SAFE XCEL IP INLINE PACKET ENGINE (EIP-93)

driving trust™ **inside**
SECURE

EIP-93: Intellectual Property (IP)

Family of low gate count security engines for accelerating IPsec, SRTP, SSL/TLS/DTLS and Public Key Operations.

<table>
<tr><td rowspan="2" style="writing-mode:vertical">SPECIFICATIONS</td><td>

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

Protocol Support:

IPsec ESP packet transforms
- Support for latest IPsec RFCs (RFC-430x, 4868)
- Header and trailer processing
- Mutable-bit handling
- Replay protection

</td><td>

- IPv4 and IPv6 support (RFC-4301)
- Performance: 550 Mbps
  (ESP, AES-SHA 1, 1500 Byte packets)

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

SRTP
- SRTP packet transforms (RFC-3711)
- ROC removal and TAG generation and insertion
- Variable offset of header length per packet

Unlimited number of Security Associations

</td></tr>
</table>

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. SafeNet addresses this need with an efficient, low gate count, highly integrated Packet Engine family, supporting cryptographic algorithms and proto-col related operations. Silicon-proven and ready-to- use, the SafeXcel IP Low Gate Count Packet Engine family, the EIP-93, is a reliable embedded security solution for semiconductors 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 SafeNet the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly product interfaces. SafeNet'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 - support-ing 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-128, SHA-1, Pseudo Random Number Generation, as well as IPsec (IP Security) and SRTP (Secure Realtime Transport Pro-tocol). Optionally, at a higher gate count a selection of the AES-192/256, ARC4, MD5, SHA-224/256, AES-CCM algorithms and the SSL (Secure Sockets Layer), TLS (Transport Layer Security) and DTLS (Datagram TLS) protocols are supported.

This broad range of features allows the Packet Engine to be used in many low cost SoCs, such as, communi-cations 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 equip-ment, and telecommunications transmission equipment.
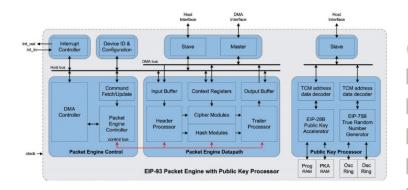
Femtocell Access Point Application

A dedicated EIP-93iw configuration targets Femtocell Access Points (FAP). The EIP-93iw provided the security hardware to both offload the IPsec protocol operation between the FAP and the Femtocell Gateway and offload securing the radio link between the FAP and the handset. The WiMAX chosen AES- CCM algorithm as well as the 3GPP Kasumi and Snow 3G algorithms can optionally be accelerated.

Efficient Processing 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 descrip-tors, 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, and byte-aligned addressing. Packet data is buffered in dual-port input and output FIFOs, enabling simultaneous reading, writing, and processing of packets.

inside SECURE

EIP-93 Packet Engine with Public Key Processor

System Integration

The EIP-93 Security Packet Engine comprises of a Lookaside Packet Engine and an optional Public Key Processor (PKP). 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 optional 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 and a True Randum Number Generator. The Packet Engine features a modular interface design, allowing flexible integration into various host systems. The Packet Engine is offered in 5 configurations, each available with an AMBA, PLB or TCM interface. 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 SafeNet.

The following configurations of the EIP-93 are available:

EIP-93i	IPSec ESP and SRTP Crypto Accelerator
EIP-93ie	EIP-93i with SHA-224/256 and AES with 192/256-bit key
EIP-93is	EIP-93i with SSL, TLS and DTLS, MD5 and ARC4
EIP-93iw	EIP-93i with AES-CCM
EIP-93ies	EIP-93ie + EIP93is

Performance/Gatecount

The approximate gatecount of the EIP-93i Security Packet Engine is 105K gates excluding PKP (50K), excluding bus interface (7K..15K) and exluding memories. The Packet Engine needs two 256 Byte 2-port memory for it's data buffers. The PLB interface has a 4 Kbit input buffer and a 4 Kbit output buffer, the AHB and TCM interfaces require no buffers. In order to offer a very low gate count, but still complete Packet Engine, not all IPsec features are supported. Amongst others Extended Sequence Numbers (only required for high speed IPsec) and SHA-512 are not supported. For those projects that require extensive feature support, please refer to the SafeXcel EIP-94. The maximum clock frequency is 300MHz in 65nm, 250MHz in 90nm and 200MHz in 130nm technology. At 300MHz, IPsec performance is 450K pps (packets per second) for 64 byte packets using ESPAES-SHA1 and 54K 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).

TECHNICAL SPECIFICATIONS

Basic cryptographic ops
- (3)DES: ECB, CBC
- AES-128: ECB, CBC, ICM, CTR
- SHA-1 & HMAC (Basic, IPsec, TLS, SRTP), MAC (SSL)
- Optional AES-192/256, SHA-2 (224, 256), MD5, ARC4, AES-CCM (WLAN, IPsec), Kasumi, Snow

Pseudo-Random Number Generator
- IV generation for (3)DES & AES
- ANSI X9.31-AES

Bus System
- PLB 4 - 128 bit, or
- AHB (AMBA 2.0) - 32 bit, or
- TCM - 32 bit
- DMA controller

Public Key Accelerator
- Optional
- Supporting RSA, DSA, DH, ECC
- Modulus sizes up to 4k
- RSA 1024 bit sign: 5 ms (CRT)
- Firmware upgradeable

True Random Number Generator
- Optional
- Non-determination noise source
- Generation of keys, IVs, cookies and nonces
- ANSI X9.31 - 3key 3DES
- Passes AIS-31

Benefits
- Silicon-proven
- High degree of integration
- Worldclass 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