PE2SFC293/A

Security Protocol Processor PCI Express Server Adapter / Freescale C293 Freescale® Based

Product Description

Silicom protocol processor PCI-Express x4 security card based on the Freescale C293 Crypto CoProcessor.

The C293crypto coprocessor family initially consists of 3 high performance crypto coprocessors, optimized for public key operations. Public key algorithms such as RSA, Diffie Hellman, and Elliptic Curve Cryptography (ECC) are the basis of digital signature and key exchange protocols that make electronic commerce possible.

The C29x product line employs C291, 2 and 3 Crypto CoProcessors. The C293 offers high-performance support for a wide range of protocols, such as: IPSEC, SSL/TLS and IPsec bulk encryption.

C293 performs the following functions:

- Modular exponentiation
- Random number generation
- Hash processing
- Bulk encryption/decryption
- Executes protocol-specific complex instructions to support SSL/TLS or IPsec security protocols

The heart of the C293 is its 3 SEC – security engines. Each engine provides design flexibility by simultaneously supporting cryptographic operations and accelerating protocol functions.

The Silicom Protocol Processor PCI Express adapter is the ideal solution for high-end and mid-end virtual private networking (VPN), firewall appliances and SSL-based appliances.

Key Features

- Single C293 Crypto CoProcessor
- Compression: See ordering information
- PCI Express Gen-2 x4 connector supporting x4, x2 and x1 links
- Dimensions: PCIe Low Profile, 64.4mm x 167.6mm
- No external power needed
- High scalability with both hardware and software scalability
    - Bulk encryption/decryption

- data compression/decompression

- 3 SEC(Security Engines), each engine supports the following functionalities
  - DMA for bus master operation
  - Job Queue Controller with two Job Rings
  - (15) Descriptor Controllers (DECOs)
- -Responsible for executing Descriptors and managing sequencing of keys, context, and data through the various CHAs
- -Performs header and trailer processing as defined by the descriptor
- Crypto Hardware Accelerators (CHAs)
  - (15) Public Key Hardware Accelerators (PKHA) supporting the following key lengths and routines
  - Modular Arithmetic in support of RSA and Diffie-Hellman (to 4096b)
  - Elliptic curve cryptography (to 1024b)
  - Point math over a prime field (Fp)
  - Point math over a binary field (F2m)
  - Montgomery Radix Constant R2 mod N
  - Greatest Common Divisor GCD(A,N)
  - Primality Test Miller-Rabin
  - DSA Sign
  - DSA Verify
  - All routines with timing equalization to defeat side channel timing attacks
  - (1) Random Number Generator
  - -NIST-compliant DRBG and SHS implementation
  - (3) Advanced Encryption Standard Accelerators (AESA)
- -Key lengths of 128-, 192-, and 256-bit
- -ECB, CBC, CTR, CCM, GCM, CMAC, OFB, CFB, and XTS
- -Differential Power Analysis Resistant design
- (3) Message Digest Hardware Accelerators (MDHA)
- -SHA-1, SHA-2 256, 384, 512-bit digests
- -MD5 128-bit digest
- -HMAC with all algorithms
- High performance Public Key Processor
  - Up to 32K 2048-bit RSA operations/second
  - Up to 115.4K 1024-bit RSA operations/second

Applications:

- VPN appliances
- VPN firewalls, routers and switches
- Secure WEB Servers and storage
- Secure Access devices

Technical Specifications

System Throughput	
System Throughout values are shown below. System values represent measured, memory-to-memory, in-system throughout on an optional platform using large buffer sizes and maximum pipelining	
Function	**C293**
Full Ipsec Processing Throughput (w/AES+SHA2)	12Gb/s
RSA 2048 bit Exponent	32Kops/s
RSA 1024 bit Exponent	115.4Kops/s
Operating Systems Support	
Operating system support:	Linux
General Technical Specifications	
Interface Standard:	PCI-Express Base Specification Revision 2.0 (5 GTs)
Board Size:	Low profile 167.6mm x 64.4mm
PCI Express Card Type:	X4 Lane
PCI Express Voltage:	+12V +- 8%
PCI Connector:	X4 Lane
Controller:	Freescale C293
Holder:	Metal Bracket
Operating Humidity:	0°C – 55°C (32°F – 131°F)

Operating Temperature:	0°C – 45°C (32°F – 113°F) Air flow requirement for this adapter is 200 LFM
Storage:	-40°C–65°C (-40°F–149°F)
EMC Certifications:	FCC Part 15, Subpart B Class A Conducted Emissions Radiated Emissions CE EN 55022: 1998 Class A Amendments A1: 2000; A2: 2003 Conducted Emissions Radiated Emissions CE EN 55024: 1998 Amendements A1: 2000; A2: 2003 Immunity for ITE Amendment A1: 2001 CE EN 61000-3-2 2000, Class A Harmonic Current Emissions CE EN 61000 3-3 1995, Amendement A1: 2001 Voltage Fluctuations and Flicker CE IEC 6100-4-2: 1995 ESD Air Discharge 8kV. Contact Discharge 4kV. CE IEC 6100-4-3:1995 Radiated Immunity (80-1000Mhz), 3V/m 80% A.M. by 1kHz CE IEC 6100-4-4:1995 EFT/B: Immunity to electrical fast transients 1kV Power Leads, 0.5Kv Signals Leads CE IEC 6100-4-5:1995 Immunity to conductive surges COM Mode; 2kV, Dif. Mode 1kV CE IEC 6100-4-6:1996 Conducted immunity (0.15-80 MHz) 3VRMS 80% A.M. By 1kHz CE IEC 6100-4-11:1994 Voltage Dips and Short Interruptions V reduc >95%, 30% >95% Duration 0.5per, 25per, 250per

Order Information

P/N	Description
PE2SFC293	Security Protocol Processor PCI Express Adapter / C293 – PKCAL Mode
PE2SFC293A	Security Protocol Processor PCI Express Adapter / C293 – SKMM Mode

1V2