Key business benefits

- Defends against cyber espionage
- Secures DSL/MPLS/BGAN services
- Facilitates compliance with security mandates
- Protects integrity of control systems
- Eliminates costly dedicated

Applicable markets

- Governments: UK, EU and international
- Defence: UK MoD, NATO and international
- Government & defence contractors
- Intelligence and diplomatic services
- NGOs

Net 20M/100M encryptors

Datasheet

Organisations across the public and private sectors need to protect their sensitive, high-value communications passing over insecure wide area networks. Whether safeguarding national security, financial data or intellectual property, escalating cyber-attacks vividly demonstrate the imperative for strong network security.

Ultra Electronics AEP Net products enable the deployment of VPNs (virtual private networks) to ensure the confidentiality, integrity and availability of information in transit. Cryptographic standards are implemented to stringent government assurance levels whilst maintaining the flexibility necessary to operate in today's complex networking environments. The products also facilitate the implementation and operation of cost-efficient, shared VPNs by managed service providers, fully protecting the confidentiality of each customer's traffic and the integrity of the management functions.

End-to-end solutions

Net encryptors can also be integrated with the Ultra Communicate line of products for secure data transport over multi-bearer communications networks for end-to-end security enhancements.

AEP | Ultra ELECTRONICS

Flexible deployment

Net encryptors are available in three models and are designed to integrate into existing networks seamlessly. The Net 20M and Net 100M are VPN gateway devices, whilst the Net Remote is designed specifically for mobile and home workers who need to access highly-sensitive applications and data over the Internet. These are all supported by a sophisticated central management platform, including AEP's unique hardware Net CA (Certification Authority), which minimises key handling requirements and eliminates the need for any local encryptor management.

Government certification

Certified by the UK Governments CAPS (CESG Assisted Products Service) up to Enhanced Grade level and approved by the EU Council to protect CONFIDENTIEL UE, the government versions of the encryptors use special algorithms to meet national policy requirements across a wide range of secure systems. For the private sector, the commercial versions combine the strength of the public-domain AES encryption algorithm with the flexibility and ease-of-deployment expected by enterprise customers.

Network integration & management

- 10/100 Mbps auto-negotiating Ethernet interfaces
- ESP tunnel mode encrypted packet format
- QoS (quality of service) marker pass-through
- Up to 2,000 simultaneous IPsec security associations
- Supports data, voice and video traffic, with minimal impact on throughput or latency
- Triple-redundancy mode for high-availability applications
- Acts as a router on the private network and a host on the public network
- Supports static routes and host-side NAT
- In-band SNMP data tables and traps
- Over-the-air re-keying (OTAR)

Security features

- Dedicated hardware platform with special-purpose embedded firmware
- FPGA-based hardware encryption for enhanced security, performance and flexibility
- Choice of algorithms to suit government or commercial use
- Certified for reverse tunnelling applications
- Employs a proprietary, hardened version of the IPsec protocol
- PKI-based key management and compromise control
- Secure, in-band device management, cryptographically isolated from user traffic
- Support for cryptographically-separated COIs (communities of interest)
- Firewalls all non-authenticated traffic arriving from the public network
- High-quality, hardware random number generator
- Continuous self-monitoring of cryptographic functions
- Sophisticated tamper protection
- Secure auditing and accounting functions
- NPM ACCSEC for government handling purposes, without the need for a CIK (crypto ignition key)
- Certified to UK CAPS Enhanced Grade & Baseline Grade standards
- Approved by the EU Council for CONFIDENTIEL UE

AEP | Ultra ELECTRONICS

Net encryptors in operation

Each IP packet is encrypted in its entirety, encapsulated inside a new packet (based on the IPsec ESP tunnelling protocol) and sent to the destination encryptor, which extracts and decrypts the payload before forwarding it to the appropriate host. The encryptors generate the necessary encryption keys and exchange them securely using an asymmetric key exchange protocol; they also generate their own signing keys to provide source authentication. A customer-specific CA remotely certifies the public signing keys and issues CRLs (certificate revocation lists) based on X.509 PKI standards under the control of an authorised administrator. The VPN topology is centrally defined using AEP's sophisticated Net Policy Manager application, with configuration information being automatically pushed out to all the encryptors. This tool also provides a full range of device management, monitoring, auditing and accounting functions.

Technical specifications

		Net 20M	Net 100M
Performance	Sustained encrypted traffic throughput †	18 Mbps	160 Mbps
	Simultaneous security associations	2,000	2,000
Physical interfaces	WAN	10 Mbps Ethernet	10/100 Mbps Ethernet
	LAN	10/100 Mbps Ethernet	
	Serial Port	V.24	
Environmental	Temperature Humidity	Operating: 5 to 40°C / Storage: -15 to 65°C 25 - 90% (non-condensing)	
Physical dimensions	Height Width Depth	51 mm 223 mm 244 mm	
Weight	< 3kg (including power supply)		
Power	External, universal in-line AC power supply 100 - 240V, 47 – 63 Hz, 42W maximum		
Electrical safety	EN 60950-1, UL 60950, CSA 60950 CB Certificate (IEC 60950-1)		
EMC	EN 55022 Class B, EN 55024 EN 61000-3-2, EN 61000-3-3 FCC CFR 47 Part 15 Class A		
MTBF	> 50,000 hours, based on British Telecom HRD5 standard		

† Typical full duplex values – actual throughput and latency vary with algorithm and packet size

Solution highlights

- Secures communications over the Internet and other untrusted networks by encrypting traffic to government assurance standards
- Highly scalable and flexible configuration options facilitate seamless integration into existing networks and rapid roll-out
- Minimises down-time with automatic recovery from power failure and hot standby feature (using up to three encryptors per cluster with fast fail-over)
- Supports converged IP services: high throughput levels without packet loss, very low packet latency and QoS marker pass-through
- Encryption at the IP level is independent of the WAN technology, enabling organisations to choose or change the WAN to meet their needs
- Comprehensive, GUI-based centralised management software suite
- Automated, remote key management capabilities eliminate the administration costs of routine manual re-keying and the risk of network downtime
- Certificates can be revoked in the event of encryptors being lost, stolen or compromised, avoiding the need to re-key the whole network
- Can be operated and managed by the customer organisation or by a managed service provider
- Developed and supported by AEP, the only company with IP encryptors and a fully integrated PKI approved to stringent UK Government and EU Council security standards
- Robust solution, proven in numerous major deployments over many years

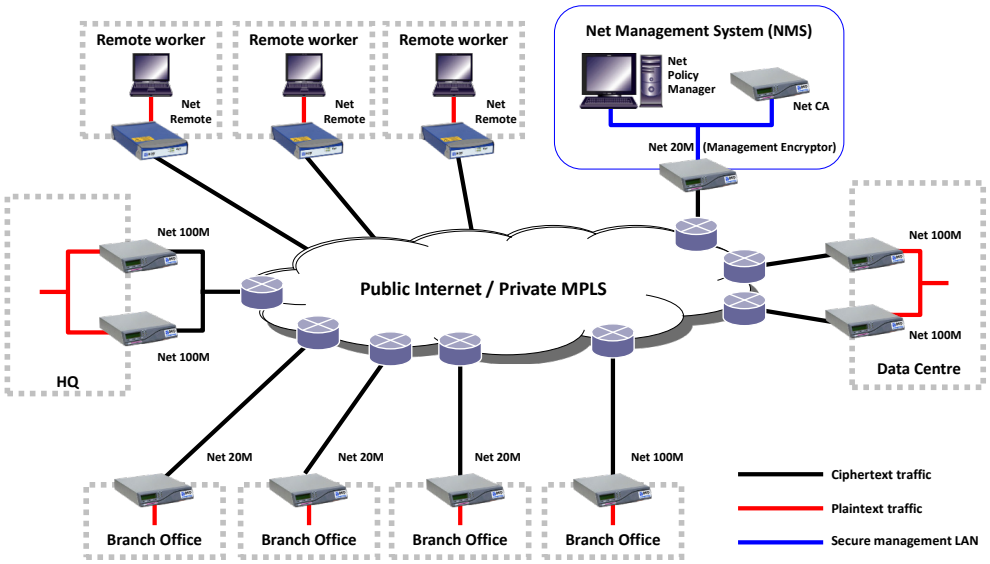
Solution summary

The Ultra Encrypt line of products comprises:

- Net 100M and Net 20M encryptors
- Net Remote encryptor
- Net Management System (incorporating Net CA and Net Policy Manager)

AEP also offers a range of off-the-shelf and bespoke deployable secure communications solutions as well as comprehensive professional services and support capabilities.

Ultra Encrypt – Typical Net Architecture



Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com