



ULTRA ENCRYPT NET 20M/100M ENCRYPTORS DATASHEET



- 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 CIRCUITS

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 Encrypt 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 and with the Ultra Protect line of Application Access gateway products for end-to-end security enhancements.

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 IPsec 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 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 use at UK OFFICIAL and in 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



APPLICABLE MARKETS

- GOVERNMENTS: UK, EU AND INTERNATIONAL
- DEFENCE: UK MOD, NATO AND INTERNATIONAL
- GOVERNMENT & DEFENCE CONTRACTORS
- INTELLIGENCE AND DIPLOMATIC SERVICES
- NGOS

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 negligible impact on throughput and under 4 µs 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

- Applications specific, 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)
- Drops 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 for use at UK OFFICIAL
- Approved by the EU Council for CONFIDENTIAL UE

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 negotiate the necessary session encryption keys without exchanging them over the untrusted network using an asymmetric key exchange protocol; they also generate their own signing keys to provide source authentication.

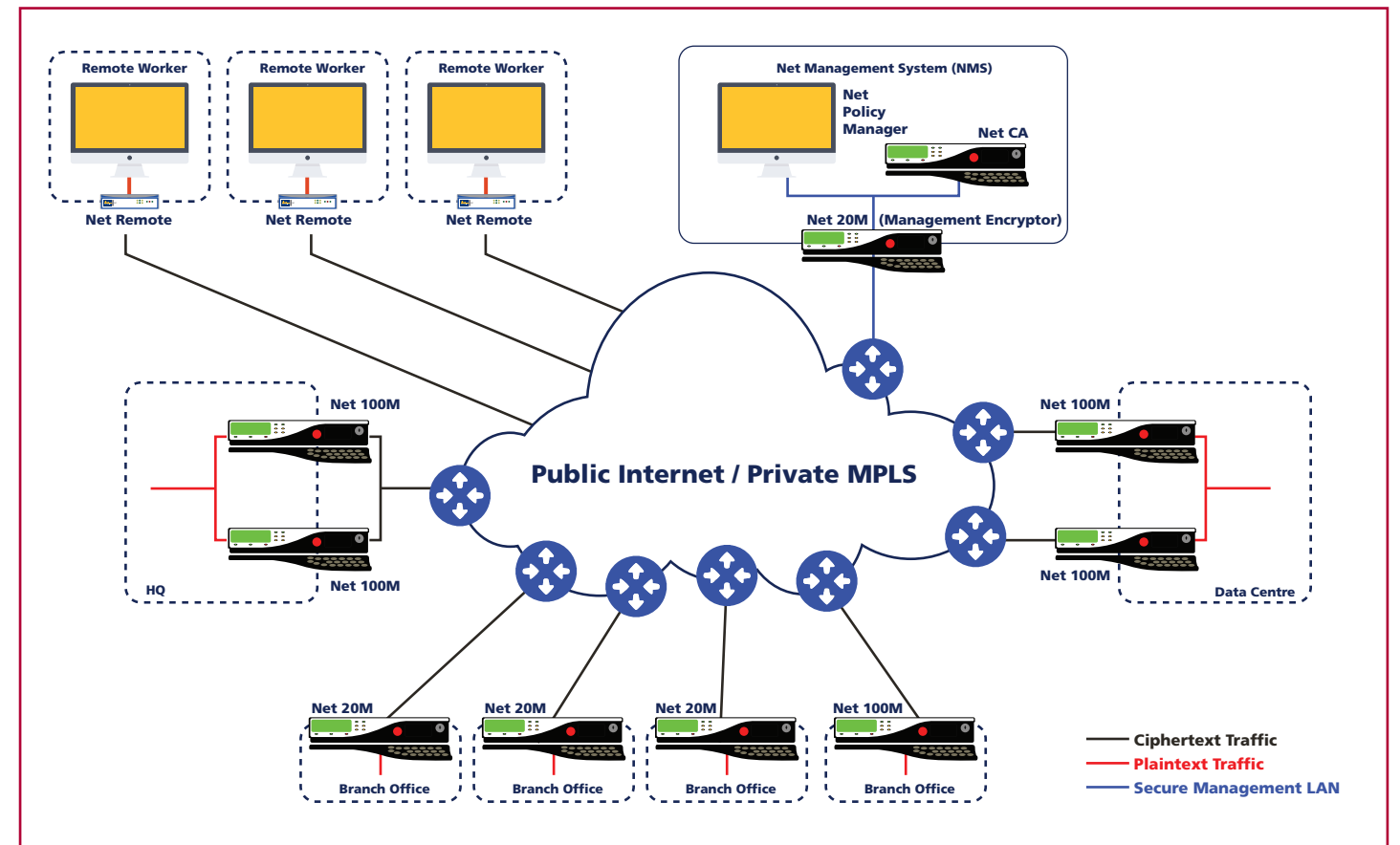
At the heart of the managed estate lies the Ultra Encrypt Net Management System (NMS), which includes a project-specific X.509 PKI standards based Net CA, under the control of an authorised administrator. Net CA provides remote certification of the encryptor's public signing keys and CRLs (certificate revocation list) as well as full on demand remote over the air re-keying (OTAR) in real time. VPN topologies are centrally defined using the sophisticated Net Policy Manager GUI, with configuration information being automatically pushed out to all the encryptors (and to a backup NMS where applicable). Policy Manager also provides a full range of centralised device management, monitoring, auditing and accounting functions. Put simply, centralised key and policy management leads to better managed service uptime, increasing both usability and security.

TECHNICAL SPECIFICATIONS

		NET 20M	NET 100M
Performance	Sustained encrypted traffic throughput †	18 Mbps	160 Mbps
	Simultaneous security associations	2000	2000
Physical Interfaces	WAN	10 Mbps Ethernet	10/100 Mbps Ethernet
	LAN	10/100 Mbps Ethernet	
	Serial Port	V.24	
Environmental	Temperature	Operating: 5 to 40°C / Storage: -15 to 65°C	
	Humidity	25 - 90% (non-condensing)	
Physical Dimensions	Height	51 mm	
	Weight	223 mm	
	Depth	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

TYPICAL NET ARCHITECTURE



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, just 4packet 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 Ultra Electronics AEP, the only company with centrally managed IP encryptors and a fully integrated PKI approve

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)

Each is available in the following versions:

- EB: UK OFFICIAL & Commercial
- ED: CAPS Enhanced Grade
- EE: EU CONFIDENTIAL

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



making a difference

Ultra Electronics
 AEP
 419 Bridport Rd,
 Greenford,
 Middlesex UB6 8UA
 Main Switchboard: +44 (0)1628 642 600
 Email: info@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 2016.
 Printed in England