

## Technical Features

### IPSec Performance

- 535 Mbps sustained ESP (AES, SHA-1, 1500 byte packets)
- 321 Mbps sustained ESP (3-DES, SHA-1, 1500 byte packets)

### Symmetric Crypto Block

- 590 Mbps Single-DES
- 306 Mbps Triple-DES
- 525 Mbps AES
- Supports all DES & AES modes: ECB, CBC, OFB, and I, 8, 64-bit CFB (DES), 128-bit CFB (AES)
- AES - Supported key lengths: 128, 192, and 256-bit
- Multi-mode padding support
- Implements complete IPsec ESP transforms
- Large 2 Kbyte I/O buffers allow efficient data transfers

### Hash Block

- 451 Mbps MD5
- 674 Mbps SHA-1
- Implements IPsec AH and HMAC
- Intelligent mutable bit handler for AH, including IPv4 option and IPv6 extension headers

### Public Key Accelerator

- Accelerator for math-intensive public key operations
- Supports up to 2048-bit modulus size
- Diffie-Hellman negotiate: 10 ms (1024-bit modulus, 180-bit exponent)
- RSA 1024-bit sign: 8.4ms
- RSA 1024-bit verify: 0.85ms
- DSA Sign: 8.9ms
- DSA Verify: 20.5ms

### Random Number Generator

- Hardware-based non-deterministic Random Number Generator (RNG)
- Can internally generate session keys, IV's, nonce's, cookies, public and private keys, etc.
- Up to 1 Mbit of random data per second

# SafeXcel-1741

## High Integration Security Co-processor IC

The SafeXcel™-1741 is a highly integrated VPN security co-processor that is optimized for very cost-sensitive designs. The SafeXcel-1741 incorporates security engines for the following protocols:

- IPSec ESP and AH transforms
- Basic encrypt/decrypt and hash operations

The SafeXcel-1741 includes new features such as:

- Advanced Encryption Standard (AES) algorithm
- 5V tolerant I/O
- Allows a small on-chip SA cache
- Supports a 33MHz PCI bus
- Hardware endian swapper

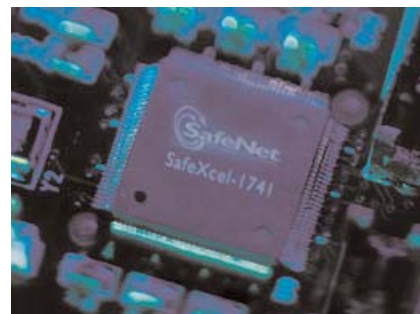
Not only are the basic algorithms supplied in the SafeXcel 1741, but the surrounding protocol handling, including header addition and stripping is included as well. The SafeXcel-1741 implements security features in hardware that are unavailable with any other chip solution in its price range, such as:

- ESP and AH header insertion and validation, including SPI and replay counter processing
- Full AH 'mutable bit' processing, including IPv4 option and IPv6 extension headers
- HMAC ICV validation on inbound packets
- Automatic IV generation and insertion

All of these features are designed to provide the maximum off-load for the host processor so that it can dedicate more of its resources to its primary functions such as routing or firewall filtering.

### Cost-Effective Acceleration

The SafeXcel-1741 provides the optimum price-performance point for low to mid-range systems. It is an ideal complement



to the fully integrated SafeNet 214x solutions that can satisfy higher system throughputs. By accelerating only the critical and processor-intensive security functions, the SafeXcel-1741 provides an excellent value proposition.

### Full Suite of Algorithms

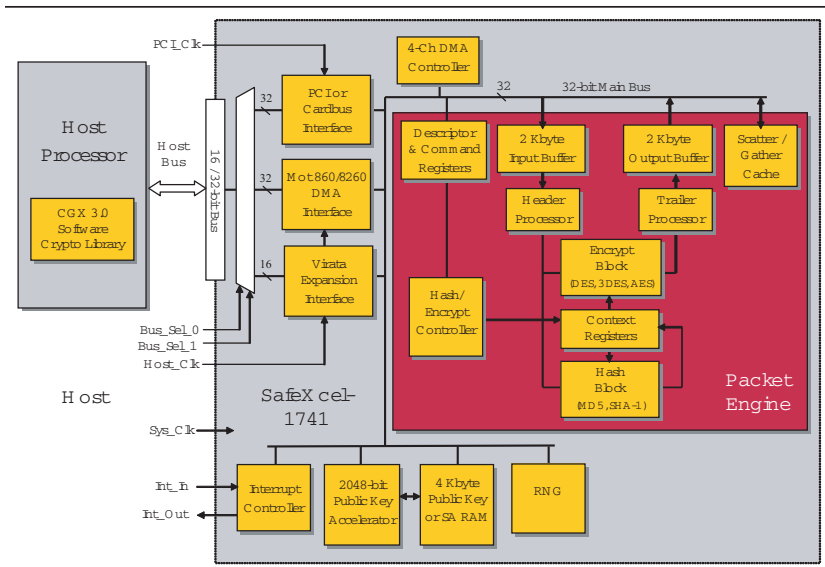
With the SafeXcel-1741 installed, host processors can off-load not only VPN packet transforms, but also the cryptographic computations needed for key management handshaking (i.e. IKE) which can have a serious impact on system performance. The public key processor in the SafeXcel-1741 will typically provide more than 20 times the performance of a 32-bit RISC processor.

### Efficient Security Processing

The SafeXcel-1741 truly offloads the Host processor, freeing it to execute its networking functions and leaving room for future feature growth. Although its performance throughput is scaled down, it still retains most of the hardware processing optimizations.

The system integration features in the SafeXcel-1741 have been carefully designed to remove performance bottlenecks. By performing virtually all of the security protocol steps on-chip, multiple bus movements are avoided, and operations may be pipelined to minimize latency.

A simple command descriptor is used to control packet processing. With the PCI host interface, the SafeXcel-1741 can



perform master PCI bus transactions to autonomously move packets through the Packet Engine.

When processing IPSec with the algorithms 3-DES and SHA-1, the SafeXcel-1741 supports 321 Mbps of throughput. This is more than adequate for SOHO routers, xDSL modems, Cable modems, and other similar applications.

### 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.

## Technical Specifications

### DMA Block

- 4-Channel, 32-bit DMA controller
- Supports DMA between Host bus interface and all internal registers and memories

### PCI Interface

- 32-bit 3.3V/5V tolerant bus interface
- 66MHz bus speed
- PCI v2.2 Compliant
- Bus Master and Target capability

### Host Co-processor Interface

- Can be interfaced with virtually any General-purpose processor, RISC processor, or Network Processor.
- "Glueless" interface to Motorola MPC-860, MPC-8260 and Viatra Expansion Interface
- 16-bit or 32-bit interfaces up to 66MHz
- Supports DMA burst transfers up to 32-bytes
- Supports big or little endian architectures

### Electrical

- Core Power: 2.5V  $\pm$ 10%
- I/O Power: 3.3V  $\pm$ 10%
- PCI Voltages: 3.3V or 5V
- Core Clock Speed: 66 MHz
- Power Consumption: 0.55W typical

### Package

- 128 pin Plastic TQFP
- RoHS-compliant package

### Development Support

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 developers kit includes drivers, documentation, and example usage code targeted at several common operating systems and platforms.

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

[www.safenet-inc.com](http://www.safenet-inc.com)

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.