HARRIS®

assuredcommunications®

BID/2370

END CRYPTOGRAPHIC UNIT (ECU)

A Sierra™ II based network-centric, programmable encryption device

The BID/2370 ECU was developed as part of the UK MOD Common-good High-grade INFOSEC Module (Programmable) or CHIM(P) programme. It is based on a modular system architecture that features programmability, module reuse, full UK sovereignty, and scalability to accommodate a wide range of cryptographic equipment and/or applications.

The BID/2370 provides functionality for legacy high-speed link and Internet Protocol (IP) packet encryption (i.e., High Assurance IP Encryptor or HAIPE) applications. The Rack-Mount ECU can simultaneously store four IP and Link Crypto applications (HAIPIS V1.3.5, IP-UKEO, High-Speed Link, and BID/1650). Applications are selectable via menu entries from the web-based management interface. The Rack-Mount ECU is field software re-programmable and can be programmed (software and firmware components) to provide future algorithm support, including a software-only upgrade to HAIPE version 3.

Contained within the BID/2370 is the Sierra™ II Core Cryptographic Module (CCM). The CCM contains cryptographic algorithms and functions in conjunction with integrated Red, Black, and management processing capabilities to maximize portability. The CCM also contains embedded network and link interface functions to allow connectivity into Ethernet or serial-based applications with the addition of the appropriate interface circuits. The CCM was independently evaluated by Communications Electronic Security Group (CESG) for use in other embedded applications.

The BID/2370 ECU and CCM are CESG-certified to pass UK EYES ONLY COMSEC traffic up through TOP SECRET CODEWORD level. The Rack-Mount ECU also supports reverse tunneling. The BID/2370 has a product form factor of 1U (19-inch rack mount). The Rack-Mount ECU product has its own internal power supply to support various AC power sources and typically consumes 20 watts. A backup battery is included to retain the cryptographic key variables and algorithms.

Sierra II was developed by Harris to address all of the cryptographic requirements of the JTRS and National Security Agency (NSA) Crypto Modernization program, including the requirement for programmability. Sierra II's software programmability provides a low-cost migration path for future upgrades (HAIPE standards evolution) to embedded communications equipment without the logistics and cost burdens associated with updating legacy cryptographic hardware.

SECURED BY: HARRIS®

Specifications for BID/2370 End Cryptographic Unit (ECU)

Features

Data throughput rates up to 100 Mbps full duplex. Higher data rates achievable with updated programming.
1U, 19-inch Rack Mountable (19" x 12.7" x 1.72")
6 kg approximate weight
Red and Black traffic interface connectors
Operational temperature: +5° to +30°C
Field reprogrammable
LCD panel–122 x 32 pixel display
5-button keypad
Power-240 VAC@50 Hz, 110/115 VAC@60 Hz, 115 VAC@440 Hz
Power varies by application (nominally 20 W)
Dedicated management programming interface
Stores up to four separate applications
Web-based software for application selection (https)
Application switching within 30 seconds without software reprogramming
CESG certified for compliance with High Grade (Top Secret UK Eyes) requirements
Front panel accessible battery and fuse
Dedicated key and algorithm zeroization and switches
Anti-tamper mechanisms
TEMPEST

Interfaces

Red/Black traffic Ethernet interface (up to 1000 Mbps)
Red management and re-programming Ethernet interface (up to 100 Mbps)
Red/Black serial (up to 10 Mbps)
Red/Black high-speed serial (up to 45 Mbps)
Cryptographic Ignition Key (CIK)
EKMS-308 Key Fill–DS-101/DS-102

HAIPE

FIREFLY/Enhanced FIREFLY, Internet Key Exchange (IKE)
500 Pre-Placed Key (PPK) or IKE generated keys
500 security association pairs
32 security policies
HAIPE V1.3.5 compliant, (SPAWAR HIT-tested) V3.1 (with software upgrade)
10/100/1000 based-TX Ethernet
100 Mbps full duplex
Web-based management interface provided
Supports UK, CCEB, and NATO EFF Key Material (software upgrade to include additional items)

U.K. Eyes Only (UKEO) Application

HAIPE application with UKEO algorithm
Same features as HAIPE
Supports UK EFF material

High-Speed Serial (HSS)

Supports LEF key specification and Algorithm/Mode definitions. Software upgradeable to support full LEF capabilities.
LVDS Red & Black Synchronous Serial
2 PPK, software upgrade to include more
LCD and keypad interface
45 Mbps serial full duplex

BID/1650 Link Encryption

V.10/V.11
Asynchronous 9600 Baud–full duplex
Synchronous 96K Baud rate–full duplex
OPT A, OPT B, TDM, HF, Redundant, non-Redundant
2 PPK
Interoperable with legacy KG-84C

"HAIPE" and the "HAIPE" design are trademarks of the National Security Agency, an agency of the United States Government and with permission. These item(s)/technical data have been reviewed in accordance with the international traffic in arms regulations, 22 CFR 12 – 130, and the export administration regulations, 15 CFR 730 – 774, and determined by the export control department to be rated EAR99. General prohibitions apply.

HARRIS®
assuredcommunications®

RF Communications | 1680 University Avenue | Rochester, NY USA 14610
www.harris.com 585-244-5830

Specifications subject to change without notice. Copyright © 2009 Harris Corporation 04/09 DS-379