



## Managed Personal Remote Access for High Assurance Networks

AEP Net Remote secures personal remote access communications to government Classified standards+. Using Net Remote, an organisation can enable its mobile workforce to access sensitive data over the Internet at costs previously associated with commercial remote access. Net Remote benefits from the AEP Net Management System, taking advantage of the proven key and device management features utilised by AEP's Net encryption products. Net Remote provides a highly scalable solution with flexible configuration options, allowing organisations to maximise their Return On Investment (ROI) as their business needs evolve.

### Remote Working

Government policy requires public sector organisations to offer home and mobile working to their workforce wherever possible. These bodies can now extend remote access to Classified data over a range of network access technologies including remote office LAN, broadband (over DSL or cable), and Ethernet-enabled WiFi, without the normal restrictions and overhead expenses. Net Remote delivers the throughput to satisfy a wide range of demanding applications, including VoIP and Video over IP.

### Integrates Fully with AEP Net Gateway Encryptors

AEP Net Remote works seamlessly with existing AEP Net encryptor deployments. A unique 'tunnel routing' feature transparently enables authorised remote users to access resources on AEP Net secured intranets and extranets.

### Deployment Options

Net Remote connects via an AEP Net encryptor in hub mode. It can be deployed as a stand-alone solution for remote access, or as a remote access adjunct to an existing AEP Net secured network. Communications continuity and disaster recovery options are available.

### High Assurance Standards

Net Remote provides secure personal remote access communications; it is approved to assure data confidentiality to national security standards across public networks such as the Internet and as a dedicated Ethernet device it eliminates the security issues inherent in a software or PC-integrated design (e.g., PCMCIA card).

## Ease of Deployment and Management

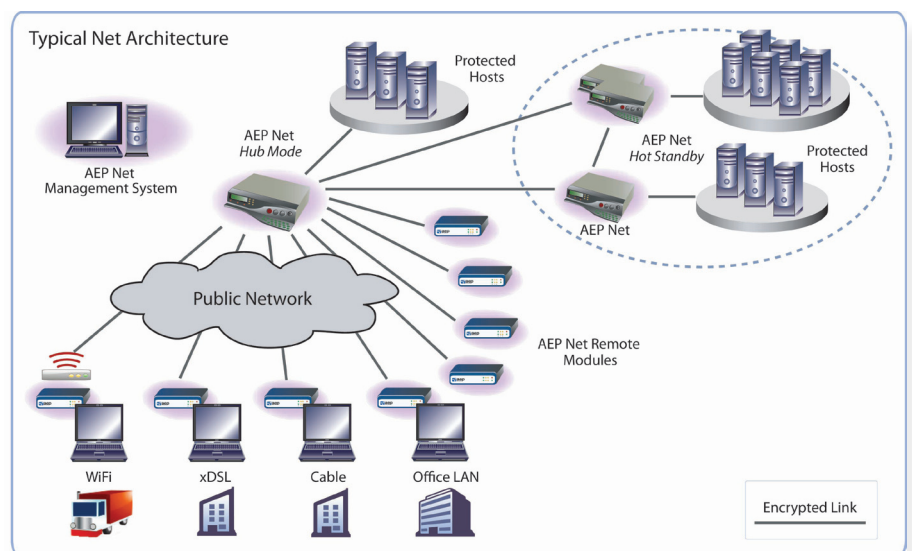
The proven AEP Net Management System has been extended to provide unparalleled scalability of security policy and key management for a remote security device. Purpose designed to facilitate rapid rollout and system evolution, the AEP Net Management System enables user communities of all sizes to be managed from the network centre.



Features include:

- Fully automated keying; no CESG key material at remote site
- Assured cryptographic separation of user communities
- Compromise control; cryptographic isolation of a suspect unit giving instant "stun" and "kill" capability in the event of compromise or loss
- No need to return units to a central site for key updates

The modular design allows operation and management by either the customer or a managed service provider and the fully automated key management eliminates most of the administration costs traditionally associated with such systems. Unique functionality enables Managed Service Providers to offer secure remote access solutions for complex user communities, including inter-operation projects.





Key Features	
<b>Net Remote</b>	
<ul style="list-style-type: none"> <li>▶ Portable IPSec-based data security module for remote access</li> <li>▶ Provides cryptographic separation of private and public networks</li> <li>▶ Dedicated Ethernet device supports 10/100 Base-T</li> <li>▶ Algorithm variants available to protect Classified data to government standard</li> <li>▶ Sophisticated tamper proofing and compromise control</li> <li>▶ Continuous output monitoring for cryptographic integrity assurance</li> <li>▶ Continuous random number generation checks</li> <li>▶ Self-test health check on power-up</li> <li>▶ Automatic traffic key management using ISAKMP</li> </ul>	
<b>Management</b>	
<ul style="list-style-type: none"> <li>▶ AEP Management System enforces security policy and provides encryptor administration and key management</li> <li>▶ AEP Net Remote and AEP Net devices supported by single AEP Management System</li> <li>▶ Highly scalable – capacity for in excess of 50,000 users</li> <li>▶ PKI authentication – using assured CA and AEP Net Keyper</li> <li>▶ Digitally signed certificate requests (smart card-based initialization)</li> <li>▶ Central control of X.509V3 certificate issuance, suspension and revocation</li> <li>▶ Encryptor management cryptographically isolated from network traffic</li> <li>▶ Both certificate and address-based Communities of Interest (COI) and Closed User Group (CUG) management, supporting hub and spoke, fully meshed and partially meshed deployments</li> <li>▶ No requirement for user to return the unit to a central site for key updates</li> <li>▶ Units can be re-keyed from the network center in the event of security compromise</li> <li>▶ Secure audit and accounting</li> </ul>	
<b>Network Integration</b>	
<ul style="list-style-type: none"> <li>▶ 10/100 Base-T public and private Ethernet interfaces</li> <li>▶ Hub side failover provides disaster recovery and maximises business continuity</li> <li>▶ Quality of Service (QoS) marker pass through</li> <li>▶ Public and private interface routing</li> <li>▶ Central connection via one or more AEP Net devices in hub mode</li> </ul>	

Technical Specifications			
<b>Performance</b>	Sustained encrypted traffic throughput †	18 Mbps	
	Remote access users per hub	20M Hub	10 concurrent
		100M Hub	100 concurrent
<b>Network Interfaces</b>	WAN	10/100 Base-T Ethernet autonegotiation (N-way)	
	LAN	10/100 Base-T Ethernet autonegotiation (N-way)	
<b>Environmental</b>	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	
<b>Physical Dimensions</b>	Height	28mm (1.1 in)	
	Width	118mm (4.65 in)	
	Depth	195mm (7.68 in)	
	Weight	.08 Kg (.18 lbs) including power supply	
<b>Power</b>	100V to 240V, 50-60 Hz auto-sensing external inline mains AC to DC converter, 28VA maximum		
<b>Electrical Safety</b>	EN 60950: 1992/A11:1997 IEC950:1991/A4:1996 + All CB Countries. CSA C22.2 No 950 UL 1505: 1995/Amended 1998 UL60950/CSA60950 AS/NZS 3260:1993/A4:1997		
<b>EMC</b>	EN 55024:1998/A1:2001 (Measured as per : IEC 61000-4-2:1995, IEC 61000-4-3:1995, IEC 61000-4-4:1995, IEC 61000-4-5:1995, IEC 61000-4-6:1995, IEC 61000-4-8:1995, IEC 61000-4-11:1995.) EN 61000-3-2:2000 EN 61000-3-3:1995/A1:2001 European Standard 55022:1994/A1:1995/A2:1997 Class B. CFR 47, Part 15 Class B. (FCC )		
<b>MTBF</b>	50,000 hrs based on British Telecom HRD5 standard		

## Accreditation



## About AEP Networks

AEP Networks offers an integrated portfolio of secure, high performance network and communications access solutions for enterprise and private sector organizations. Our secure networking products include identity-based and policy-based access control solutions, SSL VPNs, IPsec-based VPN encryptors and hardware security modules (HSMs) for key management. Our enhanced-grade communications products address the needs of organizations requiring specially designed voice and data solutions that support a wide range of communications protocols and network topologies.

### Contact Us:

#### United States

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

#### Europe

Tel: +44 1442 458 600

#### Email:

[sales@aepnetworks.com](mailto:sales@aepnetworks.com)

#### Web:

[www.aepnetworks.com](http://www.aepnetworks.com)