

# SafeXcel-I742

## Feature Rich, Highly Integrated VPN Security Co-processor IC Optimized for Cost-sensitive Designs

The SafeXcel™-I742 is a highly integrated VPN security co-processor that is optimized for cost-sensitive designs. The SafeXcel-I742 contains security engines for the following protocols:

- IPsec ESP and AH transforms
- SSL/TLS/DTLS single pass packet transforms
- SRTP packet transforms
- MACsec packet transforms
- Basic encrypt/decrypt and hash Operations

Compared to the SafeXcel-I741 the SafeXcel-I742 includes these new features:

- Support for the latests IPsec RFC's includes Extended Sequence Numbers (RFC-4304),
- SSL, TLS and DTLS, SRTP and MACsec protocol support
- ARC4 support, stateful and stateless operation
- AES Galois/Counter Mode (GCM)
  - for IPsec ESP (RFC-4106)
  - for basic operations (NIST)
- AES Galois Message Authentication Code (GMAC)
  - for IPsec (RFC-4543)
- AES-XCBC Message Authentication Code (MAC)
  - for IPsec (RFC-3566)
  - for basic operations (NIST)
- AES Counter with CBC-MAC (CCM)
  - for IPsec ESP (RFC-4309)
  - for basic operations (RFC-3610)
- Full SHA-2 support includes HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512
  - for IPsec (RFC-4868)
  - for basic operations (NIST)
- Pseudo Random Number Generator (PRNG)
  - Compliant to ANSI X9.17 Annex C
  - Can be used for automatic IV generation

For the protocol operations the SafeXcel-I742 supports not only the basic security algorithms but also the full protocol handling.



The SafeXcel-I742 implements a broad set of security features in hardware which are exceptional for a chip solution in this price range.

- IPsec full header/trailer insertion and removing for inbound and outbound packets.
- SSL, TLS and DTLS single pass processing.
- AES-GCM for MACsec
- AES-CCM for WiMAX and Wi-Fi

### Cost-Effective Acceleration

The SafeXcel-I742 provides the optimum price-performance point for low to midrange systems. By accelerating the critical and compute intensive security functions, the SafeXcel-I742 provides an excellent value proposition.

### Full Suite of Algorithms

With the SafeXcel-I742 installed, host processors can off-load not only VPN packet and MACsec frame transforms, but also the cryptographic computations needed for key management handshaking (i.e. IKE) that can have a serious impact on system performance. The public key processor in the SafeXcel-I742 will typically provide more than 20 times the performance of a 32-bit RISC processor.

### Efficient Security Processing

The SafeXcel-I742 truly off-loads compute intensive security functions from the Host processor, freeing it to execute its networking functions.

### Benefits

#### Applications:

- VPN routers
- Femto- & Pico-cells
- Cable & xDSL modems
  - VoIP
- WiMAX and WiFi
- FTTH (Fiber To The Home)

#### Protocol support:

##### IPsec ESP and AH packet transforms

- Support for latest IPsec RFCs (RFC-3566, 430x, 4434, 4543, 4868)
- Extended Sequence Number Support (RFC-4304)
- Header and trailer processing
  - Mutable-bit handling
  - Replay protection
- IPv4 and IPv6 support (RFC-4301)
- Performance: 760 Mbps (ESP, AES-SHA-1, 1500 Byte packets)

##### SSL / TLS / DTLS

- SSL, TLS and DTLS transforms (RFC-4346, 4347)
- Single pass packet transforms
  - Full header processing
  - Replay protection

##### SRTP

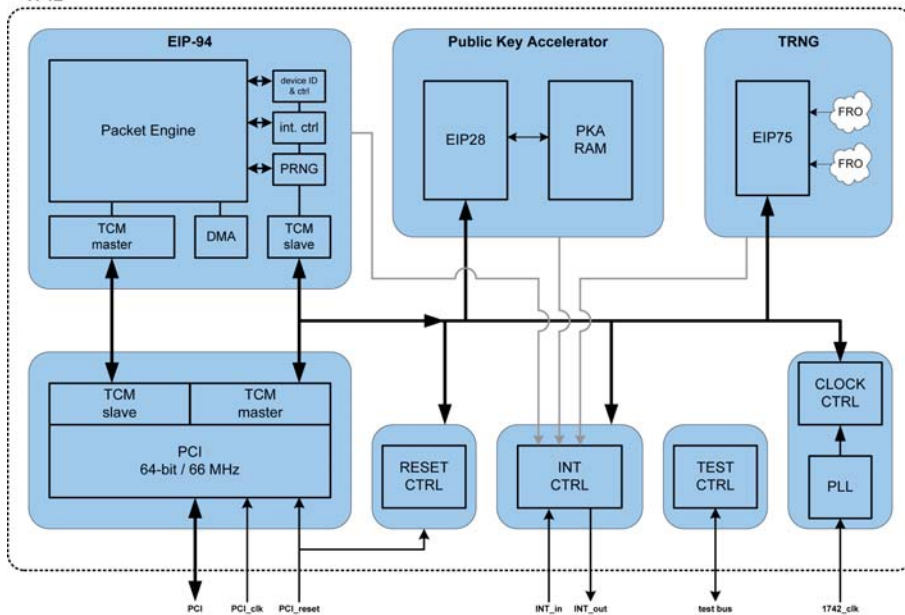
- SRTP packet transforms (RFC-3711)
- ROC removal and TAG generation and insertion
- Variable offset of header length per packet

##### MACsec

- Header insertion and removal (IEEE Std. 802.1AE-2006)
- Integrity only or integrity and confidentiality mode

**Unlimited number of Security Associations**





The SafeXcel-1742 is designed to remove performance bottlenecks by the integration of system security functions. By performing virtually all of the security protocol steps on-chip in one single pass, multiple bus movements are avoided, and operations may be pipelined to minimize latency.

With the PCI host interface, the SafeXcel-1742 can perform master PCI bus transactions to autonomously move packets through the Packet Engine. A simple command descriptor ring is used to control packet processing.

When processing IPsec with the algorithms AES and SHA-1, the SafeXcel-1742 supports 750 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.

SafeNet offers developers a simple, low-cost development kit that allows OEMs to reduce their development cycle and risks. The kit

includes SafeXcel-1742 drivers, documentation, sample code, and board development collateral.

### Complete Hardware/Software Solution

Customers can significantly reduce the 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 processor and operating systems. The QuickSec software toolkit can also leverage SafeXcel co-processors for accelerating IPsec packet processing and IKE authentication.

### SafeNet OEM Security Solutions

SafeNet's comprehensive security systems are deployed by the world's leading networking OEMs, including AMCC, AMD, Cisco Systems, Hitachi, HP, Juniper Networks, Lucent Technologies, PMC-Sierra, Samsung, Siemens, and Texas Instruments, to name a few. The leading global semiconductor, telecommunications, enterprise, and wireless OEMs trust SafeNet's best-in-class security solutions for their next-generation networking solutions.

For more information about SafeNet and the QuickSec Toolkits, please visit <http://www.safenet-inc.com/oem>

## Technical Features

### Basic cryptographic ops

- (3)DES: ECB, CBC, OFB, CFB
- AES: ECB, CBC, ICM, CTR
- ARC4: stateful and stateless
- HMAC (Basic, IPsec, TLS, SRTP), MAC (SSL), GMAC (IPsec) and AES-XCBC (IPsec)
- AES-GCM (MACsec, IPsec)
- AES-CCM (WLAN, IPsec)
- SHA-1, SHA-2 (224, 256, 384 and 512-bit), MD5

### Public-Key Accelerator

- Supporting RSA, DSA, DH, ECC
- Modulus sizes up to 2k
- RSA 1024-bit sign: 5 ms (CRT)
- Local memory for storage of operands and results
- Firmware upgradeable

### True Random Number Generator

- Non-deterministic noise source
- Generation of keys, IVs, cookies and nonces
- ANSI X9.31 annex A post-processing
- Passes AIS-31

### Pseudo-Random Number Generator

- Generation of IVs for DES, Triple-DES and AES
- ANSI X9.17 annex C post-processing

## Technical Specifications

### PCI Interface

- 32-bit and 64-bit 3.3V bus
- 33 and 66MHz bus speed
- PCI v2.2 Compliant
- Bus Master and Target capability

### Electrical

- Core Power Supply: 1.8V
- I/O Power Supply: 3.3V
- PCI Voltages: 3.3V
- Core Clock Speed: 100 MHz
- Power Consumption: 0.55W typical

### Package

- 128 pin Plastic TQFP RoHS-compliant package

### Development Support

Simple, low-cost development kit featuring: drivers, documentation, board developers manual and various usage code examples enables quick and easy implementation of the SafeXcel 1742. operating systems and platforms.



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

#### Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA  
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,  
Email: [info@safenet-inc.com](mailto:info@safenet-inc.com)

#### EMEA Headquarters:

Tel.: + 44 (0) 1276 608 000, Email: [info.emea@safenet-inc.com](mailto:info.emea@safenet-inc.com)

#### APAC Headquarters:

Tel.: + 852 3157 7111, Email: [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

For all office locations and contact information, please visit [www.safenet-inc.com/company/contact.asp](http://www.safenet-inc.com/company/contact.asp)

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.  
PB-SafeXcel1742-10.16.08