

EIP-94: Intellectual Property (IP)

security engine for accelerating IPsec, SSL/TLS, DTLS, SRTP, MACsec and Public Key Operations

SPECIFICATIONS

Applications:

- VPN routers
- Femto- & Picocells
- Cable & xDSL modems
- VoIP
- WiMAX and WiFi
- FTTH (Fiber To The Home)

Protocol support:

- IPsec ESP and AH packet transforms
- Support for latest IPsec RFCs (RFC-3566, 430x, 4434, 4543, 4868)
- Extended Sequence Number Support (RFC-4304)
- Header and trailer processing
- Mutable-bit handling
- Replay protection

- IPv4 and IPv6 support (RFC-4301)
- Performance: >1Gbps (ESP, AES-SHA-1, 1500 Byte packets)

SSL / TLS / DTLS

- SSL, TLS and DTLS transforms (RFC-4346, 4347)
- Single pass packet transforms
- Full header processing

SRTP

- Replay protection SRTP
- SRTP packet transforms (RFC-3711)
- ROC removal
- Variable offset of header length per packet

MACsec

- Header insertion and removal (IEEE Std. 802.1AE-2006)
- Integrity only or integrity and confidentiality mode
- Unlimited number of Security Associations

System-on-Chip designers are increasingly facing the challenge to support a multitude of security algorithms in order to make the product suitable for applications that require fast security processing. AuthenTec addresses this need with a high-performance, highly integrated Packet Engine, supporting cryptographic algorithms and protocol related operations. Silicon-proven and ready-to-use, the SafeXcel™ IP Packet Engine, the EIP-94, is a reliable embedded security solution for semiconductor designers – delivering quick time-to-market while reducing design and engineering costs.

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 SafeXcel IP Packet Engine is a comprehensive processor, supporting DES, 3DES, AES, ARC4, SHA-1, SHA-2 (224, 256, 384, 512), MD5, Public-Key operations including ECC, Pseudo and True Random Number Generation, as well as IPsec (IP Security), SSL (Secure Sockets Layer), TLS (Transport Layer Security), DTLS (Datagram TLS), SRTP (Secure Realtime Transport Protocol) and IEEE-802.1ae MACsec packet transforms.

This broad range of features allows the Packet Engine to be used in many SoCs, such as network processors, communications processors, general-purpose processors, and application-specific integrated circuits.

These devices can be used in networking equipment, such as gateway appliances, firewalls, modems, office automation equipment, and telecommunications transmission equipment.

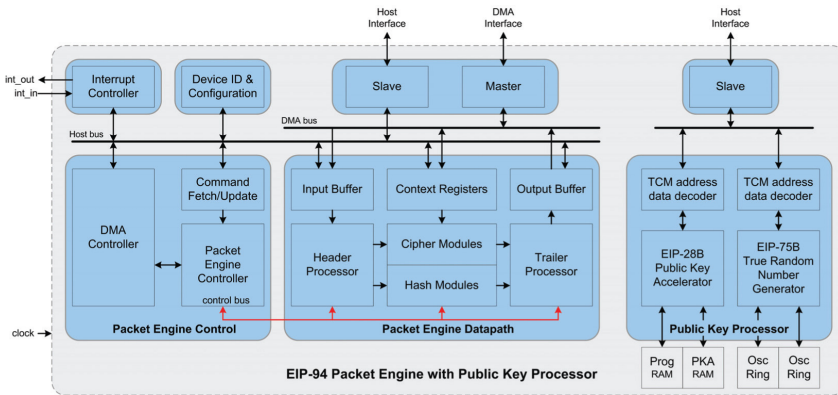
High Performance Through Autonomous Operation

The Packet Engine supports an autonomous ring mode operation that minimizes the security processing load on the host system, thereby maximizing system performance. In this mode, the Packet Engine reads and writes data and control information (packet data, packet descriptors, security association information) from host memory through DMA, without intervention by the host processor.

The information is stored in entries of ring data structures, which are processed by the Packet Engine and the host system independently (asynchronously). Status bits in the ring buffer entries ensure proper interaction between the Packet Engine and the host processor. The built-in 32-bit DMA controller supports four DMA channels, scatter/gather, and byte-aligned addressing. Packet data is buffered in dual port 2Kbyte input and output FIFOs, enabling simultaneous reading, writing, and processing of packets.

Configurations and Options

The Packet Engine features a modular interface design, allowing flexible integration into various host systems. The EIP-94 is offered in two configurations, supporting AMBA or PLB interfaces. For more options, such as support for other bus interfaces or alternate configurations of the Public-Key Accelerator and/or the True Random Number Generator, please contact AuthenTec.



Performance/Gatecount

The EIP-94 Security Packet Engine comprises of a Lookaside Packet Engine and a Public Key Processor. The Packet Engine is used as a bus master in the data plane of the system and processes packets with very little CPU intervention. The Public Key Processor is used as a bus slave in the control plane of a system for establishing sessions and setting up security associations. It comprises of a large number Public Key Accelerator (up to 4K vector support) and a True Random Number Generator.

The approximate gatecount of the EIP-94 Security Packet Engine is 380K gates (90nm, AHB) excluding memories. The Packet Engine uses 36 Kbit in 6 dual port memory instantiations, the PKP uses up to 36Kbit of program memory (RAM or ROM) and between 16Kbit and 64Kbit of operand/data RAM (depending on vector size to support).

The PLB interface has a 4 Kbit input buffer and a 4 Kbit output buffer, the AHB interface requires no buffers.

The maximum clock frequencies are ~300MHz in 65nm CMOS technology, ~250MHz in 90nm and ~200 MHz in 130nm.

At 300MHz, typical IPsec performance is 578k pps (packets per second) for 64 Byte packets using ESPAES-SHA1 and 126K pps for large packets.

Using IPsec with AES-GCM increases performance to 923K pps for 64 Byte packets and 218K pps for large packets.

At 300MHz, the Public Key Processor performs an RSA-1024 operation in 13ms (19.5ms @ 200MHz), an ECC-Add-384 operation in 0.34ms (0.51ms @ 200MHz) and an ECC-MUL-384 operation in 20ms (30ms @ 200MHz).

Protocol	Cipher	Hash	Payload	Kpps 200MHz	Mbit/s 200MHz	Kpps 300MHz	Mbit/s 300MHz
IPsec-ESP	AES-CBC	SHA-1	1536	84	1101	126	1652
IPsec-ESP	AES-CBC	SHA-1	64	385	418	578	627
IPsec-ESP	AES-GCM		1536	145	1839	218	2759
IPsec-ESP	AES-GCM		64	615	664	923	996
SSL	AES-CBC	SHA-1	1536	80	1023	120	1535
SSL	AES-CBC	SHA-1	64	310	282	465	423
MACsec	AES-GCM		1536	142	1831	213	2747
MACsec	AES-GCM		64	552	664	829	996

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

Basic Cryptographic Ops

- (3)DES: ECB, CBC, OFB, CFB
- AES: ECB, CBC, ICM, CTR
- ARC4: stateful and stateless
- HMAC (Basic, IPsec, TLS, SRTP), MAC (SSL), GMAC (IPsec) and AES-XCBC (IPsec)
- AES-GCM (MACsec, IPsec)
- AES-CCM (WLAN, IPsec)
- SHA-1, SHA-2 (224, 256, 384, 512bit), MD5

Public-Key Accelerator

- Supporting RSA, DSA, DH, ECC
- Modulus sizes up to 4k
- RSA 1024-bit sign: 5 ms (CRT)
- Local memory for storage of operands and results
- Firmware upgradable

True Random Number Generator

- Non-deterministic noise source
- Generation of keys, IVs, cookies and nuances
- ANSI X9.31 3DES
- Passes AIS-31

Pseudo-Random Number Generator

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

Bus System

- PLB4 - 128 bit, or
- AHB (AMBA 2.0) – 32 bit

Benefits

- Silicon-proven
- High degree of integration
- World-class support
- Easy to integrate
- Flexible design
- Supports wide range of applications

Deliverables

RTL source code

- Synthesizable Verilog
- Generic Memory models

Verification environment

- Test bench & simulation script

- Test & result vectors

Synthesis script

Documentation

- Product Specification
- Programmer Manual
- Operations Manual
- Integration Manual
- Verification Manual

Generic Driver Library