The first secure IP network encryptor to give you foreign interoperable capabilities is now enabling you to remotely rekey any HAIPE® device. The AltaSec KG-250 encryptor from ViaSat offers Type 1 high-speed IP network encryption with seamless foreign interoperability and centralized operation and management. This Inline Network Encryptor (INE) is certified by the National Security Agency/Central Security Services for use on classified U.S. Government communications networks, and is available to U.S. Department of Defense customers, and authorized international and Homeland Security organizations.

With HAIEP to HAIEP Keying (H2HK) warfighters no longer need to travel forward and physically deliver keys to each network node. A single KG-250 can remotely rekey a subnetwork of HAIEP devices and can function behind commercial firewalls, enabling centralized management from a physically secure location. Combined with airborne enhancements such as remote heartbeat and remote zeroize, the KG-250 can be deployed effectively in UAVs and other remote locations.

The KG-250 is not only foreign interoperable, but also coalition releasable. Featuring Suite A and/or Suite B (AES-EFF) cryptographic algorithms and both software source and key material source authentication, the KG-250 ensures that communications are controlled and restricted to members of selected Communities of Interest (COIs) via Exclusion Keys. Featuring field tamper recovery and advanced technology to handle complex missions, this AltaSec device can be deployed to support the end-to-end security requirements of the Global Information Grid (GIG), providing the warfighter with secure information when and where it is needed.

Ensuring you’re always connected and your network is up-to-date, the KG-250 includes embedded Open Shortest Path First (OSPF) routing and is based on ViaSat’s PSIAM™ cryptosystem. With OSPF routing the INE is able to continuously adapt to rapidly changing networks, and the PSIAM cryptosystem’s programmable and scalable information assurance capabilities enable the KG-250 to evolve over time.

The KG-250 is designed for low cost of ownership and ease of portability. While a centralized manager isn’t required, the VINE™ Manager software application is provided at no extra cost. Web browser based with both administrator and monitor access levels, VINE Manager software allows users to remotely manage any AltaSec parameter from the Plain Text (PT) or the Cipher Text (CI) interface.

By incorporating the latest networking features, this equipment brings full-mesh network operation to the classified user in an intuitively managed, cost-effective package.
AltaSec® KG-250: Type 1 High Speed IP Network Encryptor

SPECIFICATIONS

NETWORKING FEATURES AND PROTOCOLS
- Protocols Supported: TCP, UDP, IPv4/IPv6 Dual Stack, ICMP, IGMP, ARP, DHCP
- Networking Features: Dynamic IP addressing, dynamic key management, red address confidentiality, dynamic discovery, virtual local area networks, embedded OSPF routing
- Management: SNMP & HTTPS browser-based management, VINE manager
- Multicast: IGMP on red and black subnet
- Quality of Service (QoS): Type of service octet bypass
- Fragmentation: Supports fragmentation and header options for red IP packets

RED DATA INTERFACE – ETHERNET
- Electrical/Mechanical: IEEE 802.3; 10/100 Mbps copper, RJ-45

BLACK DATA INTERFACE – ETHERNET
- Electrical/Mechanical: IEEE 802.3; 10/100 Mbps copper, RJ-45

COMSEC CHARACTERISTICS
- Algorithms: Type 1 Suite A and Type 1 Suite B cryptography
- Key Fill Interface: DS-101
- Dynamic Key Generation: FIREFLY (9,17, Enhanced)
- Flexibility: Modular, reprogrammable architecture, remote HAIPE to HAIPE keying
- Crypto Ignition Key: CIK Removal to UNCLASSIFIED CCI

PHYSICAL
- Dimensions (WHD): 7.5 x 1.68 x 11.9 in; 190.5 x 42.7 x 302.2 mm
- Weight: 6.5 lbs; 2.9kg
- Power: +5 VDC and +3.3 VDC; 13.7W typical

RELIABILITY AND MAINTENANCE
- Predicted MTBF: 312,000 hours
- Predicted MTTR: 15 mins
- Other: Extensive power up and online BIT

ENVIRONMENT
- Operating Temperature: 0°C to +50°C cold starting; tested to -23°C ambient
- Non-Operating Temperature: -20°C to +70°C
- Operating Altitude: Up to 50,000 ft
- Non-Operating Altitude: Up to 69,000 ft
- Non-Operating Rapid: 27,000 ft to 69,000 ft in 15 seconds

DECOMPRESSION
- Shock: MIL-STD-810F 516.5 Procedure I SRS curve: 9 to 45 g from 10 Hz to 45 Hz w 6dB slope, 45 g from 45 Hz to 2000 Hz
- Vibration:
  - MIL-STD-810F 514.5 Procedure I Cat 24: 0.04g²/Hz from 20 Hz to 2000 Hz for 15 minutes each on 3 main orthogonal axes;
  - MIL-STD-810F, 516.5, Procedure I, ground equipment with a peak acceleration of 40g
  - RTCA-DO-160E, Section 8, Category S, Curve B: 0.012g²/Hz for 10 to 40 Hz, 0.012g²/Hz to 0.002g²/Hz for 40 to 100 Hz, 0.002g²/Hz for 100 to 500 Hz, and 0.002g²/Hz to 0.00013g²/Hz for 500 to 2000 Hz for 1 hr. each on 3 main orthogonal axes
- EMI/EMC: FCC Class B and EN 55022 Class B
- Humidity (Non-Condensing): 95% @+60°C for 96 hours per MIL-STD-810F, Method 507.4

CERTIFICATION
- NSA Certified for TS/SCI and below
- JITC Certified
- TEMPEST Compliant NSTISSAM 1/92

ORDERING INFORMATION
- PART NUMBERS
  - NSN: 5810-01-524-6615CA
  - Part Number: SI-017750-0000
- Available for Order: Through ISSP, IDIQ, and ViaSat

CONTACT
6155 EL CAMINO REAL, CARLSBAD, CA 92009
SALES
TEL 760.476.4755 OR 888.VIASAT.1 (888.842.7281) FAX 760.683.6815 EMAIL INFOSEC@VIASAT.COM
TECHNICAL SUPPORT
TEL 760.476.4754 OR 888.VIASAT.4 FAX 760.929.3938 EMAIL ALTASEC@VIASAT.COM WEB WWW.VIASAT.COM/SECURE

Copyright © 2011 ViaSat, Inc. All rights reserved. ViaSat, the ViaSat logo, and AltaSec are registered trademarks of ViaSat, Inc. PSIAM and VINE are trademarks of ViaSat, Inc. HAIPE is a registered trademark of the National Security Agency. All other trademarks mentioned are the sole property of their respective companies. Specifications and product availability are subject to change without notice. The Type 1 encryption provided by this High Speed IP Encryptor is part of the Department of Defense “Defense in Depth” strategy. Type 1 encryption is only one portion of the overall defense in depth. A comprehensive network Information Assurance strategy involving “Defense in Depth” is required to ensure secure and reliable protection for sensitive and classified information. 110428-061