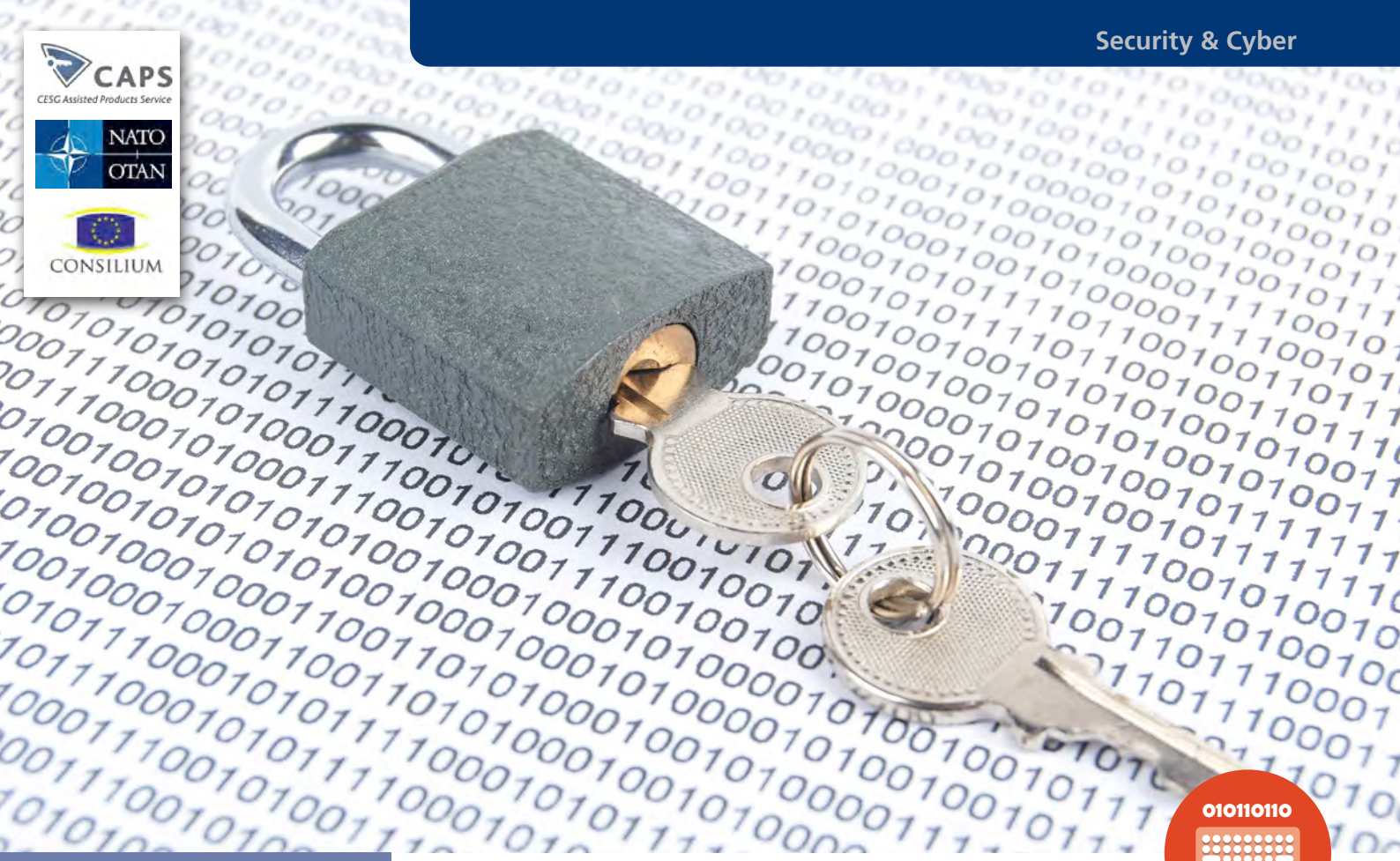
CAPS
CESG Assisted Products Service
NATO OTAN
CONSILIUM



Key business benefits

- Enables secure remote access
- Safeguards data confidentiality and integrity
- Facilitates compliance with security mandates
- Insulates client devices from internet threats
- Maintains network perimeter security

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

Net Remote encryptor

Datasheet

Organisations across the public and private sectors increasingly need to provide their employees with remote access to corporate data and applications from home or whilst travelling. However, sensitive information leaving the corporate network boundary must be protected from interception and attack, especially where sensitive personal or company data, intellectual property or national security are concerned. Moreover, a lost or compromised laptop PC could offer attackers a vector into the corporate network itself.

Ultra Electronics AEP Net Remote encryptor is a hardware VPN (virtual private network) client that offers an exceptional level of assurance where security is paramount.

End-to-end solutions

Net Remote can be deployed as a stand-alone solution for remote access, or as a remote access adjunct to an existing site-to-site VPN using Net encryptors. Communications continuity and disaster recovery options are available. For mobile personnel, AEP offers solutions integrated with our Ultra Communicate line of multi-bearer communications modules – please refer to our SecComm solutions for further details.

AEP | Ultra ELECTRONICS

Unlike traditional software VPN clients, the security of which is ultimately dependent upon the underlying PC platform, Net Remote is a dedicated encryption device that operates completely independently of the user's PC.

This makes it immune to the zero-day exploits that are discovered every month in PC operating systems, web browsers and other common software applications. Furthermore, Net Remote retains no sensitive key material whilst disconnected or switched off, so it has no special storage requirements and presents no particular security threat if lost or stolen. Once the user has authenticated to the Net Remote, it connects securely to the central VPN concentrator (provided by a Net 20M or Net 100M encryptor) and ensures that all data to and from the PC is constrained to this secure tunnel and fully encrypted. Net Remote offers high throughput and low latency to satisfy a wide range of demanding applications, including the use of voice and video. It can also play a vital role in emergency or disaster recovery scenarios where workers need speedy secure access to their corporate systems from home or a temporary location.

Flexible deployment

Net Remote can be used wherever there is a wired Ethernet connection available, such as with home broadband services, hotel networks, office LANs and satellite terminals. It provides a highly scalable solution with flexible configuration options, allowing organisations to maximise their ROI (return on investment) as their business needs evolve. It is supported by a sophisticated management platform, purpose-designed to facilitate rapid roll-out and system evolution, enabling user communities of all sizes to be managed from the centre.

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 Net Remote use special algorithms to meet national policy requirements across a wide range of secure systems. For the private sector, the commercial version combines the strength of the public-domain AES encryption algorithm with the flexibility and ease-of-deployment expected by enterprise customers.

Net Remote 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 concentrator, which extracts and decrypts the payload before forwarding it to the appropriate server. 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.

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
- 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
- No special storage requirements, as no key material is retained when disconnected or switched off
- Certified to UK CAPS Enhanced Grade & Baseline Grade standards
- Approved by the EU Council for CONFIDENTIEL UE

Network integration and management

- 10/100 Mbps auto-negotiating Ethernet interfaces
- ESP tunnel mode encrypted packet format
- QoS (quality of service) marker pass-through
- Scalable to over 50,000 remote users
- Supports data, voice and video traffic, with minimal impact on throughput or latency
- Over-the-air re-keying (OTAR)
- Supports alternative concentrators for business continuity or disaster recovery
- Common management system for remote access and site-to-site VPNs

Technical specifications

Performance	Sustained encrypted traffic throughput †	18 Mbps
	Remote access users per concentrator	Net 20M Concentrator: 100 (10 concurrent) Net 100M Concentrator: 1,000 (100 concurrent)
Physical interfaces	LAN	10/100 Mbps Ethernet
	WAN	10/100 Mbps Ethernet
Environmental	Temperature Humidity	Operating: 5 to 40°C 25 - 90% (non-condensing)
Physical dimensions	Height Width Depth	35 mm 126 mm 197 mm
Weight	0.9kg (including power supply)	
Power	External, universal in-line AC power supply 100 – 240V, 50 - 60 Hz, 21 - 28 VA	
Electrical safety	EN 60950-1, UL 60950-1, CSA 60950-1 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 B	
MTBF	> 50,000 hours, based on British Telecom HRD5 standard	

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

Solution highlights

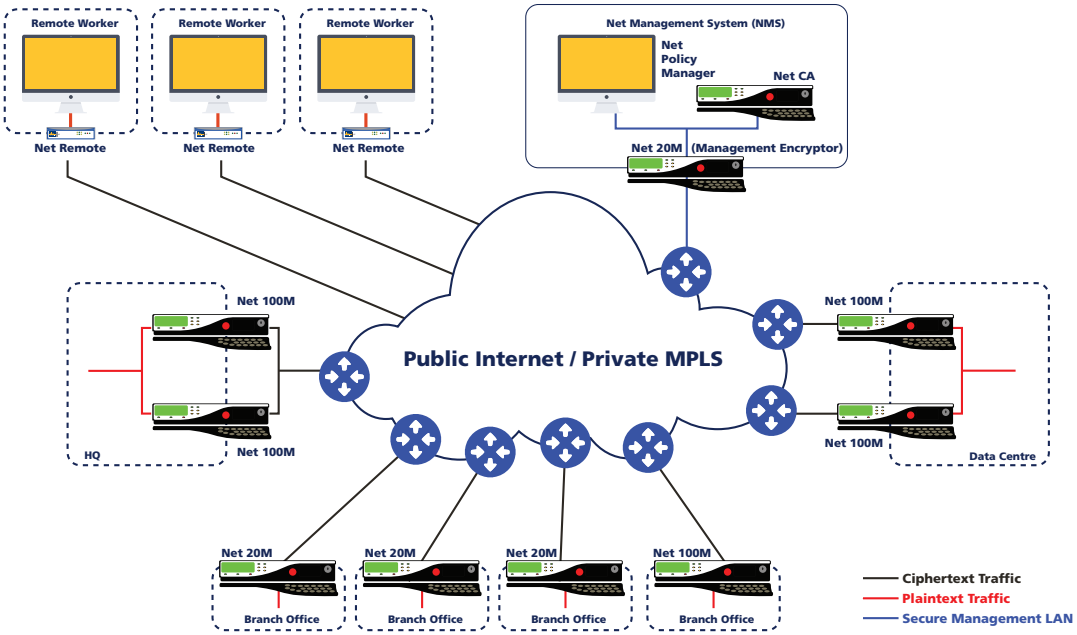
- Secures remote access over the Internet and other untrusted networks by encrypting traffic to government assurance standards
- Highly scalable to facilitate rapid roll-out and system evolution
- Flexible configuration options to support business continuity and disaster recovery
- Comprehensive, GUI-based 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 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

Made in Britain

ISOQAR REGISTERED 0026 UKAS MANAGEMENT SYSTEMS

ISO 27001