Benefits

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

SafeXcel-1841

High-Performance Security Co-Processor

The SafeXcel™-1841 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-1841 accelerates the algorithms used 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 co-processor delivers high security and high performance at the best price in the industry.

Efficient Data, Control, and Management Architecture

The SafeXcel-1841 supports PCI-X, SPI-3, and S/DRAM memory interfaces to ensure easy integration with the widest variety of network and host processors. The SafeXcel-1841 can flexibly use different interfaces for data, control, and security association (SA) database access.

Complete VPN Security Features

Several features are implemented in hardware that are not available with other competitive chip solutions 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-1841 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-1841 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-1841 quickly and easily. The kit includes drivers, documentation, and sample code.

Complete Hardware and 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 use the SafeXcel co-processors for accelerating IPSec packet processing and IKE.
Technical Specifications

**IPSec Performance**
- Sustained ESP: SPI-3 (data) + EMI (SA)
  - AES/SHA-1:
    - 2.0 Gbps (1500-byte packets)
    - 1.9 Gbps (350-byte packets)
    - 1.2 Gbps (64-byte packets)
- 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
- 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.

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

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

**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
- Asyc dual port SDRAM, Sync dual-port SDRAM, and PC-100/133 SDRAM supported

**Electrical**
- Core Power: 1.8V
- I/O Power: 3.3V
- 35 MHz PLL clock input
- Two PLL clocks: System 62.5 MHz max.; Exponentiator 210 MHz max.
- Power consumption: 3.8 W max.
- Power reduction by programming slower clock speeds

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

---

**SafeXcel -1841 Architecture Overview**

---

**Contact**

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