Benefits

- Cost-effective high performance processor
- Highly integrated, efficient architecture
- Complete VPN security features
- Broad development support
- Complete HW/SW solution
- High assurance design

**Technical Specifications**

**IPSec Performance**

- Sustained ESP: SPI-3 (data) + EMI(SA)
  - AES/SHA-1:
    - 3.2 Gbps (1500-byte package)
    - 3.1 Gbps (350-byte package)
    - 1.9 Gbps (64-byte package)
- Sustained ESP: PCI-X (data) + EMI(SA)
  - AES/SHA-1:
    - 1.9 Gbps (1500-byte package)
    - 1.3 Gbps (350-byte package)
    - 705 Mbps (64-byte package)

**Public Key Accelerator**

- Accelerator for math-intensive public key operations
- Supports up to 2048-bit modulus size
- RSA 1024-bit sign: 1400 operations/sec.
- RSA 1024-bit verify: 3900 operations/sec.
- DSA 1024-bit sign: 1440 operations/sec.
- DSA 1024-bit verify: 720 operations/sec.

The SafeXcel-1842 is a highly integrated, high-speed network security co-processor designed for VPN applications in mid-range to high-end network devices and appliances. The SafeXcel-1842 accelerates the algorithms required to implement IPsec and SSL VPNs, allowing vendors to create multi-functional security appliances with a single security co-processor. Host processors can offload not only packet processing, but also basic encryption, basic hash, and public key computations. The SafeXcel-1842 co-processor delivers high security and high performance at the best price in the industry.

**Efficient Data, Control, and Management Architecture**

The SafeXcel-1842 supports PCI-X, SPI-3, and S/DRAM memory interfaces to ensure easy integration with the widest variety of network and host processors. In addition, the SafeXcel-1842 can flexibly use different interfaces for data, control, and security association (SA) database access.

**Complete VPN Security Features**

The SafeXcel-1842 includes several features that are implemented in hardware and are not available with any other competitive chip solution, including:

- ESP header insertion/validation, including SPI and replay counter processing
- Full AH ‘mutable bit’ processing, including IPv4 options fields and IPv6 extension headers
- HMAC ICV validation on inbound packets
- Automatic IV generation and insertion
- ARCE key replication, key scheduling, and MPPE-specified key update

**Power, Flexibility, and High-Assurance**

The SafeXcel-1842 offers a variable-rate public-key accelerator clock that allows trade-offs between processing speed and power consumption. As part of SafeNet’s commitment to high assurance design, the SafeXcel-1842 chip has been implemented with FIPS-compliant cryptographic algorithms allowing our customers to achieve FIPS 140-2 certification for their appliances.

**Broad Development Support**

Full driver support is available for development on the most common Operating Systems, including Windows, Linux, VxWorks, NetBSD, and FreeBSD. Additional OS driver support can be delivered upon request.

SafeNet offers developers a simple, low-cost development kit that allows OEMs to get up and running with the SafeXcel-1842 quickly and easily. The kit includes drivers, documentation, and sample code.

**Complete Hardware/Software Solution**

Customers can significantly reduce time-to-market by licensing SafeNet’s proven QuickSec IPsec software. The QuickSec software seamlessly interfaces with any SafeXcel security co-processor and can be used on many types of host processors and operating systems. The QuickSec software can also leverage SafeXcel co-processors for accelerating IPsec packet processing and IKE authentication.
SafeXcel™-1842 Architecture Overview

Fast Packet Processing
The SafeXcel-1842 supports all necessary algorithms for IPSec and SSL applications:
- AES, DES, Triple-DES and ARC4 encryption
- MD5 and SHA-1 Hashing with HMAC
- Public-key computations, useable for
  - Diffie-Hellman Key Negotiation
  - RSA Encryption and Signatures
  - DSA Signatures
- Random Number Generation
The SafeXcel-1842 achieves high throughput not only with fast core processing engines, but also with an integration strategy that has been carefully designed to eliminate performance bottlenecks.

A hardware-enabled Descriptor Ring, located on-chip Dual-Port Memory, is used to control packet movements. This allows asynchronous processing between the host and the SafeXcel-1842. Descriptor Ring processing also allows multiple packets to be queued for processing, thereby avoiding ‘starving’ of the SafeXcel-1842.

An on-chip DMA controller intelligently allocates the packet requests among the multiple packet engines. Each packet engine contains dedicated crypto and hashing engines, allowing them to function independently. Each engine also contains its own pair of 2K-byte packet buffers that provide for efficient burst transfers of data.

This high-performance architecture allows public-key operations to be performed concurrently with Packet Engine operations.

Random Number Generator (RNG)
- Non-deterministic Random Number Generator
- Generates up to 20 Mbit/s of random data

SPI-3 Interface
- 100 MHz max bus speed
- Two independent 32-bit interfaces - 1 RX; 1 TX

PCI-X/PCI Interface
- 64-bit 3.3V bus interface, 5V tolerant
- 64-bit / 32-bit bus widths
- 100 MHz / 66 MHz maximum bus speeds for PCI-X / PCI
- PCI-X v1.0 compliant
- PCI v2.0 compliant
- Bus Master and Target capability

External Memory Interface
- 100 MHz maximum interface speed
- 64-bit / 32-bit bus widths
- 256 Mbyte address space
- Async dual port SRAM, Sync dual-port SDRAM, and PC-100/133 SDRAM supported

Electrical
- Core Power: 1.8V
- I/O Power: 3.3V
- 40 MHz PLL clock input
- Two PLL clocks: System 100 MHz max.; Exponentiator 230 MHz max.
- Power consumption: 4.7 W max.
- Dynamic power reduction by programming lower clock speeds

Packages
- 456-pin 35 x 35 mm PBGA
- JTAG Support

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