

Benefits

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

Deliverables

- Synthesizable Verilog RTL source code
- RTL test bench, including test vectors and expected result vectors
- Simulation script
- Synthesis script
- System Architecture Specification
- System Verification Specification
- User's Guide

SafeXcel IP Security Packet Engine v2

Silicon-proven Intellectual Property (IP) for accelerating IPsec, SSL/TLS/DTLS, SRTP and MACsec

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 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 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 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—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, Triple DES, AES, ARC4, SHA-1/2, SHA-2, MD5, Public-key operations (incl. 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 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 table below shows two standard configurations that support AMBA and PLB interfaces. For more options, such as support for other bus interfaces or removal of the Public-Key Accelerator and/or the True Random Number Generator, please contact SafeNet.

NAME	CONFIGURATION	MAXIMUM CLOCK FREQUENCY ¹	APPROXIMATE GATE COUNT WITH SYNTHESIS AT 150 MHz ^{1,2}
EIP-94	Packet Engine with AMBA interface	~ 200 MHz	~ 450 kgates
EIP-94-PLB	Packet Engine with Processor Local Bus interface	~ 200 MHz	~ 450 kgates

¹ Technology and synthesis dependent; based on the use of a basic design compiler and a high-speed 0.13 µm technology.

² Gate counts includes the Public-Key Accelerator and True Random Number Generators. Gate counts includes scannable flipflops. Gate counts excludes memories.

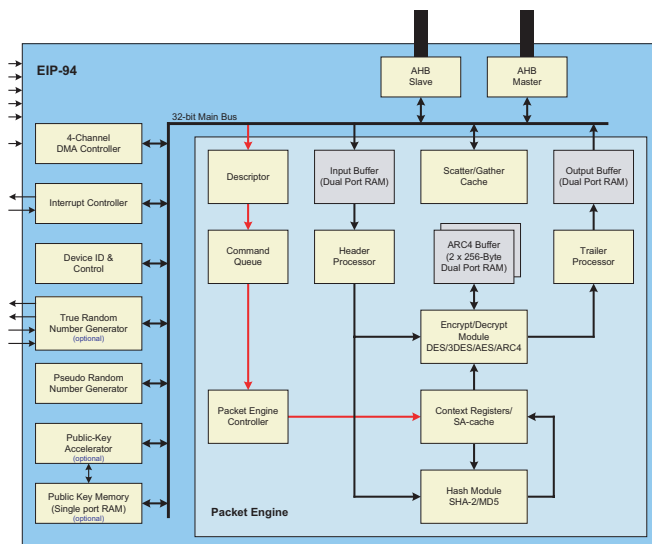
Complete Hardware/ Software Solution

SafeNet offers OEMs a wide range of product choices to build advanced networking solutions, including intellectual property and chips for hardware acceleration, as well as upper layer APIs, protocol stacks, and software toolkits such as QuickSec.

QuickSec is a family of full-featured market-leading toolkits that enable developers to quickly and reliably build sophisticated, high-performance VPN appliances.

The QuickSec products are a key component of SafeNet's fully integrated security systems for VPN, Firewall, and Intrusion Prevention solutions.

QuickSec gives appliance developers feature-rich, portable, and cost-effective VPN solutions designed for integrated security appliances that leverage hardware-based security to maximize performance and levels of security.



SafeNet Contact Information

For more information, please contact SafeNet's Embedded Security Division at +1 410-931-7500 or via email oemnetworking@safenet-inc.com, or visit our web site <http://www.safenet-inc.com/solutions/dev/intProp.asp>.

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 email: info@safenet-inc.com

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111

India +91 11 26917538
Japan +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000

U.S. (Massachusetts)
+1 978.539.4800
U.S. (Minnesota)
+1 952.890.6850
U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)

+1 949.450.7300
U.S. (San Jose, California)
+1 408.452.7651
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers located worldwide.

©2007 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.

Features

IPSec

- IPv4 and IPv6 support
- IPSec packet transforms
- Support for latest RFC's (RFC-4302, 4303 and 4308), incl. ESN
- Header and trailer processing
- Mutable-bit handling
- 1Gbit/s (ESP, AES, SHA-1, 1500-byte packets)

SSL / TLS / DTLS

- SSL, TLS and DTLS single pass packet transforms with full header processing
- One-pass hash-then-encrypt inbound transforms
- 1Gbit/s (AES, SHA-1, 1500-byte packets)

SRTP

- SRTP packet transforms
- ROC removal and TAG generation and insertion
- Variable offset of header length per packet
- 1Gbit/s (AES-ICM, SHA-1, 1500-byte packets)

MACsec

- Header insertion and removal
- Integrity only or integrity+ confidentiality mode
- 1.8Gbit/s (AES-GCM, 1500-byte packets)

Basic cryptographic operations

- (Triple-)DES: ECB, CBC, OFB, CFB modes
- AES: ECB, CBC, ICM, CTR modes
- ARC4: stateful and stateless modes
- 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 and 512-bit)
- MD5

Public-Key Accelerator

- Supporting RSA, DSA, DH and ECC
- Modulus sizes up to 4k
- RSA 1024-bit sign (CRT): 5.6 ms
- Local memory for storage of operands and results
- Interrupt output

True Random Number Generator

- Non-deterministic noise source
- Generation of keys, IVs, cookies and nonces
- ANSI X9.17 Annex C / ANSI X9.31 Annex A post-processing

Pseudo-Random Number Generator

- Generation of IVs for DES, Triple-DES, and AES
- ANSI X9.17 Annex C / ANSI X9.31 Annex A post-processing

