



Managed IP Encryption for Network Gateway VPNs

Government departments, agencies, contractors, local authorities, public health, public safety and criminal justice organisations - as well as private sector organisations - need to protect sensitive information across networks. Today many of these organisations use a variety of services including the Internet, broadband, dial-up access and commercial communications infrastructures for Intranet and Extranet connections. It is essential that encryption products used to protect sensitive data on these networks have formal assurance and approval from the relevant authorities. At the same time, these products must be easy to integrate into the network structure and have a central management capability that enables encryptors to be 'fitted and forgotten'.

AEP Net encryptors are targeted at protecting networks carrying sensitive data. The encryptors provide both data confidentiality and source authentication for network traffic enabling high confidence Virtual Private Network (VPN) communications.

Approved by the UK Government's CESG Assisted Products Scheme (CAPS) to Enhanced Grade level and the Ministry of Defense Infosec Products Co-Operation Group, AEP Net products meet the highest standards for a Commercial Off-The-Shelf (COTS) encryptor.

AEP Net products come complete with a sophisticated central management platform that minimizes key handling and removes the need for any local encryptor management. AEP Net products are designed to integrate into existing networks seamlessly, complementing other network products - including AEP Net Remote, a remote access module designed specifically for organisations that require mobile and home workers to access Classified applications and data over the Internet.

Key Features

- "Enhanced Grade" IPSec-based IP security gateway for the government market
- VPN operation – separates private and public networks Digitally signed certificate requests (smart card based initialization)
- Automatic traffic key management using ISAKMP
- Sophisticated tamper protection and compromise control
- "Enhanced grade" IP traffic protection
- Continuous output monitor for cryptographic integrity assurance
- Continuous random number generation checks
- Self-test health check on power-up



Management

- Minimal key handling – only at the network center once every 3 years
- PKI Infrastructure – using common criteria EAL4 assured CA and AEP Net Keyper HSM
- UniCERT and AEP Net Keyper HSM
- Central control of X.509V3 certificates
- Certificate suspension and revocation giving instant "Stun" and "Kill" capability

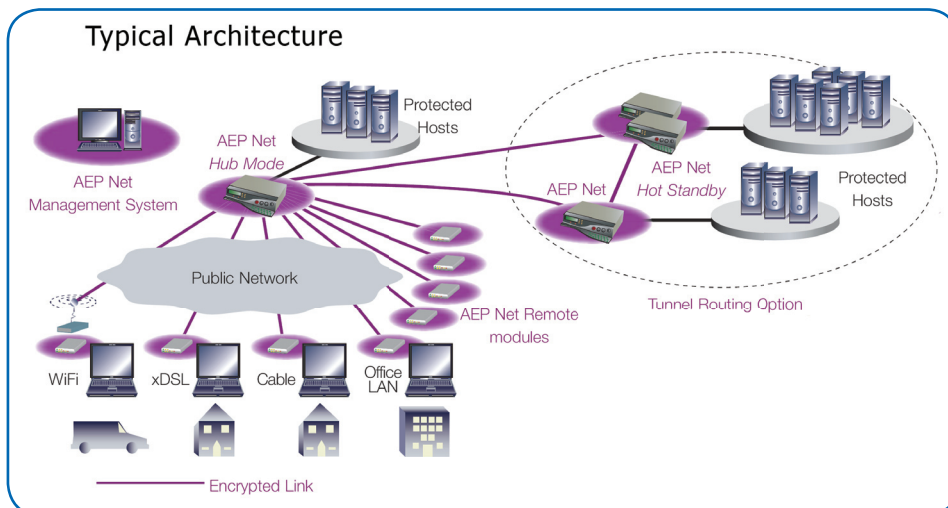
Network Integration

- Both certificate and address-based Community of Interest (COI) management
- Public and private interface routing
- SNMP in an enhanced grade environment
- Acts as a router to the private network and a host on the public network
- Supports up to 1000 secure connections
 - 10 Base-T public and 10/100 Base-T private Ethernet interfaces – true Ethernet wire rate performance
 - Secure audit and accounting
 - Resilience protocol implementation
 - NAT and DHCP support
 - Encryptor management cryptographically isolated from network traffic
 - Rack mount or desktop options

Suitable for Various Industries

AEP Net is available in different models suitable for applications in:

- UK Government
- EU Government
- US Government
- High Value Financial
- Pharmaceutical
- Other Commercial Applications



AEP Net Encryptors in Action

AEP Net products encrypt and decrypt IP datagrams. The whole of the original packet is encrypted and wrapped in a new packet, using the IP address of the destination encryptor (ESP tunnelling). The encryptors generate all transport keys and securely exchange them using the Diffie-Hellman key exchange algorithm.

AEP Net generates its own DSA signing keys to provide source authentication. A Certification Authority is used to certify the public signing key and to issue certificate revocation lists. IP address lists are created and maintained by the AEP Net Policy Manager.

Key Benefits

- Enables government business over the Internet and other open networks by protecting sensitive data to an assured standard
- Can be operated and managed by the customer organisation or by a managed service provider
- Fully automated key management eliminates administration costs of routine re-keying
- Encryption at the IP level is independent of the WAN enabling organisations to choose or change the WAN to meet their needs
- Seamless integration into existing networks
- Protection of investment as the securely programmable cryptographic kernel means that new algorithms can be loaded if required without changing the hardware
- Comprehensive GUI-based central management software suite
- Highly scalable and flexible configuration options to match the network architecture
- Designed, developed, manufactured and supported by AEP Networks, the only company to have an IPSec encryptor fully integrated with a supporting PKI that is capable of meeting stringent government security standards and ITSEC E3 independent evaluation criteria

Technical Specifications

		20M	100M
Performance	Sustained encrypted traffic throughput †	18 Mbps	160 Mbps
	Simultaneous security associations	1,000	2,000
Physical Interfaces	WAN	10 Base-T	10/100 Base-T Ethernet autonegotiation (N-way)
	LAN	10/100 Base-T Ethernet autonegotiating (N-way)	
	Serial Port	v24	
Environmental	Temperature	Operating: 5°C to +40°C Storage: -15°C to +65°C	
	Humidity	25% - 90% non condensing	
Physical Dimensions	Height	51mm	
	Width	223mm	
	Depth	244mm	
	Weight	< 4 Kg including power supply	
Power	100V to 240V, 47 - 63 Hz auto-sensing external inline mains AC to DC converter, 40VA maximum		
Electrical Safety	EN 60950: 1992/A2, 1993		
EMC	EN 50082-1, EN 55022 Class B		
MTBF	50,000 hrs, based on British Telecom HRD5 standard		

† based on 1464 byte UDP

ABOUT AEP NETWORKS

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, high assurance IPSec-based VPN encryptors, and hardware security modules for key management. Our products address the most demanding security requirements of public-sector organisations and commercial enterprises internationally. The company is headquartered in Somerset, New Jersey, with offices worldwide.

Contact Us

CORPORATE HEADQUARTERS

347 ELIZABETH AVE., SUITE 100
SOMERSET NJ 08873
TOLL-FREE: 1 877 638 4552
TEL: (+1) 732 652 5200

EUROPE

FOCUS 31, WEST WING
CLEVELAND ROAD
HEMEL HEMPSTEAD
HERTS HP2 7BW U.K.
TEL: (+44) 1442 458 600

GREATER CHINA

(MAINLAND, TAIWAN, HONG KONG)
SHANGHAI, CHINA
TEL: (+86) 136 4626 0288

JAPAN, SOUTHEAST ASIA, AUSTRALIA, NEW ZEALAND

JOYO BLDG 6-22-6
SHIMBASHI MINATO-KU
TOKYO 105-0004
JAPAN
TEL: (+81) 3 3432 3336

Accreditation

