

SafeNet™

SafeXcel 182-PCI Card

High Performance Cryptographic Acceleration

The SafeXcel™ 182-PCI Card is a highly integrated, high speed network security PCI-X plug-in card targeted to VPN applications in mid to high-range network devices and appliances.

With the SafeXcel 182-PCI Card accelerator card installed, system applications can off-load the burden of time-consuming crypto applications that can have a serious effect on system performance. This means that the host processor has more free cycles to perform its main tasks and leaves room for additional features to be implemented.

**The SafeXcel
182-PCI Card
has the best
price/performance
value in the
industry**



The SafeXcel 182-PCI Card delivers complete IPsec processing, including full header and trailer handling for ESP and AH. It also provides acceleration for IKE handshaking, including the very processor-intensive public key computations.

Designed for the VPN Appliance Market and Optimized for IPsec

With the acceleration of VPN performance in mid to high-end network devices and appliances as a design focus, the SafeXcel 182-PCI Card provides powerful and efficient IPsec processing. By accelerating only the critical and processor-intensive security functions, the SafeXcel 182-PCI Card delivers high security

and high performance at the best price in the industry. The SafeXcel 182-PCI Card also accelerates the algorithms used to implement SSL VPNs, allowing vendors to create multi-functional security appliances with a single security co-processor.

Efficient Data, Control, and Management Architecture

The SafeXcel 182-PCI Card incorporates separate interfaces for data, control, and security association (SA) database access, enabling both fast packet processing and highly efficient control and SA management systems. The SafeXcel 182-PCI Card also incorporates convenient

and common hardware interfaces, supporting PCI-X, SPI-3 (optional), and S/DRAM memory interface capabilities to ensure easy integration with the widest variety of network and host processors, such as IBM NP4GS3, Intel IXP 2400, and Agere APP5xx.

Broad Platform Support

Full driver support is available immediately for development on most common Operating Systems, including Windows, Linux and VxWorks. A variety of other OSs are already supported, and additional OS driver support can be delivered on request.

Complete VPN Security Features

The SafeXcel 182-PCI Card incorporates a complete suite of security features in hardware, including:

- IPsec Security Protocols: ESP and AH
- Basic (bulk) encrypt/decrypt and hash operations
- SSL, TLS, and MPPE cryptographic operations

Not only are the core algorithms supplied in the SafeXcel 182-PCI Card, but the surrounding protocol handling, including header insertion and stripping, is also incorporated in the design. Several features are implemented in hardware that are unavailable with other competitive PCI-X 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

Full Suite of Algorithms

The SafeXcel 182-PCI Card incorporates all of the necessary algorithms for IPsec and SSL applications:

- AES, DES, Triple-DES and ARC4 encryption
- MD-5 and SHA-1 Hashing with HMAC
- Public Key computations:
 - Diffie-Hellman Key Negotiation
 - RSA Encryption & Signatures
 - DSA Signatures
- Random Number Generation

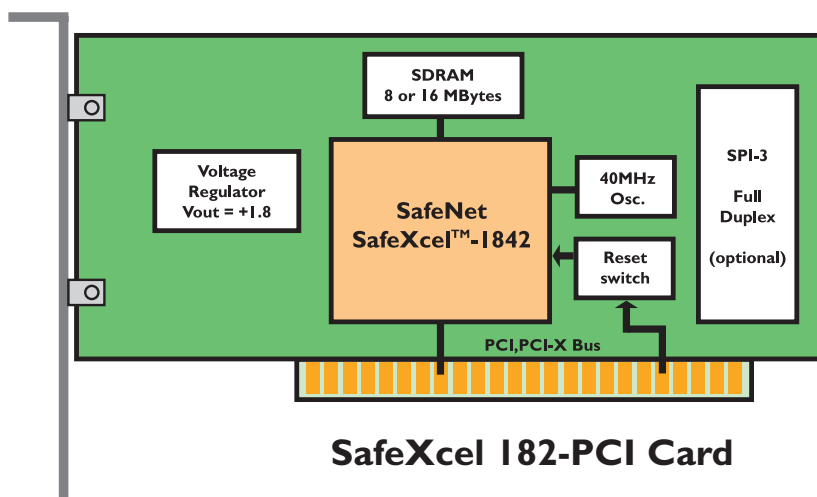
Power, Flexibility, and High-Assurance

The SafeXcel 182-PCI Card offers plenty of design flexibility with a variable-rate public key operations clock that allows trade-offs between public key processing speed and power consumption. And as a feature of SafeNet's commitment to high assurance design, the SafeXcel-1842 chip contained on the SafeXcel 182-PCI Card has all been implemented with FIPS compliant cryptographic algorithms allowing our customers to achieve FIPS 140-2 certification for their appliances.

Gigabit Throughput

The SafeXcel 182-PCI Card achieves high throughput not only with fast core processing engines, but also with an integration strategy that has been carefully designed to remove 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 182-PCI Card. Descriptor Ring processing also allows multiple packets to be queued for processing, thereby; 'starving' of the SafeXcel 182-PCI Card is avoided.

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.



Two high speed Host bus interfaces, PCI-X and the optional SPI-3, are provided to support efficient data paths to the chip. As a result, the SafeXcel 182-PCI Card design can support full-duplex OC-24 when processing IPsec with the worst case algorithms (Triple-DES and SHA-1) and 1500-byte packets.

Applications

- **Crypto Engine for Internetworking Devices**
 - Routers & Switches.
 - VPN Gateways
 - Firewalls
- **Server IPsec or SSL accelerator**
- **iSCSI Storage Security**
- **Workstation Security Module**

SafeNet QuickSec Toolkit

Customers wanting to deploy the SafeXcel 182-PCI Card can also reduce development time by licensing SafeNet's proven QuickSec Toolkit. Unique in the security market, QuickSec can seamlessly interface with any SafeXcel security processor and be configured for any combination of host processor and operating system. Capable of taking full advantage of the features in the SafeXcel 182-PCI Card, QuickSec also provides a rich suite of commands for IKE and key management features while also transparently providing a path for future upgrades of software and hardware.

The QuickSec Toolkit leverages SafeNet's track record and experience in developing IPsec / IKE / X.509 solutions to the leading vendors in the industry. QuickSec provides application specific, high value network access features, allowing quick time to market with guaranteed and proven interoperability.

The QuickSec Toolkit implements the following for Access Networks:

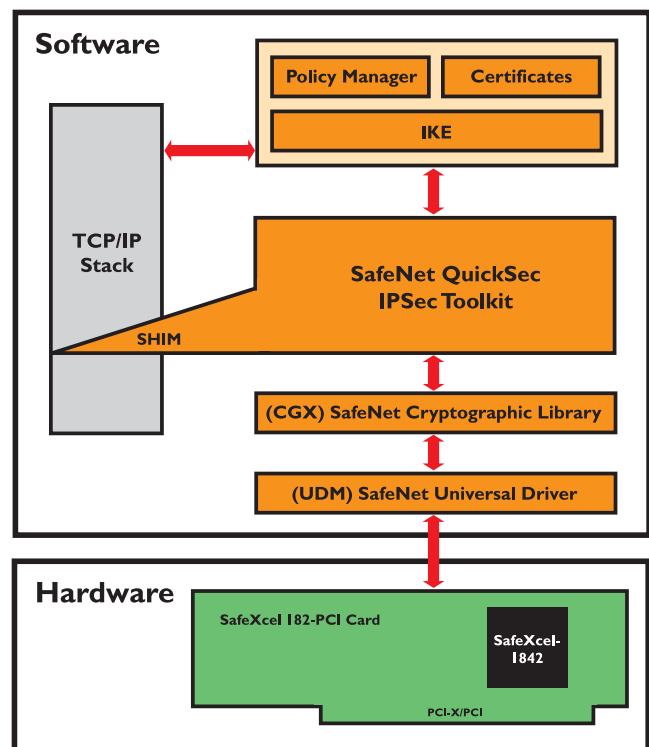
- IPsec security layer functionality:
 - IPsec packet layer
 - IKE authentication protocol
 - X.509 certificate based authentication
- TCP/IP firewall

QuickSec is targeted to access networks such as:

- Edge gateways, access concentrators
- Access devices, CPE products

Development Support

SafeNet offers developers a simple, low-cost development kit that allows OEMs to get up and running with the SafeXcel 182-PCI Card quickly and easily. The developers kit includes a Universal Driver Module (UDM) for Win NT/2000/XP, Linux, VxWorks, and Solaris platforms, documentation, sample applications and test code.



SafeXcel I 82-PCI Specifications

IPSec Performance

Sustained ESP: PCI-X (data) + EMI(SA):
AES and SHA-1

- 1.4 Gbps (1500-byte pkts)
- 900 Mbps (350-byte pkts)
- 500 Mbps (64-byte pkts)

3DES and SHA-1

- 1.3 Gbps (1500-byte pkts)
- 820 Mbps (350-byte pkts)
- 450 Mbps (64-byte pkts)

MPPE Performance (ARC4, 1500 byte packets)

- 1.3 Gbps sustained Stateless PCI-X

Crypto Block

- 2.8 Gbps Single-DES
- 2.2 Gbps Triple-DES
- 2.8 Gbps AES (256-bit key)
- 2.5 Gbps ARC4
- Supports modes: ECB; CBC
- Multi-mode Padding support

Hash Block

- 2.9 Gbps MD-5
- 2.9 Gbps SHA-1
- Implements IPSec AH and HMAC
- Includes mutable bit handler for AH, including IPv4 option and IPv6 extension headers

Public Key Accelerator

- Accelerator for math-intensive public key operations up to 2048-bit modulus.
- Diffie-Hellman negotiate: 2100 ops/sec (1024-bit modulus, 180 exponent)
- RSA 1024-bit sign: 1400 ops/sec
- RSA 1024-bit verify: 3900 ops/sec
- DSA Sign 160-bit exp: 1440 ops/sec
- DSA Verify 160-bit exp: 720 ops/sec

Protocol Support

- Full IPSec transforms including ESP, AH and bundled header/trailer processing
- Basic Encrypt, Decrypt, Hash and HMAC operations

Random Number Generator

- Hardware-based, Non-deterministic Random Number Generator
- Used to internally generate session keys, IV's nonce's, cookies, public & private keys, etc.

PCI-X/PCI Interface

- 32/64-bit 3.3V bus, 5V tolerant
- PCI: 33 or 66 MHz bus speeds
- PCI-X: 66 or 100 MHz bus speeds
- Up to 6.4 Gbps burst throughput
- PCI-X v1.0 compliant
- PCI v2.2 compliant
- Bus Master and Target capability

SPI-3 Interface (optional)

- Level 3 support
- 100 MHz max bus speed
- Two independent 32-bit interfaces: 1 RX; 1 TX
- Used for packet descriptor and packet data transport (In & Out)
- 3.2 Gbps burst transfers per direction.

On-board Memory

- SDRAM
- 8 MBytes (16 MBytes optional)

Electrical

- PCI Voltage: 3.3V / 5V \pm 10%
- PCI Bus Signaling: 3.3V (5V tolerant)
- Power Consumption: 5.5W Max
- Dynamic power reduction by programming lower clock speeds

Mechanical

- Universal PCI form factor (short card)
- 17.5 cm x 10.7 cm (6.875" x 4.2")

QuickSec IPSec Toolkit (license required)

Dynamic addressing and config.

- L2TP
- IKE Configuration
- Legacy authentication
- XAUTH
- RADIUS client
- NAT (Network Address Translation)
- Application layer gateways
- NATT (NAT Traversal)
- Enables IPSec connectivity over NATed networks
- TCP/IP Firewall
- Application layer Gateways for common applications

CGX Library (license required)

Advanced cryptographic library, with Integrated Key Management support

Targeted to Host processor

Symmetric Algorithms

- DES/3DES (HW accelerated)
- AES Rijndael (HW accelerated)
- ARC4 (HW accelerated)
- RC5

Hash Algorithms

- SHA-1 (HW accelerated)
- MD5 (HW accelerated)
- RIPEMD-128
- RIPEMD-160

Compression Algorithm

- Deflate

Protocol Support

- IPSec ESP, AH (HW accelerated)
- IPSec IKE (HW accelerated)
- IPcomp
- SSL/TLS, WTLS

Distributors and resellers located worldwide.



Corporate: 4690 Millennium Drive, Belcamp, MD 21017, USA Tel: 410.931.7500 or 800.533.3958 eMail: info@safenet-inc.com

Australia +61 3 9882 8322

Brazil +55 11 6121 6455

China +86 10 8266 3936

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 2691 7538

Japan +81 3 5719 2731

Japan (Tokyo) +81 3 5719 2731

Korea +82 31 705 8212

Mexico +52 55 5575 1441

Netherlands +31 73 658 1900

Singapore (1) +65 6274 2794

Singapore (2) +65 6297 6196

Taiwan +886 2 6630 9388

UK +44 1932 579200

UK (Basingstoke) +44 1256 345900

U.S. (Massachusetts) +1 978.539.4800

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. (Santa Clara, California)

+1 408.855.6000

U.S. (Torrance, California)

+1 310.533.8100