

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 12 Generic Security Devices.....	12-1
12.1 HAIPE.....	12-1
12.2 Link Encryptor Family (LEF).....	12-2
12.3 Secure Voice	12-3

SECTION 12

GENERIC SECURITY DEVICES

12.1 HAIPE

ENC-000010 [Required: HAIPE] High Assurance Internet Protocol (IP) Encryptor (HAIPE) Electronic Control Units (ECUs) shall have the capability to be loaded and configured with legacy algorithms and modes to provide legacy-interoperable encryption services with 90 percent reliability.

ENC-000020 [Required: HAIPE] HAIPE ECUs shall have an inherent Information Assurance capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 90 percent reliability.

ENC-000030 [Required: HAIPE] HAIPE ECUs shall be capable of loading and accepting keying material (KEYMAT) from National Security Agency (NSA)-approved key fill devices with 90 percent reliability.

ENC-000040 [Required: HAIPE] HAIPE ECUs shall include a DS-101 cryptographic fill port interface in accordance with (IAW) Electronic Key Management System (EKMS) 308 with 90 percent reliability.

ENC-000050 [Required: HAIPE] The ECUs shall recover last known, good operational state/settings after loss of primary power with 90 percent reliability.

ENC-000060 [Optional: HAIPE] The ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90 percent reliability.

ENC-000070 [Required: HAIPE] The HAIPE(s) shall not preclude operation over low bandwidth networks as low as 2.4 kbps with 90 percent reliability.

ENC-000080 [Optional: HAIPE] The HAIPEs should have the capability to execute the In-Line Network Encryptor (INE) Management command and control function with 90 percent reliability.

ENC-000090 [Optional: HAIPE] The HAIPEs should have the capability to execute the Backup Remote Management (RM) command and control function with 90 percent reliability.

ENC-000100 [Required: HAIPE] The ECUs shall prevent the accidental deletion of all loaded operational key with 90 percent reliability.

ENC-000110 [Required: HAIPE] As a minimum, new software releases shall be backward compatible with the previous NSA-certified version of software with 90 percent reliability.

ENC-000120 [Required: HAIPE] The HAIPE(s) shall be able to recover security associations after loss of power on one end or both ends of the link with 90 percent reliability.

ENC-000130 [Required: HAIPE] The HAIPE(s) shall adhere to standard commercial interfaces (e.g., Ethernet, Fast Ethernet, Gigabit Ethernet, or 10Gigabit Ethernet).

ENC-000140 [Required: HAIPE] The HAIPE(s) devices shall be compatible with network components such as routers and hosts in common usage within the Global Information Grid (GIG) Information Assurance architecture with 90 percent reliability.

ENC-000150 [Required: HAIPE] The HAIPE(s) shall be capable of being reprogrammed with updated cryptographic software and algorithms with 90 percent reliability.

ENC-000160 [Required: HAIPE] The HAIPE(s) shall operate over connections to satellite links that experience delays of up to 2 seconds aggregate with 90 percent reliability.

ENC-000170 [Required: HAIPE] When subjected to 70 percent or greater of rated throughput, the HAIPE(s) shall maintain secure communications without interruption (i.e., without reboot) with 90 percent reliability.

ENC-000180 [Required: HAIPE] The INE shall achieve 85 percent of its OEM's advertised throughput.

ENC-000190 [Required: HAIPE] The average, minimum, and maximum latency shall be calculated for each frame size at the highest frame rate that yields 0 percent packet loss. Latency Tests are conducted to measure the response time of packets through a pair of Units Under Test (UUTs). The latency numbers are pulled from the throughput results. The average, minimum, and maximum latency is calculated for each frame size at the highest frame rate that yields 0 percent packet loss.

ENC-000200 [Required: HAIPE] The INE shall properly tunnel multicast data from a single host on one RED enclave to multiple hosts on a remote RED enclave 99 percent of the time.

ENC-000210 [Required: HAIPE] The INE shall demonstrate the Quality of Service (QoS), if the device can properly bypass Type of Service (TOS) bits 99 percent of the time, in accordance with multiple modes of bypass that the vendor has incorporated.

12.2 LINK ENCRYPTOR FAMILY (LEF)

ENC-000220 [Required: LEF] The LEF ECUs shall have the capability to be loaded and configured with legacy algorithms and modes to provide legacy-interoperable encryption services with 90 percent reliability.

ENC-000230 [Required: LEF] The LEF ECUs shall have an inherent Information Assurance capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 90 percent reliability.

ENC-000240 [Required: LEF] The LEF ECUs shall be capable of loading and accepting keying material (KEYMAT) from NSA-approved key fill devices with 90 percent reliability.

ENC-000250 [Required: LEF] The LEF ECUs shall include a DS-101 cryptographic fill port interface IAW EKMS 308 with 90 percent reliability.

ENC-000260 [Required: LEF] The LEF ECUs shall implement data interfaces that conform to the EIA-530 standard.

ENC-000270 [Required: LEF] The LEF ECUs shall implement data interfaces that conform to the RS-232 standard.

ENC-000280 [Required: LEF] The LEF ECUs shall be able to recover last known, good operational state/settings after loss of primary power with 90 percent reliability.

ENC-000290 [Optional: LEF] The ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90 percent reliability

ENC-000300 [Required: LEF] The LEF ECUs shall be capable of operating with legacy Time Division Multiple Access (TDMA) architectures for networked data exchange with 90 percent reliability.

ENC-000310 [Required: LEF] The LEF ECUs shall be able to automatically recover security connections after loss of power on one end or both ends of a channel with 90 percent reliability.

ENC-000320 [Required: LEF] The ECUs shall prevent the accidental deletion of all loaded operational keys with 90 percent reliability.

ENC-000330 [Required: LEF] As a minimum, new software releases shall be backward compatible with the previous NSA-certified version of software with 90 percent reliability.

ENC-000340 [Required: LEF] The LEF ECUs shall provide autophase if interoperable with KG-84C with 90 percent reliability.

ENC-000350 [Required: LEF] The LEF ECUs shall have Over-the-Air-Rekey (OTAR) capability with 90 percent reliability.

12.3 SECURE VOICE

ENC-000360 [Required: SCIP Enabled DSCD] The enabled Department of Defense Secure Communications Device (DSCD) shall be only those that are Type Approved by NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA-approved secure protocol. If the DSCD supports more than one secure protocol, then it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD.

ENC-000370 [Required: SCIP Enabled DSCD] The DSCD devices that use a two-wire analog or Basic Rate Interface (BRI) shall meet the End Instrument (EI) requirements as specified in Section 3.7, Customer Premises Equipment. The DSCD devices that use an IP interface shall

meet the EI requirements as specified in Section 2, Session Control Products. DSCD devices that support Defense Switched Network (DSN) trunk interfaces [Primary Rate Interface (PRI) or IP (Unified Capabilities [UC] Session Initiation Protocol [SIP] [UC SIP])] shall meet the interface requirements defined in the following:

- a. Section 2.14.10, MG Support for Integrated Services Digital Network (ISDN) PRI Trunks, of Unified Capabilities Requirements (UCR) 2013.
- b. UC SIP 2013.

ENC-000380 [Required: SCIP Enabled DSCD] A DSCD device that supports one of the required signaling modes shall interoperate with and establish secure sessions with other compatible devices with at least an 85 percent secure call completion rate.

ENC-000390 [Required: SCIP Enabled DSCD] The DSCD shall be capable of using the protocol(s) provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call.

ENC-000400 [Required: SCIP Enabled DSCD] The DSCD shall operate in a network that has an E2E latency of up to 600 milliseconds.

ENC-000410 [Required: SCIP Enabled DSCD] The DSCD shall achieve and maintain a secure voice connection with a minimum Mean Opinion Score (MOS) of 3.0.

ENC-000420 [Required: SCIP Enabled DSCD] Once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate.

ENC-000430 [Conditional: SCIP Enabled DSCD] If the DSCDs establish secure sessions on a Continuously Variable Slope Delta (CVSD) switch and terminate on a CVSD switch, without ever traversing or otherwise interacting with the DSN, Defense RED Switch Network (DRSN), or Public Switched Telephone Network (PSTN), then it must do so with a 50 percent completion rate.

ENC-000440 [Conditional: SCIP enabled DSCD] If the DSCDs establish secure sessions on IP networks using Secure Communications Interoperability Protocol (SCIP), then it shall satisfy all the end point requirements described SCIP-215 and SCIP-216.

ENC-000450 [Required: SCIP Enabled DSCD] The DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.