AdvancedMC™

AM4330
AdvancedMC IPSec Module



AdvancedTCA / AdvancedMC Open Modular Solutions

The Kontron AM4330 AdvancedMC IPSec module significantly reduces the computational overhead of host processors in routers and other networking equipment, all at full-duplex gigabit speeds. This PCI-Express-based IPSec encryption module is ideal to dynamically handle both IPSec and SSL VPN processing applications deployed within mobile communications infrastructure systems, including Media Gateways (MGW), Radio Network Controllers (RNC), and Serving GPRS Support Nodes (SGSN). The AM4330 may be integrated with AdvancedTCA Carrier boards and CPU Nodes, as well as in MicroTCA-based systems.

Kontron's AM4330 is designed with a Hifn HIPP-II 8155 IPSec encryption controller which performs multi-protocol packet processing for security protocols such as IPSec (ESP and AH), SSL/TLS, L2TP, and PPTP and IPComp. The Hifn encryption controller is complemented by a PCI-X to PCIexpress bridge and, with a 128MB private memory interface, can handle more than 200,000 IPSec small sessions (optionally 500,000 small sessions).

Moreover, it enables dynamic processing of both IPv4 and IPv6 traffic flows, meaning it can support ESP transforms where IPv4 is tunneled inside IPv6 (and vice versa). The AM4330 IPSec module is available in a mid-size formfactor and supports IPMI v1.5 which simplifies the management of the Kontron Module Management Controller (MMC).

- **Mid-size formfactor**
- **IPsec encryption performance**
  - IPV4/IPV6 ESP (3DES/SHA1) 1.5Gbps (1500-byte Packet)
  - IPV4/IPV6 ESP (AES128/SHA1) 2.6Gpbs (1500- byte Packet)
- **Public key performance**
  - 1K IKE handshakes/sec (quickmode w/2DH)
  - 1K SSL/TLS handshakes/sec
- **Compression engines**
  - LZS and MPPC engines run at up to 3.5 Gbps and increase the effective data rate throughput of the 8155 when enabled
- **Support for up to 3,072-bit public keys**
- **IPMI 1.5 support plus remote upgrade capability from all IPMI interfaces (via IPMB)**

Technical Information

Compliancy
- AMC.0 R1.0
- AMC.1 R1.0

PCI-Express Features
- One (1) X4 upstream port
- Hot pluggable
- PCI-Express 1.0a compliant

PCI-X Features
- 64bits / 133MHz between PLX bridge an Hifn encryption controller

Network Security Processor Features
- Total Solution Package (Support for IPSec (ESP, AH, Transport and Tunnel Modes), IPComp, SSL/TLS, IPV4/IPV6, and 802.11i
- Gigabit Performance
- Intelligent protocol processing
- PK Support, Data Compression (Supports IPComp and Block Level Compression)
- Private Memory Support

IPMI Features
- Management Controller compliant to PICMG 3.0, AMC.0 and IPMI v1.5 rev 1.1.
- Management Controller is run time field reprogrammable without payload impact.
- Robust fail safe reprogrammation implementation (which includes two firmware images) that could perform automatic or manual rollback if a problem occurs during critical reprogramation phase.
- Remote upgrade capability from all IPMI interfaces (via IPMB)
- Management Controller self test which can detect failure under its code integrity and trig an automatic rollback.

Supervisory
- Hardware system monitor through IPMI (voltage, temperature), temperature monitor / alarm; board temperature sensor, power failure.

Mechanical
- 181.5 x 73.8 x 18.96 mm, mid-size, single-width
- Weight: TBD

Power Requirements
- Management power is less than 150 mA peak
- Payload power < 15W

Environmental

	Operating	Storage and Transit
Temperature*:	0 to 55 °C / 32 to 131°F	-40 to 70°C / -10 to 158°F
Humidity*:	5% to 90% @55°C / 131°F non-condensing	5% to 95% @40°C / 104°F non-condensing
Altitude*:	4 000m / 13,123 ft	15 000m / 49,212 ft
Shock*:	30G, half-sine 11ms each axis	Belcore GR-63-CORE Section 4.3
Vibration*:	5-500Hz. 1G, each axis	5-50Hz, 2G; 50-500Hz, 3G each axis
Airflow:	TBD	

* Designed to meet or exceed.

Reliability
MTBF: > TBD hours @ 30°C / 77°F (Telcordia SR-332, Issue1)

Safety / EMC
Designed to meet or exceed:
- Safety: UL60950 3rd ED.; CSA C22.2 Ho 60950-00; EN 60950:2000; IEC60950-1
- EMI/EMC: FCC 47 CFR Part 15, Class B; CE Mark to EN55022/EN55024

Warranty
- Two years limited warranty

Hardware Features
- IPsec encryption performance
  - IPV4/IPV6 ESP (3DES/SHA1) 1.5Gbps (1500-byte Packet)
  - IPV4/IPV6 ESP (AES128/SHA1) 2.6Gpbs (1500-byte Packet)
- Public key performance
  - 1K IKE handshakes/sec (quickmode w/2DH)
  - 1K SSL/TLS handshakes/sec
- Wide key AES (128-bit, 192-bit, 256-bit), including counter mode
- Support for up to 3,072-bit public keys
- LZS and MPPC compression engines run at up to 3.5 Gbps and increase the effective data rate throughput of the 8155 when enabled; supports IPComp and Block level compression
- Stateful packet processing and support of ARC4 algorithm maximize PPTP performance

Operating System and Software Support
- LSP for CG Linux Kernel 2.4
- Hifn HIPP SDK

Sample of complementary AMC Everywhere-enabled Kontron AdvancedTCA platforms

* Kontron AT8020 Processor Board



- Dual Intel® Dual-Core Xeon®
- Support for up to 16GB SDRAM
- **2 X Mid-Size AdvancedMC bays**
- Dual Dual-Gigabit on Fabric
- SAS interface available

Kontron builds all of its AdvancedTCA platforms 'AMC Everywhere' enabled, offering support for AdvancedMC modules in its processor, switch and carrier products. This is a major factor in providing TEMs with unprecedented flexibility in the design of new, IMS-based applications, as well as increase economies of scale by freeing up valuable AdvancedTCA system slots for other payload blades.

AdvancedMC modules are the smallest Field Replaceable Units (FRU) on the market that are hot swappable and support the RASM concept of "Reliability, Availability, Serviceability, and Maintainability". Ultimately for Service Providers and Carriers, this translates into a significantly lower OPEX with easy upgrades in the field, reduced risk for the introduction of new subscriber services, and the ability to expand networks.

* Additional Kontron Mid-Size AdvancedMC Modules

Kontron AM4301 Quad GbE Module
- Mid-size, single-width
- 4 x Gigabit Ethernet (GbE) via RJ45 connectors
- Full fast path buffer for QoS
- Virtual LANs 802.3q
- VLAN tagging
- Manages hot-swap control, power and temperature



Corporate Offices

Europe, Middle East & Africa
Kontron AG
Oskar-von-Miller-Straße 1
85386 Eching/Munich - Germany

Tel.: +49 (0)8165 77 0
Fax: +49 (0)8165 77 279

sales@kontron.com

North America
Kontron America
Corporate Office
14118 Stowe Dr
Poway, CA 92064-7147

Tel.: (858) 677-0877
Fax: (858) 677-0898
sales@us.kontron.com

Asia Pacific
Asia Pacific
4F, No. 415, Ti-Ding Blvd.,
Sec.2, NeiHu District
Taipei, Taiwan 114
Tel. +886-2-2799-2789
Fax +886-2-2799-7399

sales@kontron.com.tw

AM4330 V1.0 11/2006
All data is for information purposes only and not guaranteed for legal purposes. Subject to change without notice. Information in this datasheet has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo are registered trademarks of Kontron AG. All brand or product names are trademarks or registered trademarks of their respective owners. RoHS compliant logo means that product will be lead-free/RoHS compliant latest by June 30th, 2006. ISO 9001:2000 Quality System Registered.