DTLS

- SSL 3.0, TLS and DTLS transforms (RFC-4346, 4347)
- Full header processing

###### Benefits

- Silicon-proven IP Design
- Programmable packet processing
- Excellent throughput across all packet sizes
- Available now

Support for cryptographic security has become a basic requirement for many networking and mobile silicon devices. This creates a challenge for semiconductor designers who realize that cryptographic security processing needs assist from dedicated hardware to achieve the levels of throughput required by today's applications. Implementing security functionality on dedicated hardware enables designers to achieve higher throughput performance, lower power consumption, and a higher degree of security over software-based implementations running on a general-purpose processor. AuthenTec offers its expertise in the design and integration of dedicated security hardware to semiconductor designers by means of its SafeXcel™ IP product portfolio. The SafeXcel IP Inline Packet Engine (EIP-96) is one of AuthenTec's sophisticated, highly-integrated security modules, designed 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.

### Wide Range of Applications

The EIP-96 is an Inline Cryptographic Accelerator designed to fully off-load the very CPU intensive IPsec, MACsec, SRTP, SSL, TLS and DTLS protocol operations. The EIP-96's unique instruction set based control interface makes the engine suited for communications processors and other general-purpose processors that require maximum data plane off-load to dedicated security hardware. The EIP-96 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-96 can be used in various SoC architectures, even 'look-aside' architectures, to accelerate cryptographic operations and off-load them from the CPU.

In systems where no packet classification hardware is available, AuthenTec also offers the EIP-96 Flow-Through Packet Engine that complements the EIP-96 with flow pre and post processors to accelerate this classification.

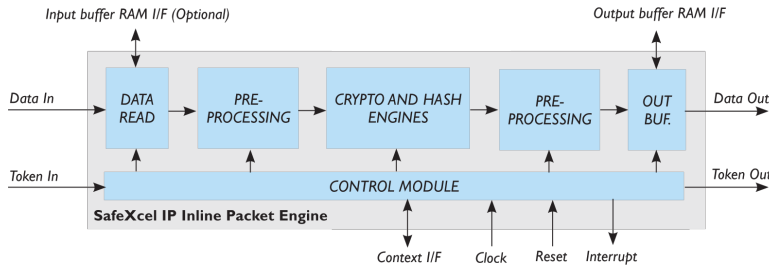
### Inline Packet Processing

The EIP-96 implements various data manipulation instructions, including data insertion, data removal, data replacement, and data retrieval, along with crypto, hash, and checksum operations. It performs such operations on incoming data, as instructed by the external Packet Classifier/Flow Processor. The EIP-96 supports widely used mature algorithms DES, 3DES, AES, ARC4, SHA-1, SHA-2, MD5 and new high-speed combined algorithms AES-CCM, AES-GCM, AES-GMAC.

A set of instructions used to transform each individual packet is called a 'token'. To perform full packet transform of security protocols, AuthenTec provides an extensive set of token templates for all protocols supported by the EIP-96. Customers can build their own token templates according to guidelines in the product documentation.

### High-Performance Architecture

In order to achieve Gigabit rate throughputs, the EIP-96 uses a three-stage processing pipeline, which includes security association pre-fetching and optimal update. This allows the engine to achieve superior performance across all packet sizes. EIP-96 V2.0: Intellectual Property (IP), includes a family of security engines for In-line processing of IPsec, MACsec and SRTP protocols, and acceleration of SSL/TLS/DTLS protocols.



## Configurations and Options

The EIP-96 features a modular interface design, allowing flexible integration into various systems. The EIP-96 is offered in four configurations, each available with either a TCM/DMA or FIFO interface for packets and context data. For more options, such as support for other bus interfaces or alternate configurations of the encryption and authentication algorithms, please contact AuthenTec.

## Gatecount

The EIP-96 gate count values listed below are NAND equivalents and indicative for generic cell libraries:

Configuration	Description	Gate count (kGates)*	Max Freq. (MHz)*
EIP-96i	IPSec, MACsec, sRTP + AES-GCM/CCM/GMAC/XCBC-MAC	250	405
EIP-96ie	The EIP-96i extended with SHA-384, SHA-512	290	390
EIP-96is	The EIP-96i extended with SSL/TLS/DTLS + ARC4	310	400
EIP-96ies	The EIP-96i extended with SSL/TLS/DTLS + ARC4, SHA-384, SHA-512	350	390

\* Gate count and maximum frequency figures are for 90nm TSMC technology.

## Performance

The maximum throughput figures are shown in the table below:

Protocol	Cipher	Hash	Plaintext size, bytes	Throughput, Mbit/s*		
				250 MHz	333 MHz	450 MHz
IPv4 ESP tunnel	AES-CBC	SHA-1	44	1250	1665	2250
			1418	2575	3430	4635
802.1ae (MACsec)	AES-GCM	AES-GCM	64	1625	2165	2925
			1446	3000	3996	5400
SSL/TLS	ARC4 stateful	MD5	64	600	799	1080
			1446	1475	1965	2655
DTLS	AES-CBC	SHA-1	64	1075	1432	1935
			1446	2700	3596	4860
SRTP	AES-ICM	SHA-1	64	1350	1798	2430
			1350	2725	3630	4905

\* The throughput calculation is based on the size of Layer 3 outbound packets.

## 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](mailto:embedded@authentec.com)  
[www.authentec.com](http://www.authentec.com)

## TECHNICAL SPECIFICATIONS

### Cryptography Support

- DES and 3DES: ECB, CBC, OFB, CFB
- AES: ECB, CBC, ICM, CTR with 128/192/256 bit key
- ARC4: stateful and stateless
- SHA-1, SHA-2 (224, 256, 384 and • 512-bit), MD5
- Basic hash and HMAC for all MD5 and SHA algorithms
- SSL MAC for MD5 and SHA-1
- GHASH, AES-XCBC-MAC
- AES-GCM/AES-GMAC
- AES-CCM

### Data-path

- Instruction set driven
- Cryptographic and non-cryptographic data processing
- Basic hash and authentication
- Basic encrypt / decrypt
- Encrypt-hash / hash-decrypt
- Hash-encrypt / decrypt-hash

### Pseudo-Random Number Generator

- Generation of IVs for DES, 3-DES and AES
- ANSI X9.31 3DES

### Interfaces

#### Input/Output Packet interface

- Generic TCM/DMA
- FIFO 32-bit

#### Context interface

- Generic TCM/DMA
- FIFO 32-bit

#### Token interface

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

#### Control bus interface

- TCM 32-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

- Hardware Specification and Programmers Manual
- Operations Manual
- Token Examples Document
- Integration Manual
- Verification Specification