TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

SECTION 12
GENERIC SECURITY DEVICES

12.1 INTRODUCTION

Interoperability and supportability needs are addressed in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). CJCSI 6212.01E establishes policies and procedures for developing, coordinating, reviewing, and approving interoperability and supportability needs, as well as certifying that those needs have been met. This section of the Unified Capabilities (UC) Framework provides a product overview of End Cryptographic Units (ECUs) encryption products (e.g., High Assurance Internet Protocol Encryptor [HAIPE], Secure Communications Interoperability Protocol [SCIP] Device, and Link Encryptor Family [LEF]) and a framework of the interoperability testing of these products.

12.2 SECURITY PRODUCTS OVERVIEW

12.2.1 HAIPE

ECUs are components of information systems that provide security services, which may include confidentiality, identification and authentication, integrity, and non-repudiation, to the overall system. Typically, the ECU is integrated with other components to provide the overall security required for the system. As such, neither the ECU nor the encryption function provided is a standalone system. Figure 12.2-1, Sample Network, illustrates the use of the ECU in a system.

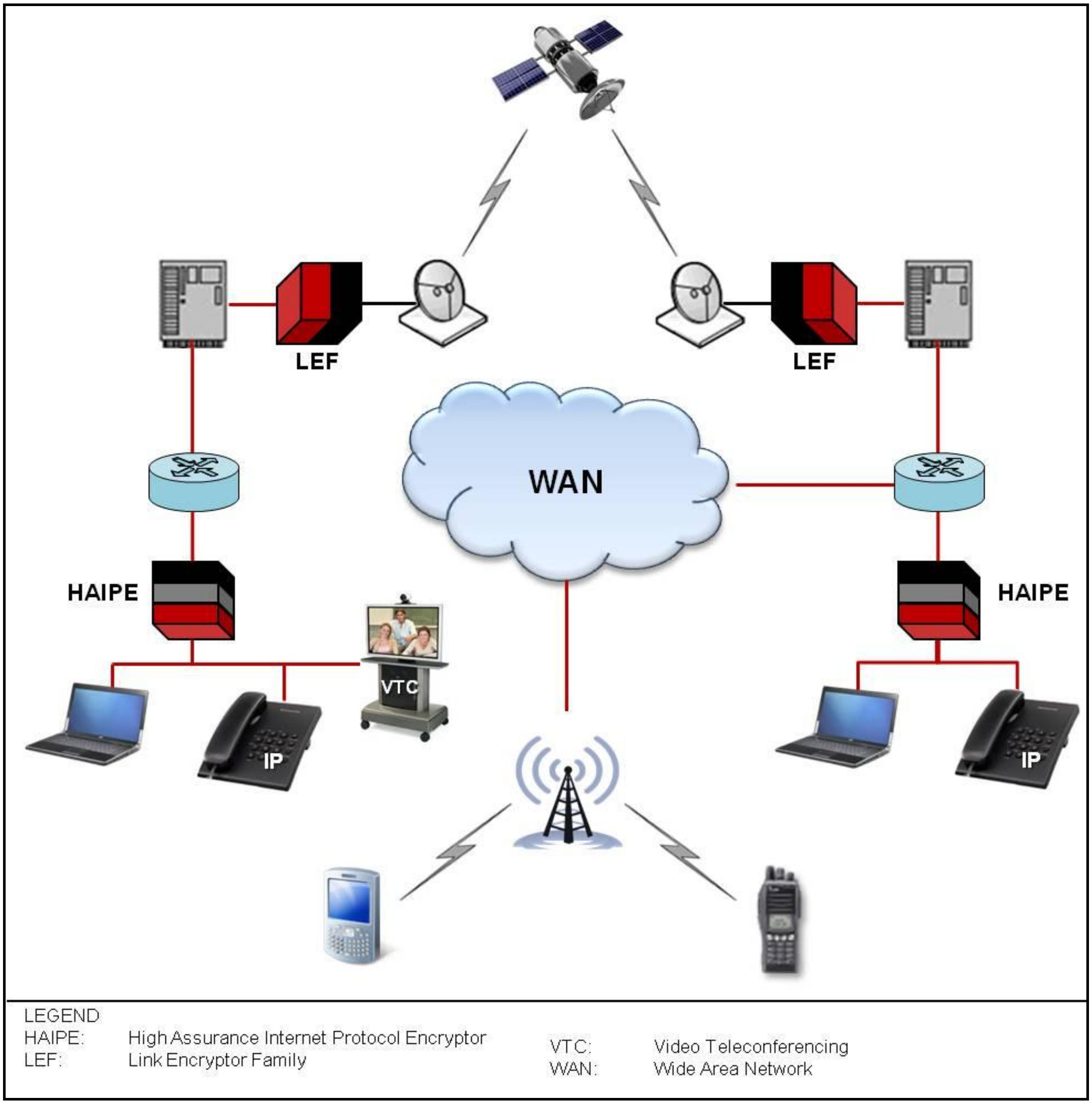

Figure 12.2-1. Sample Network

A HAIPE is a programmable Internet Protocol (IP) Information Security (INFOSEC) device with traffic protection, networking, and management features that provide Information Assurance services for IPv4 and IPv6 networks. The HAIPE(s) that are version 3.x or higher compliant meet the DoD mandate for IPv6 compatibility and the goals of the Cryptographic Modernization Initiative (CMI), and are a key component of the Global Information Grid (GIG) Vision. The HAIPE device is designed to provide confidentiality, integrity, and authentication services for IP traffic for Deployable and Fixed network applications. The HAIPE enables secure transmission across wide area networks (WANs) via IP packet encryption to compatible destination network security devices where decryption takes place. Figure 12.2-2, Example HAIPE Application Diagram, provides an example of HAIPE implementation within a WAN.

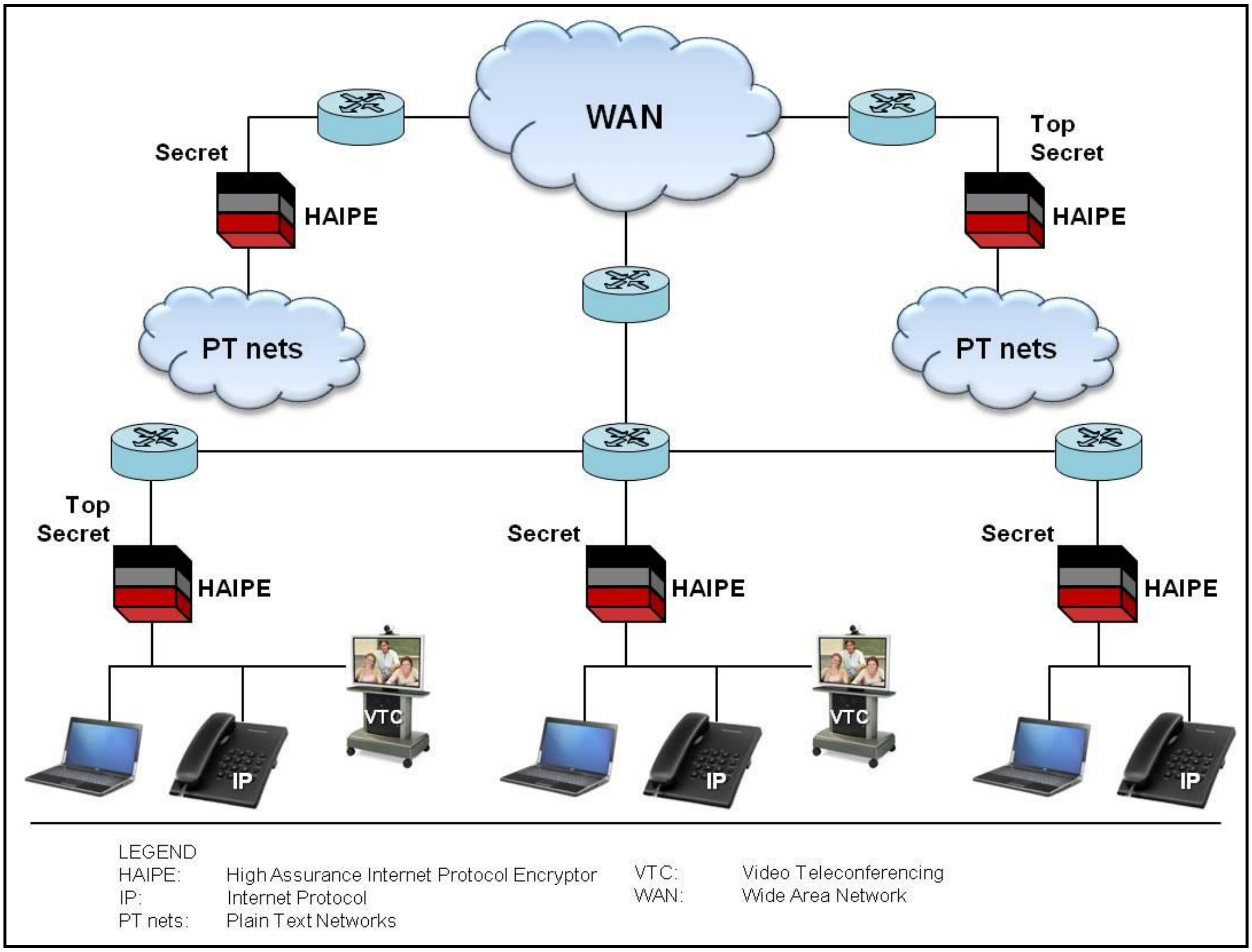

Figure 12.2-2. Example HAIPE Application Diagram

Design requirements are captured and promulgated in the HAIPE Interoperability Specification (IS). The HAIPE IS provides interoperability requirements for the following interconnections:

- HAIPE Device to HAIPE Device.
- HAIPE Device to Key Management Infrastructure (KMI).
- HAIPE Device to Security Management Infrastructure (SMI).
- HAIPE Device to Network Component Infrastructure (NCI).

A HAIPE compliancy, (that is, “HAIPE Interoperability Certification”) is granted by the National Security Agency (NSA) for a communications security (COMSEC) device that complies with HAIPE IS. Whereas Joint Interoperability Test Command (JITC) interoperability Certification deals with interoperability as defined by CJCSI 6212.01E, JITC certification will not be granted until the device is certified by the NSA. The HAIPE compliance is met by meeting the requirements in the Networking Core and Traffic Protection Core Specifications, plus the three Classified cryptography specifications (Suite A, Suite B, and Legacy), and any Extension Specifications. In HAIPE IS 3.1.x, the Networking Core and Traffic Protection Core Specifications have been combined into a single Core specification.

12.2.1.1 HAIPE IS V1.3.5 Devices

The devices listed below should be tested using Legacy (HAIPE IS v1.3.5) algorithms/transforms for both PPK (Baton-48) and Firefly (Medley-8):

- General Dynamics TACLANE KG-175 Classic. The KG-175 Classic is limited to 10-Half Duplex Speeds.
- General Dynamics TACLANE KG-175 E100. The KG-175 E100 is capable of 10/100-Full Duplex Speeds.
- General Dynamics TACLANE KG-175A (GigE). The KG-175A is capable of 10/100/1000-Full Duplex Speeds.
- General Dynamics TACLANE KG-175B (Mini). The KG-175B is capable of 10/100-Full Duplex Speeds.
- General Dynamics Sectera KG-235. The KG-235 is capable of 10-Half Duplex Speeds.
- Altasec KG-255. The KG-255 is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KOV-26 (Talon). The KOV-26 (Talon) is capable of approximately 10-Full Duplex Speeds.
- Harris KIV-54 (SecNet 54). The KIV-54 is capable of 10/100-Full Duplex Speeds.
- Safenet KIV-7MIP. The KIV-7MIP is capable of 10/100-Full Duplex Speeds.

12.2.1.2 HAIPE IS 1.3.X Devices

Devices listed below should be tested using Modern (HAIPE IS 3.x) algorithms/transforms for both PPK and Firefly (Medley-4).

- General Dynamics TACLANE KG-175D (Micro). The KG-175D is capable of 10/100-Full Duplex Speeds
- L-3 Communications KG-245A. The KG-245A is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KG-240A. The KG-240A is capable of 10/100-Full Duplex Speeds.
- L-3 Communications KG-245X. The KG-245X is capable of 10 Gigabit-Full Duplex Speeds.
- Altasec KG-250. The KG-250 is capable of 10/100-Full Duplex Speeds
- Altasec KG-250X. The KG-250X is capable of 10/100-Full Duplex Speeds.

12.2.1.3 Suite B Devices

Suite B devices include the HAIPE 3.x devices interoperating in Suite B mode, as well as standalone Suite B only devices known as Controlled High Value Products (CHVP). All of the following devices are Suite B devices and should be tested using Suite B algorithms/transforms for both PPK and Firefly (AES-4).

- General Dynamics TACLANE KG-175D (Micro). The KG-175D is capable of 10/100-Full Duplex Speeds.
- L-3 Communications KG-245A. The KG-245A is capable of 10/100/1000-Full Duplex Speeds.
- L-3 Communications KG-240A. The KG-240A is capable of 10/100-Full Duplex Speeds.
- Altasec KG-250. The KG-250 is capable of 10/100-Full Duplex Speeds.
- Altasec KG-250X. The KG-250X is capable of 10/100-Full Duplex Speeds.
- Altasec IPS-250. This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.
- General Dynamics C-100. This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.

12.2.2 Link Encryptor Family

LEF ECUs provide data security for the U.S. Military, U.S. Government, Allied forces, and coalition security environments. Current LEF devices include link and bulk encryptors. The LEF's primary mission is to protect Classified and sensitive digital data in a multitude of network environments: point-to-point, netted, broadcast, or high-speed trunk. The LEF ECU provides the means for encryption and decryption using Suite A and Suite B data security while providing advanced key management features that support the current key distribution system and the KMI initiatives.

The LEF ECUs are backward compatible with their legacy family members of equipment (HAIPE IS v1.35) to the degree necessary to support continuous operations. Although LEF requirements will vary based on implementation, JITC interoperability testing is still required. Additional testing may be required based on individual Services requirements.

The LEF Specification establishes the detailed cryptographic requirements and basic functional, performance, and security requirements of the Cryptographic Modernization (CM) version of the LEF link/bulk ECUs. This section incorporates the appropriate LEF Specification requirements to provide a sufficiently detailed baseline set of requirements while allowing vendors design flexibility as to the form, fit, and additional functionality of the resulting ECUs. Figure 12.2-3, Example LEF Application Diagram, illustrates the use of the LEF in a system.

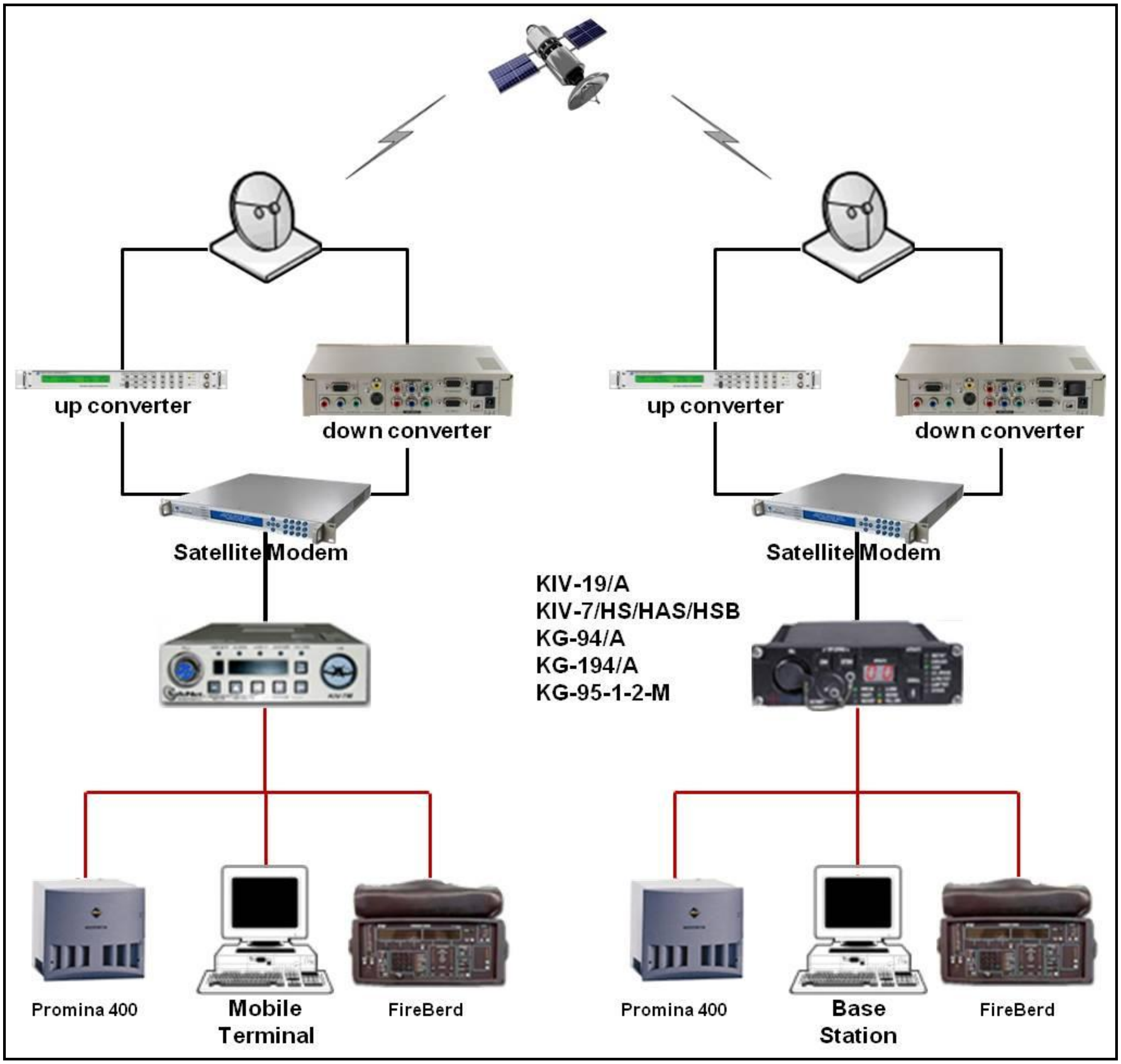

Figure 12.2-3. LEF Application Example

12.2.3 Secure Communications Interoperability Protocol (SCIP)

SCIP is a multinational standard for secure voice and data communication. SCIP derived from the U.S. Government Future Narrowband Digital Terminal (FNBDT) project after the United States offered to share details of FNBDT with a number of other nations in 2003. SCIP provides voice and data security for the U.S. Military, U.S. Government, Allied forces, and coalition security environments. SCIP supports a number of different modes, including national and multinational modes, which employ different cryptography. Many nations and industries are actively developing SCIP devices to support the multinational and national modes of SCIP.

SCIP has to operate over the wide variety of communications systems, including commercial landline telephone, military radios, communication satellites, Voice over IP (VoIP), and the different cellular telephone standards. It was designed to make no assumptions about the underlying channel other than a minimum bandwidth of 2400 Hz. It is similar to a dial-up modem in that, once a connection is made, two SCIP phones first negotiate the parameters they need and then communicate in the best way possible. Figures 12.2-4 and 12.2-5 illustrate SCIP network examples.

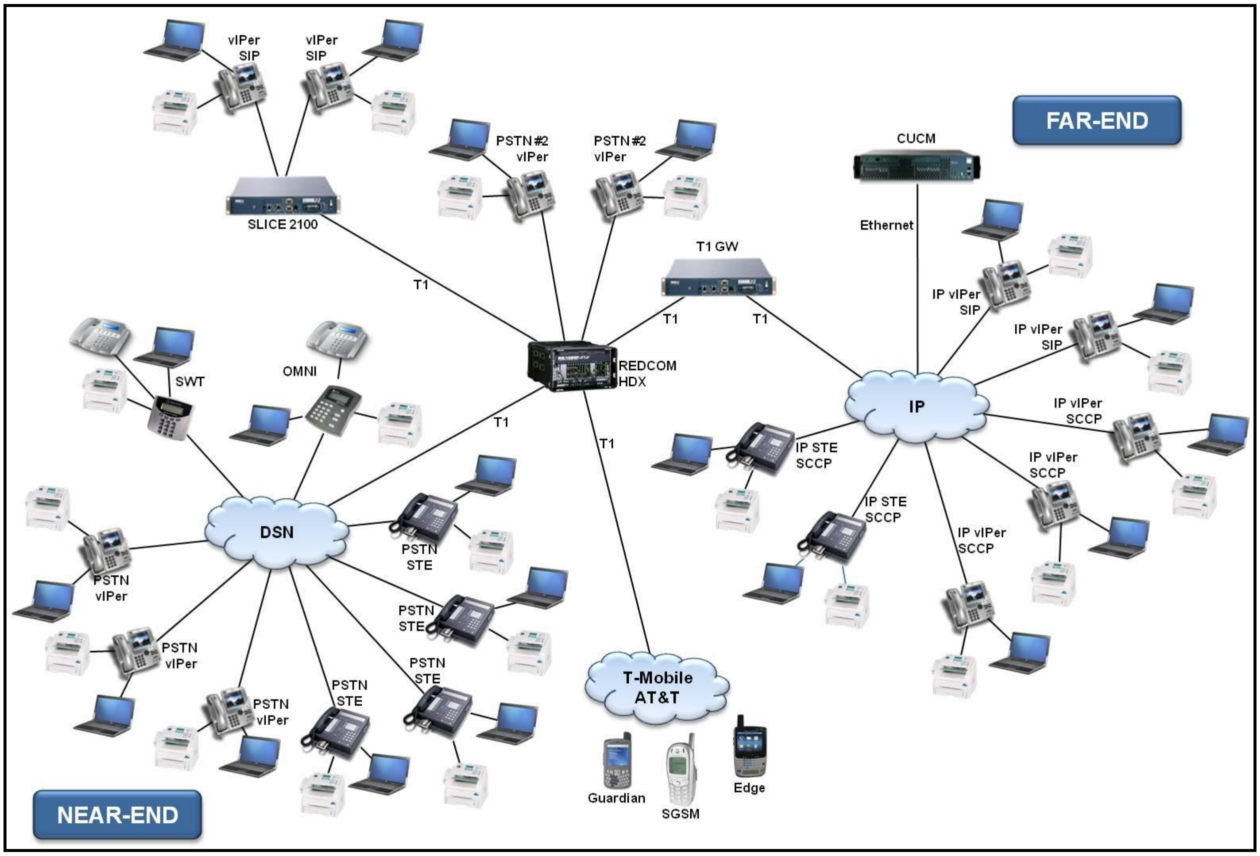

Figure 12.2-4. SCIP Network Example 1

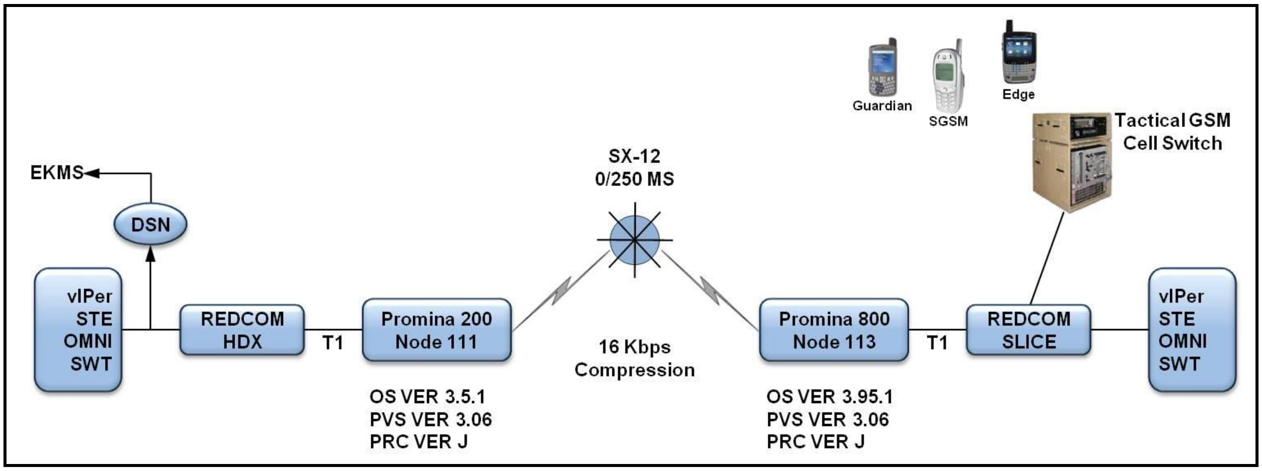

Figure 12.2.5. SCIP Network Example 2

12.3 DEVICE EVALUATION

This section provides information on HAIPE, LEF, and SCIP devices' performance and interoperability evaluation.

12.3.1 HAIPE

12.3.1.1 Throughput Test

Throughput testing should be conducted with a packet loss acceptance of 0 percent as per Request for Comments (RFC) 2544. Tests should run on both copper and fiber interfaces (if available) using both IPv4 and IPv6 addresses. The following key areas are evaluated in these tests:

- Maximum throughput in bidirectional scenarios with varied frame sizes (64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, and 1400 bytes).
- Effects of changing Encapsulating Security Payload (ESP) settings (Tunnel vs. Transport).
- Effects of changing Crypto Block settings (4 bytes, 8 bytes, 48 bytes).
- Effects of changing IP version (IPv4 vs. IPv6).
- Effects of changing Fixed Packet Length (FPL) settings.
- Effects of changing physical medium (Ethernet vs. Fiber).

12.3.1.2 Reliability Test

Reliability should be measured throughout the technical performance tests. A failure is defined as the inability to reboot, initialize, pass traffic as specified, and/or report status.

12.3.1.3 Configuration Changes

Configuration changes in the unit under test (UUT) may require a reboot or a loss in communications. These evaluations are performed to determine which configuration settings require the device to be rebooted, or cause a temporary loss of communications.

Configuration-change downtime is rated as follows:

Poor 1:	All configuration changes require downtime.
Fair 2:	≥ 50 % configuration changes require downtime.
Good 3:	< 50 % configuration changes require down time.
Excellent 4:	No configuration changes causes downtime.

12.3.1.4 Field Tamper Recovery

Tamper recovery requirements are derived from CES-CDD, Section 14.6.4 “Support Equipment,” and KSA, Section 6 b(7), “Tamper Detection.”

12.3.1.5 Loss of Physical Medium

Tests should be done to determine device responses and device recovery time from power outages. Results can be classified as:

Poor 1:		Recovery time	≥	2 minutes.
Fair 2:	1 minute ≤	Recovery time	<	2 minutes.
Good 3:	30 seconds ≤	Recovery time	<	1 minute.
Excellent 4:		Recovery time	<	30 seconds.

12.3.1.6 Line Impairment

The Line Impairment test should be conducted to verify that the device recovers secure communications after or during the interruptions.

12.3.1.7 Latency Test

Latency testing should be conducted with a packet loss acceptance of 0 percent as per RFC 2544. Network tools such as ping tests and trace route measure latency by determining the time it takes a given network packet to travel from source to destination and back on both copper and fiber interfaces (if available) using both IPv4 and IPv6 addresses.

12.3.1.8 Denial of Service Test

The INE should be tested for its ability to protect itself against denial of service (DOS) attempts. This test should be done on both the RED and BLACK side interfaces.

12.3.1.9 Vulnerability Test

The INE should protect against intentional and non-intentional malicious activity within the network. Fuzzing, enumeration, and spoofing are among the suite of attacks that should be run against the device. The device should not react at all to the malicious activities.

12.3.1.10 Configuration and Management

Configuration Management tests should be conducted to satisfy CES-CDD KSA, Section 6b(2), “Multiple Algorithms, Modes, Keys”; KSA, Section 6 b(5), “Configuration Management”; AA, Section 6c(1), “Operational Information”; KSA, Section 6b(4), “Management and Control”; KSA, Section 6b(6), “Cryptographic Product Distribution”; and KSA, Section 6b(8), “Form, Fit, Operational Function Replacement.”

The Configuration Management is a software application that enables an administrator to locally or remotely configure or monitor an INE..

12.3.1.11 Secure Tunnel Setup and Security Policy Database Management

A Configuration Manager must be capable of configuring the Security Policy Database (SPD) entries in the two communicating INE UUTs. These evaluations should be conducted to determine ease or complexity for an administrator to set up the SPD.

12.3.1.12 Management of Remote Devices

Management of remote INE UUTs is essential to the Warfighter. The ability to manage these devices with ease is critical. Tests should be done to evaluate how easily a remote UUT can be configured, keyed, and monitored.

12.3.1.13 Cryptographic Key Loading

Cryptographic Key Loading evaluations should be performed with all available key loading devices. These include the Data Transfer Device (DTD) (AN-CYZ 10), Simple Key Loader (SKL), and Secure DTD2000 System (SDS).

12.3.1.14 Firefly Vector

Tests should be conducted to determine the complexity of loading Firefly Vector (FFV) sets into the UUT, using all available key loading devices.

12.3.1.15 Enhanced Firefly Vector Set

Tests should be conducted to determine the complexity of loading the Enhanced FFV (EFFV) into the UUT, using all available key loading devices.

12.3.1.16 Pre-Placed Key

Tests should be done to determine the complexity of loading the pre-placed key (PPK) into the UUT, using all available key loading devices.

12.3.1.17 Algorithms Supported

Tests should be conducted to determine which specific algorithms are supported by the UUT (Suite A, Suite B).

12.3.1.18 Usability

Usability evaluation should be conducted in accordance with the Functional requirements for the UUT covered in the CES-CDD KPP Section 6 a(2) "Programmability."

12.3.1.19 Device Software Upgradeability

The following key areas should be evaluated for software upgradeability:

1. Software (SW) Version display.
2. Ease for an administrator to install a software update.
3. Determination that, during or after SW update, UUT network connections are maintained.
4. Remote SW update.
5. SW update roll-back.
6. Remote SW update done via RED network.
7. Upgrade of SW while the device is actively in service.
8. UUT accomplished with restart or other downtime.

12.3.2 Interoperability

There are three different types of devices:

- HAIPE IS v1.3.5 devices.
- HAIPE IS 3.x devices.
- Suite B (a subset of HAIPE IS 3.x devices using Suite B encryption).

12.3.2.1 Reachability

The HAIPE IS 3.0.2 introduces two functionalities:

1. Peer HAIPE Reachability Detection (PHRD).
2. Peer Destination Unreachable Notification (PDUN).

PHRD performs a keep-alive function between two HAIPEs to determine if a Security Association (SA) endpoint is reachable. PDUN is a notification message sent by a HAIPE, if the destination address of the de-capsulated packet is no longer available on that HAIPE's local PT network.

PDUN should be tested to ensure that, when a destination network is removed, the source network's Peer Enclave Prefix Table updates accordingly. The PHRD option is tested to ensure that, when one UUT is removed from the network, the accompanying SA from the source network shows that the removed network is now "Unreachable."

12.4 LEF TEST & EVALUATION

12.4.1 Initialization/Functional

These tests confirm power-up, self test, operating, and general use from one day to the next without reset; loading of cryptographic keys; unit tests; and loading of personalities. The LEF device must perform by operating at a minimum of 24 consecutive hours without any errors. The LEF device should also be tested in various timed intervals after a stress test of operations. These intervals should be at least 10–15 executions of the feature under-test.

12.4.2 Personality/Cryptographic Algorithms

Tests should be conducted to verify that the LEF encryptor's initialization procedure matches its personality. The KIV-194 personality is verified to function as a KG-194/KIV-19A, and the KG-84 (KIV-7) personality is verified to function as a KG-84/KIV-7.

12.4.3 Interoperability

Interoperability tests should be performed to verify all known configurations in use.

12.4.4 Asynchronous Modes

Asynchronous data communication is used throughout many older Army systems. It is a vital part of the KG-84A/C operation. The UUT must operate in the Suite A and Suite B personalities, using the equivalent asynchronous options.

12.4.4.1 Synchronous Modes

The LEF has different synchronous modes available for use. Each mode is designed for use in different environments ranging from reduced synchronization overhead to high- and low-bit error rates.

The LEF encryptor UUT should be tested against all supported modes. In each mode, data rates from 50 bps to the maximum data rate supported by that algorithm are tested.

12.4.4.2 Link Encryption Interoperability and Interchangeability

UUT must be interoperable with modern link encryptors.

To test interoperability, the UUT should be tested with KIV-7M and KIV-19M to determine any deficiencies in modern encryptors so that users are made aware of the issue. Each mode and interface are tested from a minimum data rate of 50 bps to a maximum data rate of 50 Mps with 25 randomly picked frequencies.

12.4.5 Reliability

Reliability tests/assessment should be conducted to document defects and to determine Mean Time between Failures (MTBF).

A software defect which causes a lockup that can be cleared with a reboot is noted as a Severity 3. If the incident can be reproduced and/or happens more than three times during test conduct, it is noted as a Severity 2 defect. If the software failure cannot be cleared with a reboot or power cycle and requires the reloading of the software image, or COMSEC keying material, it is considered a catastrophic defect (Severity 1; refer to Section 5). All software failures (e.g., lockups and hangs) are noted in the evaluation report. Repeated sequential software defects are considered a failure. Any operational problems (except an intentional zeroize) that causes reproducible lockup of the unit is considered a major software failure (i.e., Severity 1 defect).

12.4.6 Reboot Test

The UUT is tested to ensure that, if power is removed and replaced, an operational circuit will retain key and previous strap settings so as to resume operational status without the unit going into alarm. This test is performed at least 500 times with an expected failure rate of less than 1 percent.

12.4.6.1 Key Loading

The UUT should be tested for its ability to accept keys through the fill port. Keys are loaded using DS-101, DS-102, and RS-232 protocols. The UUT must operate with the AN/CYZ-10 (DTD) or simple key loader (SKL). Proper operation consists of the Key Management Interface being able to recognize the proper and improper key for the respective personalities. The UUT would be categorized as a failure if the UUT does not recognize improper key or goes into a hard fault error state.

12.4.6.2 Over-the-Air-Distribution or Over-the-Air-Re-Key

The UUT must properly perform the Over-the-Air Distribution (OTAD) and Over-the-Air-Re-Key (OTAR) operations with the supported algorithms. Operations will consist of being the receiving and transmitting side of the link. An OTAR/OTAD operation is considered a FAILURE if the key is improperly transferred or cannot be performed. A limited PASS will be given if a workaround (i.e., disabling "UpdateU") has to be performed for the operation to be successful.

12.4.6.3 Change Key/Local Update Operations

The UUT must properly perform the change key operation using both PPK and EFF. Change key operations will be performed during testing at a minimum of 10 times initiated from each side and be performed in 1/2/3 consecutive sequences at random. The operation will consist of performing a change key and then awaiting for the link to be reestablished. No other user operation should be performed if the link has resynchronized enabled.

The UUT must properly perform a local update when using PPK. Change key operation is conducted to set the count at a random number. If the link does not re-establish, the UUT should be categorized as FAIL.

12.4.7 Network Management

The UUT must be manageable via Ethernet port by a remote system. The UUT should be tested using human manual interaction and computer automated HyperText Transfer Protocol, Secure (HTTPS) requests/posts to verify the robustness and viability of the UUT. The UUT should not enter an alarm state. Table 12.4-1 lists the test criteria.

Table 12.4-1. Network Management Test Criteria

RANK	GRADE	CRITERIA
Failure	0	No Ethernet port
Poor	1	Poor configuration of HCI
Fair	2	Clear configuration of HCI, able to process all requests
Good	3	Clear configuration of HCI, able to manage multiple units
Excellent	4	Robust user interface, manage multiple units, capable to save and reload different configurations

12.4.8 Software Download

Assessments should be done to determine the level of effort required to load and upgrade software for the device. This should include validating the instructions in the documentation provided by the OEM. Evaluating the UUT for mass updating capabilities and isngle-button operation updates should be considered. Table 12.4-2 lists some criteria for assessment.

Table 12.4-2. Software Download Test Criteria

RANK	GRADE	CRITERIA
Failure	0	No Management port
Poor	1	No Instruction
Fair	2	Minimal instruction, requires highly skilled user
Good	3	Step-by-step instruction provided
Excellent	4	Step-by-step instruction with images for clarification

12.4.9 Degraded Network Capability and Robustness

LEF devices should be tested for its capabilities to function in a degraded network environment. LEF devices should be able to accept a wide variety of network timing and variable speeds. Standard LEF test speeds range from 50 bps to 50 Mbps. Table 12.4-3 lists the test criteria.

Table 12.4-3. Degrated Network Capability and Robustness Criteria

RANK	GRADE	CRITERIA
Failure	0	Device works only in ideal condition – No delay or error
Poor	1	Device works with minimal delay and error (10^-7)
Fair	2	Device passes test with intermediate delay and error (<10^5)
Good	3	Device passes test with intermediate delay and error (<10<3)
Excellent	4	Device passes test with extreme delay and error (>=10^3)

12.4.10 Required Ancillaries Devices

Interface connections should be verified for each device. There are more than 24 variants of rack-mounted adapters for different KIV-7, KIV-19, KG-84, KG-94, and KG-194 applications. Each of these rack mounts have different connectors and use different pin-outs.

12.4.11 Control Signal Requirements

Control signal options should be tested to ensure that they operate as used in the field and specified in the manual.

Table 12.4-4 lists the types of signals supported for each device. The UUT should be tested for its supported control signals. Any signals not supported should be considered as deficiencies.

Table 12.4-4. Control Signal Requirements Matrix

	KIV-7M	KIV-7M	KIV-7M	KIV-7M	KIV-19M	KIV-19M	KIV-19M	KIV-19M	KIV-7	KIV-7HSA	KIV-7HSB	KIV-7HS	KG-84A	KG-84C	KIV-19	KIV-19A	KG-194	KG-194A	KG-94	KG-94A
ALGORITHM	**A**	**B**	**W**	**S**	**A**	**B**	**W**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**W**	**W**	**W**	**W**	**W**	**W**
RED Request to Send	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X						
RED terminal Ready	M	M	X/L	X/L	M	M	X/L	X/L												
RED Clear to Send	M	M	X/L	X/L	M	M	X/L	X/L												
RED DCE Ready	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Clear to Send	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X						
BLACK Ready to Receive	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK DTE Ready	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Ready to Send	M	M	X/L	X/L	M	M	X/L	X/L												
BLACK Terminal Ready	M	M	X/L	X/L	M	M	X/L	X/L												
Contact Closure Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Differential Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Single-Ended Positive Resyn.	M	M	X/L	X/L	M	M	X/L	X/L	X	X	X	X	X	X	X	X	X	X	X	X
Single-Ended Negative Resyn.	M	M	X/L	X/L	M	M	X/L	X/L						X	X	X	X	X	X	X
Single-Ended Balanced Resyn.	M	M	X/L	X/L	M	M	X/L	X/L						X	X	X	X	X	X	X

Legend:
L: Denotes the requirement for legacy transitioning testing.
M: Denotes the requirement for modern testing.
X: Denotes the requirement for legacy testing.

12.4.12 Interface Requirements

The LEF devices should be tested against various combinations of interface specifications: RS-232, EIA-530, and EIA-644. Table 12.4-5 lists which combination of interfaces will be required for test conduct.

Table 12.4-5. Interface Requirement Matrix

	KIV-7M	KIV-7M	KIV-7M	KIV-7M	KIV-19M	KIV-19M	KIV-19M	KIV-19M	KIV-7	KIV-7HSA	KIV-7HSB	KIV-7HS	KG-84A	KG-84C	KIV-19	KIV-19A	KG-194	KG-194A	KG-94	KG-94A
ALGORITHM	**A**	**B**	**W**	**S**	**A**	**B**	**W**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**W**	**W**	**W**	**W**	**W**	**W**
RED RS-232 BLACK RS-232									X	X	X	X	X	X						
RED RS-232 BLACK EIA-530									X	X	X	X	X	X						
RED RS-232 BLACK EIA-644																				
RED EIA-530 BLACK RS-232									X	X	X	X	X	X						
RED EIA-530 BLACK EIA-530					M	M			X	X	X	X	X	X	X	X	X	X	X	X
RED EIA-530 BLACK EIA-644																				
RED EIA-644 BLACK RS-232																				
RED EIA-644 BLACK EIA-530																				
RED EIA-644 BLACK EIA-644					M	M														
Legend: M: Denotes the requirement for modern testing. X: Denotes the requirement for legacy testing.																				

12.5 SCIP EVALUATION

12.5.1 General Description

The SCIP requirements are used to certify DoD Secure Communications Devices (DSCDs) when directly connected to or otherwise traversing the Defense Switched Network (DSN), the Public Switched Telephone Network (PSTN), or the Defense RED Switch Network (DRSN) Gateway to or from the DSN.

This section applies to the evaluation of secure mode operation of any DSCD that either directly connects to the DSN, the PSTN, or the DRSN Gateway or traverses these networks in the course of conducting a secure communications session, regardless of where the telephone call originates or terminates. The certification test environment for DSCDs shall include configurations that realistically simulate fixed networks (i.e., DSN, DRSN via the DSN Gateway, PSTN) and deployed networks, as illustrated in Figures 12.2-4 and 12.2-5.

12.5.1.1 Evaluation Methods

The secure voice equipment will be evaluated to include features and capabilities of a DSCD device to include voice, data, and facsimile transmission.

1. SCIP Protocol.

   The enabled 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, 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.

2. Interface.

   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 DSN trunk interfaces (Primary Rate Interface [PRI] or IP [UC Session Initiation Protocol (SIP)]) shall meet the interface requirements defined in AS-SIP 2013, Section 2.14.10, MG Support for ISDN PRI Trunks, for PRI, and Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, for the AS- SIP.

3. Call Completion Rate.

   A DSCD device that supports one of the required signaling modes should interoperate with and establish secure sessions with other compatible devices.

4. Multiple SCIP Modes.

   The DSCD should be capable of using the protocol(s) provided to establish a secure session and should maintain secure communications for the duration of the secure portion of the call.

5. Minimum Essential Requirements.

   If the DSCDs that establish secure sessions on IP networks use SCIP, then it shall satisfy all the end point requirements described in SCIP-215 and SCIP-216.