

SafeXcel™-IP-97: Intellectual Property (IP)

Family of security engines for Look-aside processing of IPsec, MACsec & SRTP Operations, and acceleration of SSL/TLS/DTLS Operations

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 support 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 High Speed Look-aside Packet Engine (SafeXcel-IP-97) is AuthenTec's latest addition to its family of highly-integrated security modules, designed for networking applications.

SPECIFICATIONS

Applications:

- NPU SoC
- VPN routers
- MACsec routers
- L2 & L3 Secure Switches
- VoIP
- WiMAX and WiFi
- FTTH (Fiber To The Home)

Protocol Support

IPsec

- IPsec ESP and AH packet transforms
- Support for latest IPsec (RFC-3566, 430x, 4494, 4543, 4868)
- Extended Sequence Number Support
- Replay protection
- Full header and trailer processing
- Mutable-bit handling
- IPv4 and IPv6 support (RFC-4301) and header updates

MACsec

- Header insertion / 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 including IP header modifications
- Excellent throughput across all packet sizes
- Supports wide range of applications
- World-class support
- Available now

Unlimited number of Security Associations

Ease of Integration and World-class Support

Years of experience in silicon security design has made AuthenTec the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly interfaces. With its global presence and expertise in system design, AuthenTec offers 24/7 world-class support that is unmatched in the industry — supporting customers' design-in process and ensuring the success of their projects.

Wide Range of Applications

The SafeXcel-IP-97 is a Look-aside Cryptographic Accelerator designed to partially offload or fully offload the very CPU intensive IPsec, MACsec, SRTP, SSL, TLS and DTLS protocol operations. The SafeXcel-IP-97's unique instruction set 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 SafeXcel-IP-97 can be used in SoC architectures to accelerate various cryptographic operations and offload them from the CPU.

Packet Processing

The SafeXcel-IP-97 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 SafeXcel-IP-97 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, called a 'token', is used by the SafeXcel-IP-97 to transform each individual packet.

To perform a full packet transform for security protocols, an extensive set of token templates is available for all protocols supported by the SafeXcel-IP-97. The flexibility of the tokens allow in system or in field upgradability of your Security Solutions or SoC.

The fast-path is a multi-stage pipeline that allows pre-fetching of token, context and source packet data and post-writing of context update and result packet data. Buffers decouple the Processing Engine(s) from the bus interface. This allows the engine to achieve superior performance across all packet sizes.

High-Performance Architecture

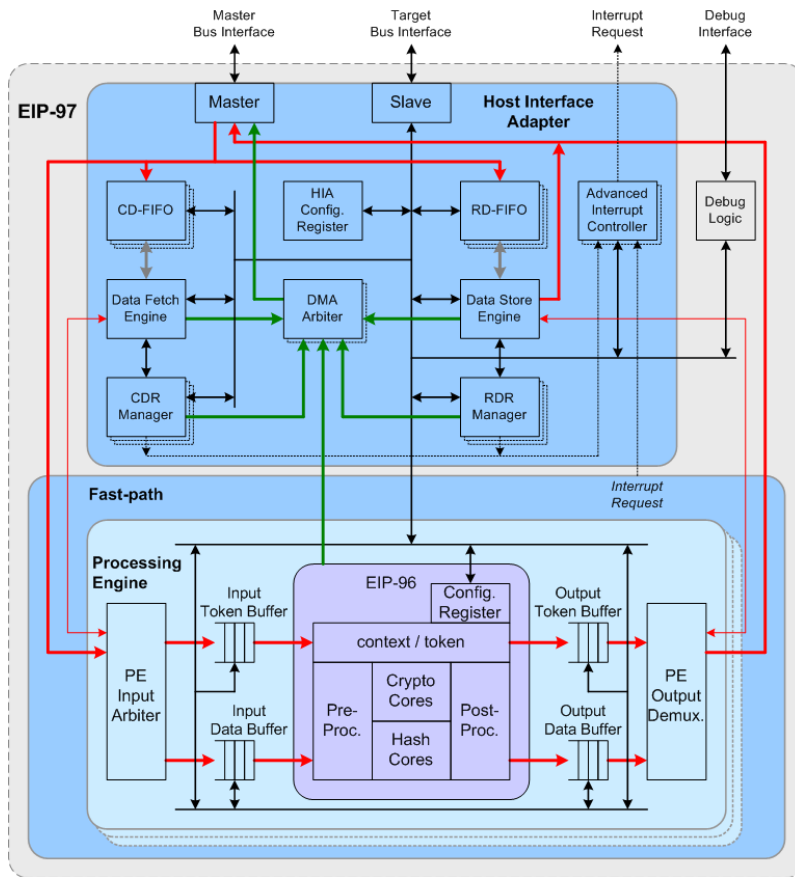
To achieve Gigabit rate throughputs, the SafeXcel-IP-97 has a high-throughput Host Interface Adapter that attaches the Processing Engine to the system bus (AXI, AHB, PLB or TCM), and provides a standardized software view for off-loading tasks. This standardized software view consists of:

- Up to 15 Command and 15 Result Descriptor Ring(s) with individual access for multi-processor support, containing control structures ('descriptors') that reference the source data, context and transform instructions (input), capture result status and reference the result data (output).
- A programmable interrupt output per host processor towards the host system.
- A configuration view for configuring the Host interface Adapter as well as the Processing Engine.
- DMA operations to and from system memory, optimized for the bus interface.
- A standardized method of gathering source data from and scattering result data to system memory.

Configurations and Options

The SafeXcel-IP-97 features a modular interface design, facilitating flexible integration into various systems. The SafeXcel-IP-97 is available in four configurations, each available with an AHB, PLB or AXI system bus interface. For more options, such as support for other bus interfaces or alternate configurations of the encryption and authentication algorithms, please contact AuthenTec. An SoC with the SafeXcel-IP-97 can be extended to a complete Security Processor by adding AuthenTec True Random Number Generator (EIP-76) and Public Key Accelerator IP modules (EIP-28).

General Block Diagram



Configuration	Description <small>Gate count and max frequency are given for TSMC 40nm</small>	Gate Count (kGates)	Max. Freq. (MHz)
EIP-97-i	IPSec + AES-GCM/CCM/GMAC/XCBC-MAC	335	708
EIP-97 -ie	EIP-97-i extended with SHA-384, SHA-512	375	682
EIP-97-is	EIP-97-i extended with SSL/TLS/DTLS + ARC4	395	700
EIP-97-ies	EIP-97-ie + EIP-97-is	435	682

The SafeXcel-IP-97 maximum throughput figures (based on size of Layer 3) outbound packets:

Protocol	Cipher	Hash	Plain text size, bytes	Throughput, Mbit/s		
				250 MHz	500MHz	700MHz
IPv4 ESP tunnel	AES-CBC	SHA-1	44	1250	2500	3500
			1418	2575	5150	7210
802.1 ae (MACsec)	AES-GCM	AES-GCM	64	1625	3250	4550
			1446	3000	6000	8400
SSL/TLS	ARC4 stateful	MDS	64	600	1200	1680
			1446	1475	2950	4130
DTLS	AES-CBC	SHA-1	64	1075	2150	3010
			1446	2700	5400	7560
SRTP	AES-ICM	SHA-1	64	1350	2700	3780
			1350	2725	5450	7630

Cryptography Support

- (3)DES: 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/SHA-1
- GHASH, AES-XCBC-MAC
- AES-GCM/AES-GMAC
- AES-CCM

Data-path

- Instruction set driven
- Header pre-processing and trailer post-processing
- Basic hash and authentication
- Basic encrypt/decrypt
- Encrypt-hash/hash-decrypt
- Hash-encrypt/decrypt-hash

Pseudo-Random Number Generator

- 3DES IV Generation
- ANSI X9.31 3DES

Host Interface Adapter with DMA and Bus mastering

- Multiple Descriptor Rings with individual access for multi-processor support
- Scatter/Gather processing
- Automatic arbitration and bus flow control
- Big and little endian support
- DMA aborts

Interfaces

- AXI, AHB, PLB or TCM master and slave interface
- Convenient debug interface
- 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 Reference Manual
- Programmers Manual
- Operations Manual
- Token Examples Document
- Integration Manual
- Verification Specification