

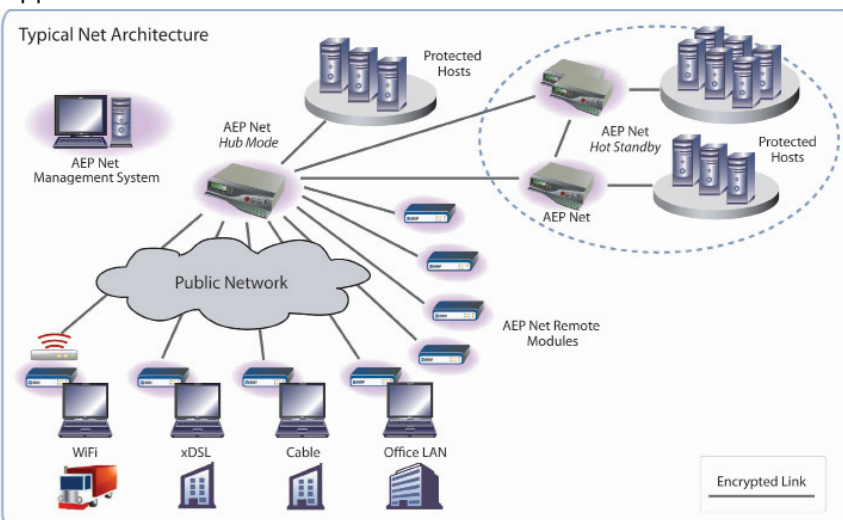
Managed IP Encryption for Network Gateway VPNs

Government departments and agencies, contractors, public health, public safety and criminal justice organizations, as well as enterprise organizations, need to protect sensitive data across networks. Encryption products used to protect data should provide centralized management across mixed environments, as well as have assurance and accreditation from relevant authorities that the solution will perform to its specifications.

AEP Series E D100/D20 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 Series E products meet the highest standards for a Commercial Off-the-Shelf (COTS) encryptor.

AEP Series E Secure products come complete with a sophisticated central management platform that minimizes key handling and eliminates the need for any local encryptor management. AEP Series E products are designed to integrate into existing networks seamlessly, complementing other network products - including AEP Series E DRemote, 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 Series E Keyper HSM
- UniCERT and AEP Series E 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
- 10Base-T public and 10/100Base-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 and Organizations

Available in different models for applications in:

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

AEP Series E Encryptors in Action

AEP Series E 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 Series E 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 Series E Policy Manager.

Cryptographic Functions and Services

- ▶ 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 organizations 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

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 autonegotiation (N-way)	
	Serial Port	v24	
Environmental	Temperature	Operating: 5°C (41°F) to 40°C (104°F) Storage: -15°C (5°F) to 65°C (149°F)	
	Humidity	25% - 90% non-condensing	
Physical Dimensions	Height	51mm (2 in)	
	Width	223mm (8.78 in)	
	Depth	244mm (9.6 in)	
	Weight	< 4 Kg (8.82 lbs) 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: 199/A2, 1993		
EMC	EN 50082-1, EN 55022 Class B		
MTBF	50,000 hrs based on British Telecom HRD5 standard		

Accreditation



United States

Toll-Free: +1-877-638-4552
Tel: +1-732-652-5200

Email: sales@aepnetworks.com

Europe

Tel: +44 1344 637 300

Web: www.aepnetworks.com

Greater China

Tel: +8621 5116 7120

SE Asia, Singapore

Tel: +852 2961 4566

Japan

Tel: +8180 5645 4503

Australia/New Zealand

Tel: +61 2 9413 2282

Malaysia

Tel: +60 32166 2260