

EIP-196: Intellectual Property (IP)

Family of security engines for high-speed flow-through processing of IPsec, MACsec & look-aside acceleration of security operations.

SPECIFICATIONS

Applications:

- NPU SoC
- VPN/MACsec routers
- L2 & L3 Secure Switches
- IPsec aware NICs
- VoIP, WiMax, WiFi and FTTH

Features:

Hardware offloaded functionality

- Stateless classification and sanity checking
- Input side classification
- Security packet transform
- Output side classification
- Output data post-processing

Protocol Support

- IPv4 and IPv6
- Jumbo packets
- IPsec ESP packet transforms

- MACsec frame transform
- NAT, NAT, NAT-T
- Complete IP header modifications and updates

Complete HW/SW solutions:

- IPsec in-line gate
- IPsec aware Ethernet MAC
- MACsec aware Ethernet MAC
- Single-pass IPsec/MACsec gateway
- Look-aside crypto accelerator

Benefits:

- Silicon-proven concept
- Includes Packet Classification and Flow Processing
- Superior throughput across all packet sizes
- Flexible and modular architecture
- Integrated with QuickSec IPsec and QuickSec MACsec toolkits
- Worldclass support

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 flow-through engine (SafeXcel IP-196 / EIP-196) is one of AuthenTec's sophisticated, highly-integrated security modules, designed for networking applications.

High-Performance Security Processing

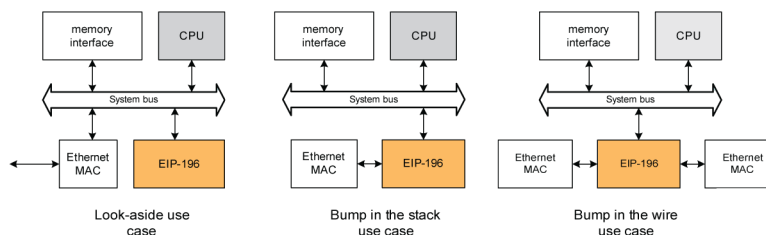
The SafeXcel IP-196 value lies in its unique capability to maximize data plane offloading from a host processor to dedicated hardware. In traditional Soc architectures, hardware assist is usually limited to modules that perform cryptographic security processing under full control of an embedded general-purpose processor. In these architectures, the general-purpose processor still needs to process each packet to some extent. Especially at high data rates and for small packet sizes, this approach creates a significant processing burden on the processor, and it may even create an overall throughput bottleneck. With the SafeXcel IP-196 on the other hand, the general-purpose CPU is not involved in processing packets that belong to an existing data flow. This allows the CPU to dedicate its clock cycles to data flow setup and other processing tasks. The SafeXcel IP-196 embeds the SafeXcel IP-96 packet engine. The result is a high-performance security solution that delivers Gigabit rate processing.

Micro-programmed Packet Classification/ Flow Processing

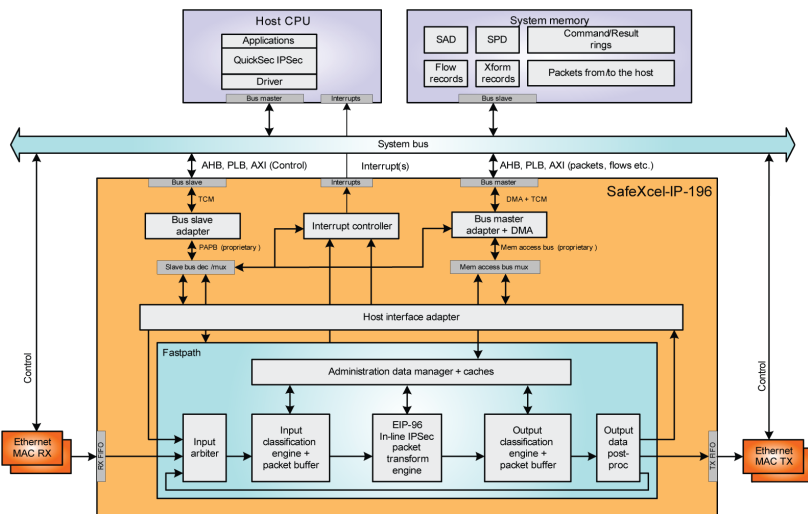
The SafeXcel IP-196 provides full data plane processing up to the IP/IPsec layer. This capability is enabled by the engine's unique packet classifiers and flow processors and is not offered by other security IP vendors. While traditional offerings need to rely on external classification, the SafeXcel IP-196 includes micro-programmed hardware assist for this time-consuming task. The SafeXcel IP-196 autonomously inspects packets, determines required processing and instructs the packet engine which transformation to execute.

Application use cases and solutions

The SafeXcel IP-196 is intended to be used in the following use cases:



In the look-aside use case, the EIP-196 is a co-processor in the system and is processing packets that are prepared and consumed by the host cpu. in the bump in the stack use case, the EIP-196 sits in between MAC and OS network stack and takes care about data plane processing for MACsec or IPsec. OS stack will never see encrypted packets. In the bump in the wire use case, the EIP-196 is used to process packets from one MAC to another MAC for established connections without host being involved.



Solutions	Look-aside	Bump in the stack	Bump in the wire
IPsec gateway	-	-	+
IPsec aware EMAC	-	+	+
MACsec aware EMAC	-	+	+
Look-aside crypto accelerator	+	+	+

Hardware configurations and Options

The SafeXcel-IP-196 features a modular interface design, allowing flexible integration into various host systems. The Packet Engine is offered in 4 configurations, each with a choice of an AHB, AXI or PLB interface. For more options or alternate configurations of the ciphers please contact AuthenTec.

Configuration	Hardware capability
EIP-196i	IPsec, MACsec, sRTP + AES-GCM/CCM/GMAC/XCBC-MA
EIP-196ie	The EIP-96i + with SHA-384/512
EIP-196is	The EIP-96i + with SSL/(D)TLS + ARC4
EIP-196ies	The EIP-96i + with SSL/(D)TLS + ARC4, SHA-384/512

Performance

Due to its capability to perform complete packet processing in hardware, at 300MHz (TSMC 90nm) the SafeXcel-IP-196 reaches up to 1 Gbit full-duplex throughput (2 Gbit aggregate) for all packet sizes.

Complete Hardware/Software Solution

Integrated software support is increasingly becoming a critical success factor for complex SoCs. Hardware security functionality in a SoC needs to be supported by state-of-the-art software to make the SoC successful in its market. The SafeXcel-IP-196 works seamlessly with AuthenTec's leading QuickSec IPsec toolkit. The QuickSec IPsec toolkit's advanced architecture offloads data plane processing to a SoC's Inline Security Engine, maximizing application performance. The toolkit also enforces policies upon the Packet Classifier as part of its control plane functionality.

TECHNICAL SPECIFICATIONS

Fast-path

- Reconfigurable for different performance and size targets
- Packet processing without need of external DRAM data buffers
- High-speed inline packet engine supporting multiple cipher suites and protocols
- Programmable classification and transform operations
- In-field upgradable functionality
- Extensive debug capabilities
- Run-time self check and well defined exception handling

Cryptography Support

- DES and 3DES: ECB, CBC
- AES: ECB, CBC, CTR, ICICM with 128/192/256 bit key
- ARC4 stateful and stateless
- SHA-1, SHA-2 (224/256/384/512)
- Basic hash and HMAC for MD5/SHA-1/SHA-2
- SSL-MAC for MD5 and SHA-1
- GHASH
- AES-XCBC-MAC
- AES-GCM / AES-GMAC
- AES-CCM
- Pseudo RNG for IV generation

Host Interface Adapter

- Descriptor ring based
- Packet scatter/gather
- Automatic arbitration and bus flow control
- Programmable support of big and little-endian host systems

Host Bus Interface

- PLB Rev4.6 128 bit, or
- AHB (AMBA 2) 32 bit, or
- AXI (AMBA 3) 32/64 bit

Line Interface

- Two input FIFO 32/64 bit
- Two output FIFO 32/64 bit

IPsec Solution

- QuickSec IPsec toolkit
- Device driver and toolkit
- Firmware for classifiers
- Reference system based on FPGA development board

Deliverables

- Hardware IP package
- Driver Development Kit
- Software Development Kit for reference FPGA board

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/embedded