

SafeXcel-I746

Feature-rich HSM, VPN and SSL Security Co-processor IC Optimized for Designs requiring High Performance Public Key Acceleration



The SafeXcel™-I746 is a Security Co-Processor designed to offload a Host processor, providing acceleration of cryptographic functions and reducing power in power-conscious products. The ultra high performance Public Key Accelerator sub-system facilitates use as SSL accelerator, HSM engine or secure high-performance Public Key signature generator/checker. The integrated Packet Engine allows use in DSL routers, SOHO routers, Cable Modems, Firewalls and VPN Appliances.

Combining the SafeXcel-IP-94 Packet Engine Core with the SafeXcel-IP-154 Public Key Accelerator Farm, the SafeXcel-I746 chip implements security engines for the following protocols:

- RSA, DH, DSA, ECDSA public key algorithms
- 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-I742, the SafeXcel-I746 adds a farm of 10 very high performance Public Key Accelerator cores, allowing up to 7,700 RSA-1024 sign operations per second (using CRT). The SafeXcel-I746 adds black private key decrypt using AES ECB or OFB.

Compared to the SafeXcel-I84x or SafeXcel-I741, the SafeXcel-I746 includes these new features:

- Support for the IPsec v3 RFC's, including ESN
- SSL, (D)TLS, SRTP and MACsec protocol support
- ARC4 support, stateful and stateless operation
- AES Galois/Counter Mode (GCM) for IPsec ESP (RFC-4106) and for basic operations (NIST)
- AES Galois Message Authentication Code (GMAC) for IPsec (RFC-4543)

- AES-XCBC Message Authentication Code for IPsec (RFC-3566) and basic operations (NIST)
- AES Counter with CBC-MAC (CCM) for IPsec ESP (RFC-4309) and 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) and for basic operations (NIST)
- Pseudo Random Number Generator, compliant to ANSI X9.17 Annex C, for automatic IV generation

For the protocol operations the SafeXcel-I746 supports not only the basic security algorithms, but also the full protocol handling.

The SafeXcel-I746 combines the implementation of a broad set of security features with very high performance public key acceleration in hardware which are exceptional for a chip solution in this price range.

- High level acceleration of algorithms: RSA, DH, DSA and ECDSA, not limited to raw large number modular operations only.
- IPsec full header/trailer insertion and removing for in- 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-I746 provides the optimum price performance point for low to midrange systems. By accelerating the critical and compute intensive security functions, the SafeXcel-I746 provides an excellent value proposition.

Benefits

Applications:

- SSL & IPsec VPN routers
- HSMs
- FTTH (Fiber To The Home)

Protocol support:

Public Key Acceleration

- 7,700 RSA-1024 ops/sec
- Upto 4160 bit modulus
- High level key negotiate & sign/verify operations
- 4 independent command/result queues
- Hi Assurance mode with secure boot & zeroize inputs
- Black private key decrypt with AES

IPsec ESP and AH packet transforms

- Support for latest IPsec RFCs (RFC-3566, 430x, 4434, 4543, 4868)
- ESN Support (RFC-4304)
- Header and trailer processing
- IPv4 and IPv6 support (RFC-4301)
- Performance: 1200 Mbps (ESP, AES-SHA-1, 1500 Byte packets)

SSL / TLS / DTLS

- SSL, TLS and DTLS transforms (RFC-4346, 4347)
- Single pass packet transforms

SRTP

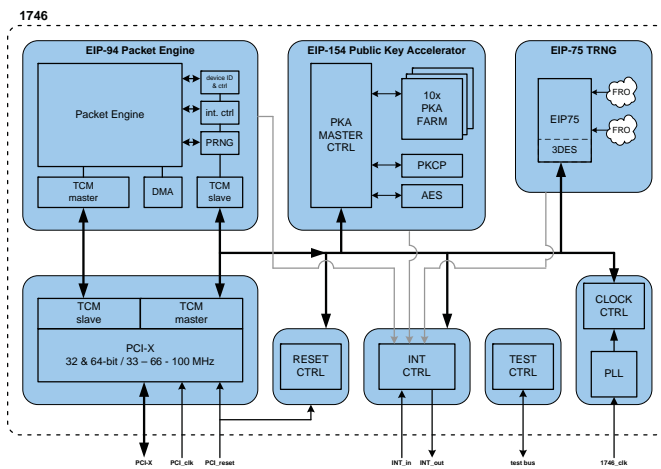
- SRTP packet transforms (RFC-3711)

MACsec

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

Unlimited number of Security Associations





Full Suite of Algorithms

With the SafeXcel-1746 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 or SSL handshakes) that can have a serious impact on system performance. The public key accelerator in the SafeXcel-1746 will typically provide more than 1000 times the performance of a 32-bit RISC processor.

Efficient Security Processing

The SafeXcel-1746 truly off-loads compute intensive security functions from the Host processor, freeing it to execute its networking functions.

The SafeXcel-1746 is designed to remove performance bottlenecks through 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-X host interface, the SafeXcel-1746 can perform master PCI bus transactions to autonomously move packets through the PKA Farm and Packet Engine. Multiple command descriptor rings are used to control (concurrent) Packet and PKA processing.

When processing IPsec with the algorithms AES and SHA-1, the SafeXcel-1746 supports 1.2 Gbps 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-1746 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

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

Technical Features

Public-Key Accelerator

- Implements RSA, (EC)DSA, (EC)DH
- Modulus sizes up to $4k+64$
- RSA 1024-bit sign: 7700/sec (CRT)
- DH 180-bit negotiate: 14000/sec
- DSA 160-bit sign: 48000/sec
- ECDSA 192-bit sign: 3100/sec
- ECDSA 384-bit sign: 1000/sec
- Local memory for storage of operands and results
- Firmware upgradeable

Basic cryptographic ops

- (3)DES: ECB, CBC, OFB, CFB
- AES: ECB, CBC, ICM, CTR
- ARC4: stateful and stateless
- HMAC, MAC, GMAC and AES-XCBC
- AES-GCM, AES-CCM
- SHA-1, SHA-2 (224..512-bit), MD5

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 & diehard

Pseudo-Random Number Generator

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

Technical

Specifications

PCI-X Interface

- 32-bit and 64-bit 3.3V bus
- 33, 66 & 100 MHz bus speed
- PCI-X v1.0a / PCI v2.2
- Bus Master and Target capability

Electrical

- Core Power Supply: 1.2V
- I/O Power Supply: 3.3V
- PCI Voltages: 3.3V
- Core Clock Speed: 166 MHz
- Power Consumption: <1W typ, 1.8W max

Package

- 208 pin 23x23mm BGA RoHS compliant package

Environment

- Industrial temperature range (-40 .. +85 °C)

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-1746, operating systems and platforms



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

EMEA Headquarters:

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

APAC Headquarters:

Tel.: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2009 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-SafeXcel1746-04.01.09