

SafeXcel-1840

High-Performance Security Co-Processor

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: PCI-X (data) + EMI(SA)

AES/SHA-1:

- 1.3 Gbps (1500-byte packets)
- 900 Mbps (350-byte packets)
- 510 Mbps (64-byte packets)

Public-Key Accelerator

- Supports up to 2048-bit modulus size
- Diffie-Hellman 1024-bit, 180-bit exponent: 1100 operations/sec.
- RSA 1024-bit sign: 1220 operations/sec.
- RSA 1024-bit verify: 3790 operations/sec.
- DSA 1024-bit sign: 1250 operations/sec.
- DSA 1024-bit verify: 620 operations/sec.

The SafeXcel™-1840 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-1840 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 to the security co-processor, but also encryption, hash, and public key computations. The SafeXcel-1840 co-processor delivers high security and high performance at the best price in the industry.

Efficient Data, Control, and Management Architecture

The SafeXcel-1840 supports PCI-X and S/DRAM memory interfaces to ensure easy integration with the widest variety of network and host processors. In addition, the SafeXcel-1840 can flexibly use different interfaces for data, control, and security association (SA) database access.

Complete VPN Security Features

The SafeXcel-1840 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
- ARC4 key replication, key scheduling, and MPPE-specified key update



Power, Flexibility, and High Assurance

The SafeXcel-1840 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-1840 chip has been implemented with FIPS-compliant cryptographic algorithms allowing our customers to achieve FIPS 140-2 certification for their appliances.

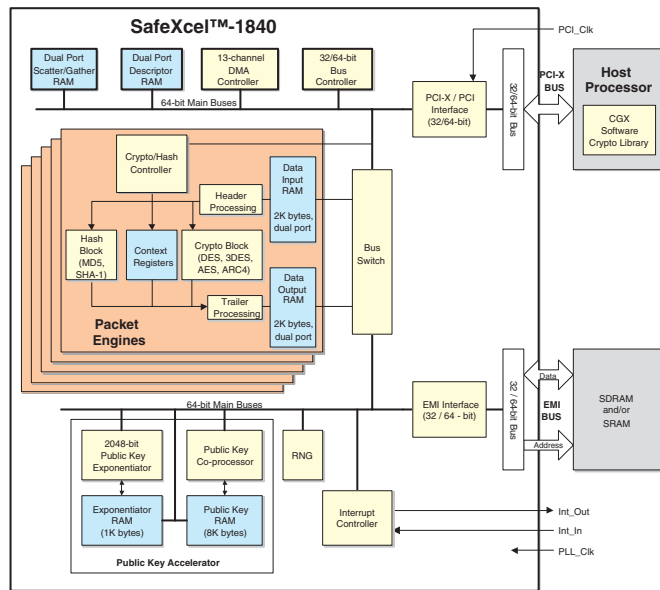
Broad Development Support

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-1840 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-1840 Architecture Overview

Fast Packet Processing

The SafeXcel-1840 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 & Signatures
 - DSA Signatures
- Random Number Generation

The SafeXcel-1840 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 in on-chip Dual-Port Memory, is used to control packet movements. This allows asynchronous processing between the host and the SafeXcel-1840. Descriptor Ring processing also allows multiple packets to be queued for processing, thereby avoiding 'starving' of the SafeXcel-1840.

An on-chip DMA controller intelligently allocates the packet requests among the multiple packet engines. Each packet engine contains dedicated core 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
- Generates up to 20 Mbit/s of random data

PCI-X/PCI Interface

- 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 v2.2 compliant
- Bus Master and Target capability

External Memory Interface

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

Electrical

- Core Power: 1.8W
- I/O Power: 3.3V
- 25 MHz PLL clock input
- Two PLL clocks:
 - System 62.5 MHz max.
 - Exponentiator 210 MHz max.
- Power consumption: 3.0 W max.
- Power reduction by programming lower clock speeds

Package

- 456-pin 35 x 35 mm PBGA
- Pin-compatible with SafeXcel-1842, allowing for easy migration path to higher performances

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.

