



Key business benefits

- Defends against cyber espionage
- Secures DSL/MPLS/BGAN services
- Facilitates compliance with security mandates
- Enables secure remote access
- Protects integrity of control systems
- Eliminates costly dedicated circuits
- Replaces legacy P2P encryptors

Applicable markets

- Governments: UK, EU and international
- Defence: UK MoD, NATO and international
- Government & defence contractors
- Intelligence and diplomatic services
- NGOs
- Critical national infrastructure
- Managed service providers
- Commercial enterprises

Ultra Encrypt

Product line overview

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.

The Ultra Encrypt product line enables 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.

Cost benefits

A secure VPN solution provides significant cost-savings over traditional, point-to-point private circuits. It also facilitates data sharing, secure remote access and conferencing capabilities that can drive increased efficiency and productivity whilst reducing real estate overheads, travel costs and environmental impact.

End-to-end solutions

Ultra Electronics AEP Networks Net encryptors can also be integrated with the Ultra Communicate line of products for secure data transport over multi-bearer communications networks and with the Ultra Protect line of Application Access gateway products for end-to-end security enhancements.

AEP Networks

Ultra
ELECTRONICS

Moreover, VPNs help to protect organisations from the direct or indirect financial losses and repetitional impairment that can result from security breaches.

AEP Networks further strengthens the business case for VPNs by maximising the security benefits whilst minimising the total cost of ownership. The Net encryption solution provides government-grade security with unparalleled flexibility and ease-of-use. For example: the powerful policy management tools simplify initial deployment and subsequent changes with low training overheads; the fully-centralised key management system, based on a true, standalone PKI, eliminates the costs of transporting, handling and storing large volumes of sensitive key material; cryptographic data separation enables the sharing of infrastructure and the provision of secure networks as a managed service; the certificate revocation capability mitigates the cost impact of encryptor compromises or losses; and the risk of expensive down-time is significantly reduced as a result of Nets' high-availability features and the minimal opportunity for operator mis-configuration.

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 Networks 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 Government's 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.

Typical uses

Below are some examples of how Net encryption products are being used today:

Customer Type	Typical Applications	Major Benefits
Commercial enterprises, critical national infrastructure, and NGOs	<ul style="list-style-type: none"> Virtual private networks Secure conferencing Asset protection 	<ul style="list-style-type: none"> Government-grade security Assists compliance with data protection legislation Flexibility Ease of use
Government departments	<ul style="list-style-type: none"> Inter-office communications Remote working 	<ul style="list-style-type: none"> Confidentiality Cost savings Business continuity
Pan-government intranets	<ul style="list-style-type: none"> Inter-departmental communications Application and data sharing 	<ul style="list-style-type: none"> Confidentiality Increased efficiency Cost savings
Military and defence	<ul style="list-style-type: none"> Fixed infrastructure In-theatre communications Reverse tunnelling Remote working 	<ul style="list-style-type: none"> Confidentiality Centralised key management Ease of use
Diplomatic and intelligence services	<ul style="list-style-type: none"> Embassy communications Field operative communications 	<ul style="list-style-type: none"> Confidentiality Centralised key management Portability
Managed service providers	<ul style="list-style-type: none"> Secure managed network services platform 	<ul style="list-style-type: none"> Manageability High availability Scalability Low cost of ownership

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 Networks, 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

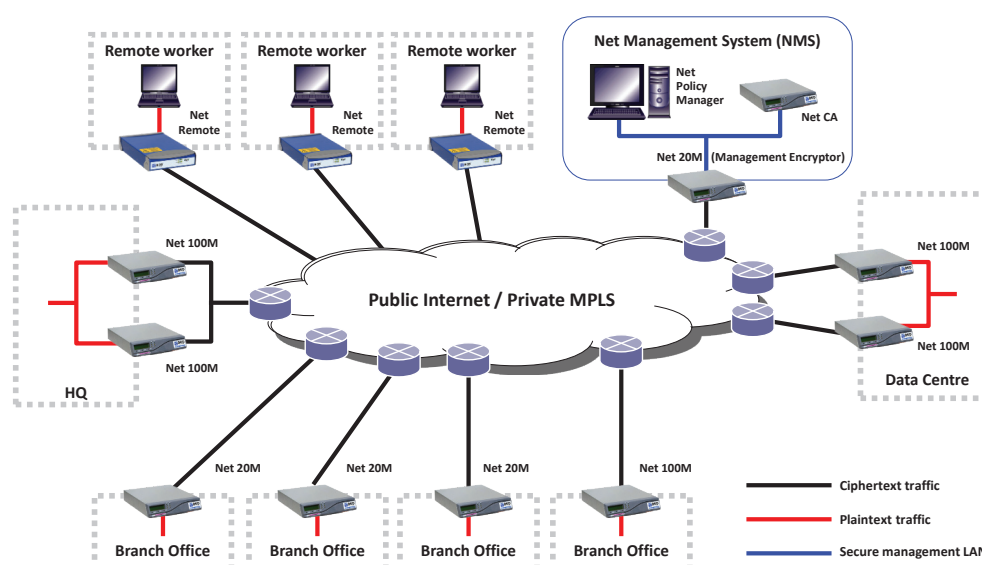
Solution summary

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 Networks also offers a range of off-the-shelf and bespoke deployable secure communications solutions as

Ultra Encrypt – Typical Net Architecture



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

Ultra Electronics reserves the right to vary these specifications without notice.
© Ultra Electronics Limited 2012.