M1ESC62

Protocol Processor ExpressModule Server Adapter / CN1620

Product Description

Silicom protocol processor ExpressModule server adapter is a complete ExpressModule server adapter solution that incorporates IPSec, IKE, SSL and TLS protocol processing.

The Silicom protocol processor ExpressModule adapter is a PCI-Express x4 security card based on the Cavium Nitrox PX Security macro processor.

The Silicom protocol processor ExpressModule adapter provides bulk cryptographic acceleration for 3DES, DES, AES and ARCFOUR symmetric encryption algorithms, for the SHA-1 and MD5 hash algorithm, and for the HMAC-SHA-1 and HMAC-MD5 keyed authentication algorithms. It provides public key acceleration for the RSA, DSA, and diffie-Helman asymmetric algorithms, as well as basic Modular Math functions.

The Silicom protocol processor ExpressModule adapter provides a True Random Number Generator and can use it to generate on-chip random values for Diffie-Helman key generation and DSA signatures.

The Silicom protocol processor ExpressModule adapter provides combined encryption and HMAC authentication for single authentication for single-pass Ipsec processing. It also executes protocol-specific instruction to support the SSL/TLS or IPsec/IKE security protocols.

Macro processing within the CN1620 processor, allows systems to offload high-level SSL or IPsec protocol commands that reduce the host I/O traffic and system processor to increase the total system throughput. This also frees system processor resources for other functions, increasing overall system performance.

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

Key Features

- Single Chip solutions that accelerates all cryptographic operations and the SSL, IPsec / IKE, ans CCMP protocols
- Up to 32K 180-bit Diffie-Hellman Public Key generation (groups 1,2,5)
- Up to 17K 1024-bit RSA operations/second
- Up to 2.5Gbps Bulk Data Encryption + Hashing (SSL, IPSec, or CCMP)
- Multi Algorithm support
- RSA and Diffie-Helman (Groups 1,2,5)

- DES/3DES, AES, ARCFOUR
- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- AES-GCM
- KASUMI
- SHA-256/384/512
- 200Mbps Random Number Generator
- Host Interface standard support PCI Express ExpressModule 1.0
- Hot Plug not supported. Can be supported by assembly change

Applications:

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

Technical Specifications

System Throughout 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	**Value**
Full SSL processing throughout AES+SHA	2500 Mbp/s
Full IPSec AES/SHA	2500 Mbp/s
MAX Diffie-Helman (1024-bit module, 180-bit exponent)	32000 Transaction /Second
MAX RSA 1024-bit exponent with CRT	17000 Transaction /Second
Random Number Generator	200 Mbps
Operating Systems Support	
Operating system support:	Linux

	FreeBSD
General Technical Specifications	
Interface Standard:	PCI ExpressModule Specification revision 1.0
Board Size:	168.2mm x 98mm (6.62”X3.858”)
PCI Express Card Type:	X4 Lane
PCI Express Voltage:	+12V ± 15%
PCI Connector:	X4 Lane
Controller:	Cavium CN1620
Holder:	Not included
Operating Temperature:	0°C – 50°C (32°F – 122°F)
Storage:	-20°C–65°C (-4°F–149°F)
EMC Certifications:	FCC Part 15, Subpart B Class B Conducted Emissions Radiated Emissions CE EN 55022: 1998 Class B Amendments A1: 2000; A2: 2003 Conducted Emissions Radiated Emissions CE EN 55024: 1998 Amendments 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, Amendment 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
LEDs	
LEDs location:	No LEDs
Connectors:	No Connector

Order Information

P/N	Description	Notes
M1ESC62-R	Security Protocol Processor ExpressModule Adapter / CN1620	RoHS Complaint, X4, based on Cavium CN1620, PCI-E ExpressModule

Notes:

Order information: Model P/N -R

-R: RoHS Compliant / Lead free adapter

1V0