

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 12 Generic Security Devices.....	12-1
12.1 Introduction.....	12-1
12.2 Security Products Overview	12-1
12.2.1 HAIPE.....	12-1
12.2.2 Link Encryptor Family.....	12-4
12.2.3 Secure Communications Interoperability Protocol	12-5
12.3 Evaluation	12-7
12.3.1 HAIPE.....	12-7
12.3.1.1 Throughput Test.....	12-7
12.3.1.2 Reliability Test.....	12-7
12.3.1.3 Configuration Changes on the Fly	12-8
12.3.1.4 Field Tamper Recovery.....	12-8
12.3.1.5 Loss of Physical Medium.....	12-8
12.3.1.6 Line Impairment.....	12-9
12.3.1.7 Latency Test.....	12-9
12.3.1.8 Denial of Service Test.....	12-9
12.3.1.9 Vulnerability Test	12-9
12.3.1.10 Configuration and Management	12-9
12.3.1.11 Secure Tunnel Setup and Security Policy Database Management	12-10
12.3.1.12 Management of Remote Devices	12-10
12.3.1.13 Cryptographic Key Loading	12-10
12.3.1.14 Firefly Vector.....	12-10
12.3.1.15 Enhanced Firefly Vector Set.....	12-10
12.3.1.16 Pre-Placed Key.....	12-10
12.3.1.17 Algorithms Supported.....	12-10
12.3.1.18 Usability	12-11
12.3.1.19 Device Software Upgradeability.....	12-11
12.3.2 Interoperability.....	12-11
12.3.2.1 Legacy Devices.....	12-11
12.3.2.2 Modern Devices	12-12
12.3.2.3 Suite B Devices.....	12-13
12.3.2.4 Reachability	12-13
12.4 LEF Test & Evaluation	12-14
12.4.1 Initialization/Functional.....	12-14

12.4.2	Personality/Cryptographic Algorithms	12-14
12.4.3	Interoperability.....	12-14
12.4.3.1	Synchronous Modes.....	12-14
12.4.3.2	Modern Link Encryption Interoperability and Interchangeability	12-14
12.4.4	Reliability.....	12-15
12.4.5	Reboot Test	12-15
12.4.6	Key Management Interface.....	12-15
12.4.6.1	Key Loading.....	12-16
12.4.6.2	Over-the-Air-Distribution or Over-the-Air-Re-Key	12-16
12.4.6.3	Change Key/Local Update Operations	12-16
12.4.7	Network Management.....	12-16
12.4.8	Ease of Software Loading.....	12-17
12.4.9	Degraded Network Capability and Robustness	12-17
12.4.10	Required Ancillaries Devices	12-18
12.4.11	Control Signal Requirements.....	12-18
12.4.12	Interface Requirements	12-19
12.5	SCIP Evaluation.....	12-20
12.5.1	General Description	12-20
12.5.1.1	Evaluation Methods	12-21

LIST OF FIGURES

<u>FIGURE</u>		<u>PAGE</u>
Figure 12.2-1.	Sample Network.....	12-2
Figure 12.2-2.	Example HAIPE Application Diagram	12-3
Figure 12.2-3.	LEF Application Example.....	12-5
Figure 12.2-4.	SCIP Network Example 1	12-6
Figure 12.2.5.	SCIP Network Example 2	12-7

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
Table 12.4-1.	Network Management Test Criteria.....	12-16
Table 12.4-2.	Ease of Software Loading Test Criteria	12-17
Table 12.4-3.	Clarity of Threshold Levels	12-17
Table 12.4-4.	Control Signal Requirements Matrix	12-18
Table 12.4-5.	Interface Requirement Matrix	12-20

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.

Use of Cryptographic Devices from Approved Products List (APL): Service components and organizations shall confirm with their respective Chief Information Officer (CIO) which cryptographic devices are appropriate for use on their communications networks. Devices on the UC APL must be internally validated by the services and components for use at the service or component level. The UC APL supports the Unified Capabilities or the Defense Information Systems Network (DISN); it does not replace a requirement for the services or components to obtain authorization from their service-specific CIO prior to procurement.

Devices that have not met service-specific requirements must be evaluated for appropriateness prior to acquisition and installation on any Department of Defense (DOD) network, either Deployable or Fixed.

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.

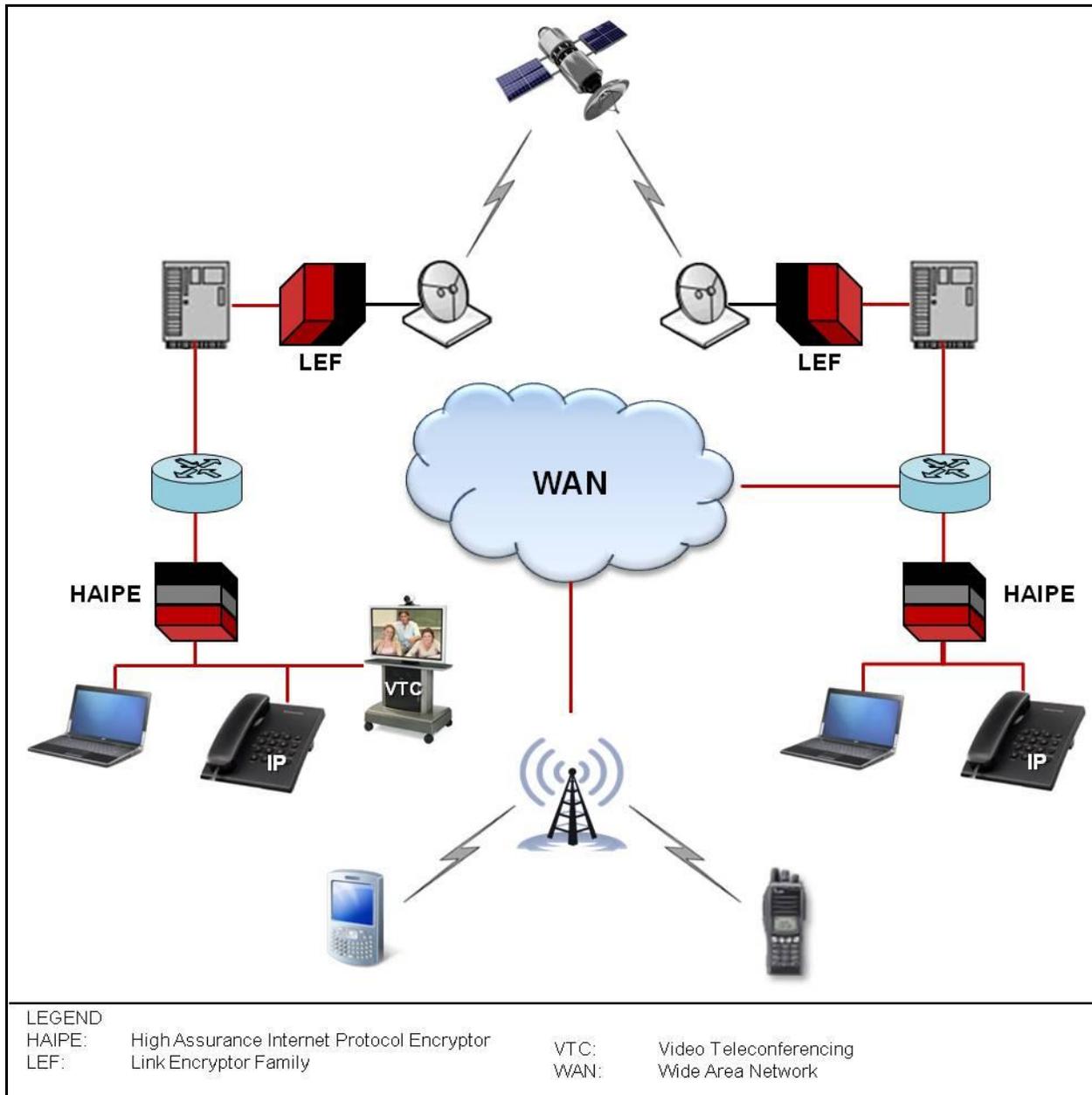


Figure 12.2-1. Sample Network

A HAIZE 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 HAIZE(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 HAIZE device is designed to provide confidentiality, integrity, and authentication services for IP traffic for Deployable and Fixed network applications. The HAIZE 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.

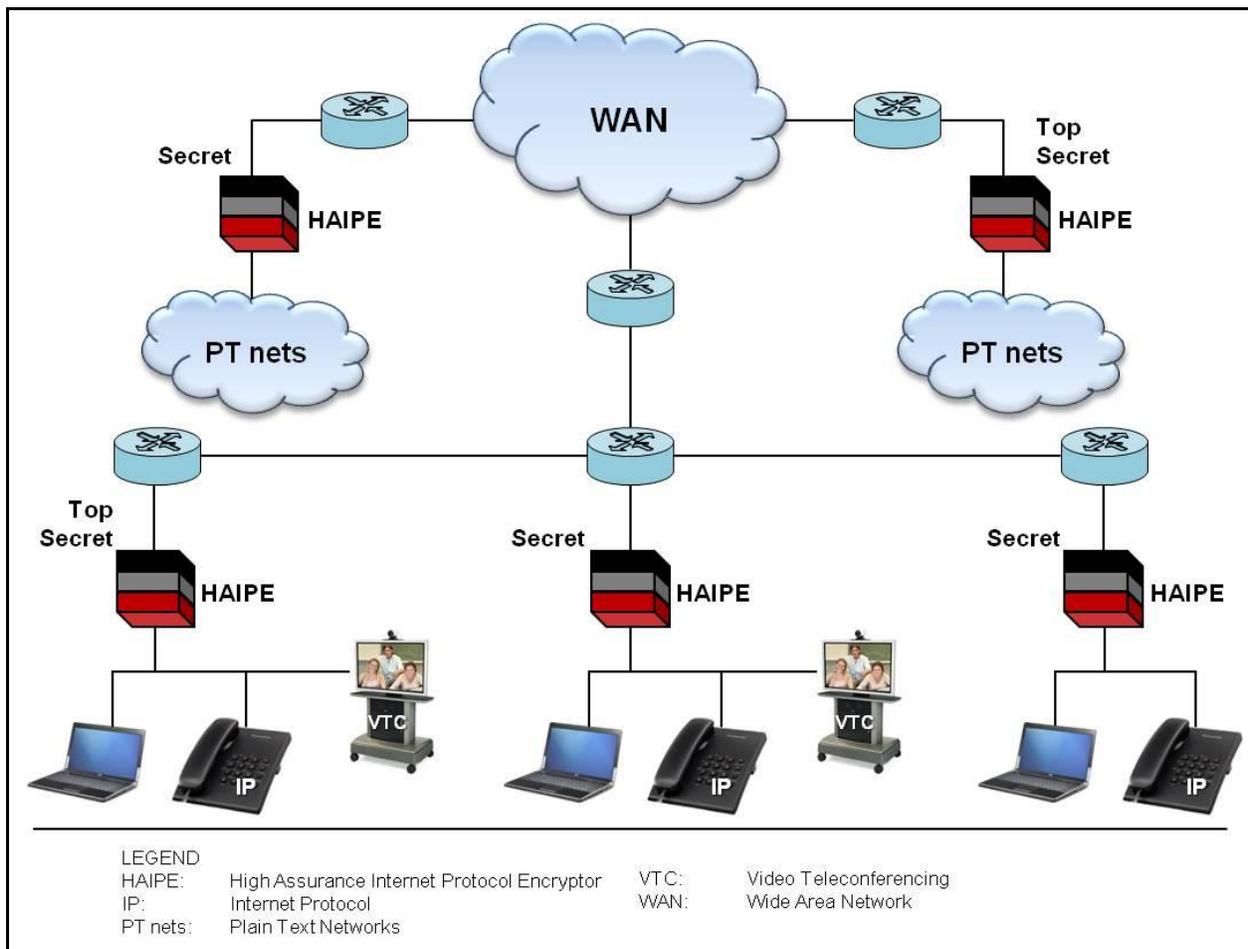


Figure 12.2-2. Example HAIPE Application Diagram

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.

12.2.2 Link Encryptor Family

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 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](#), LEF Application Example, illustrates the use of the LEF in a system.

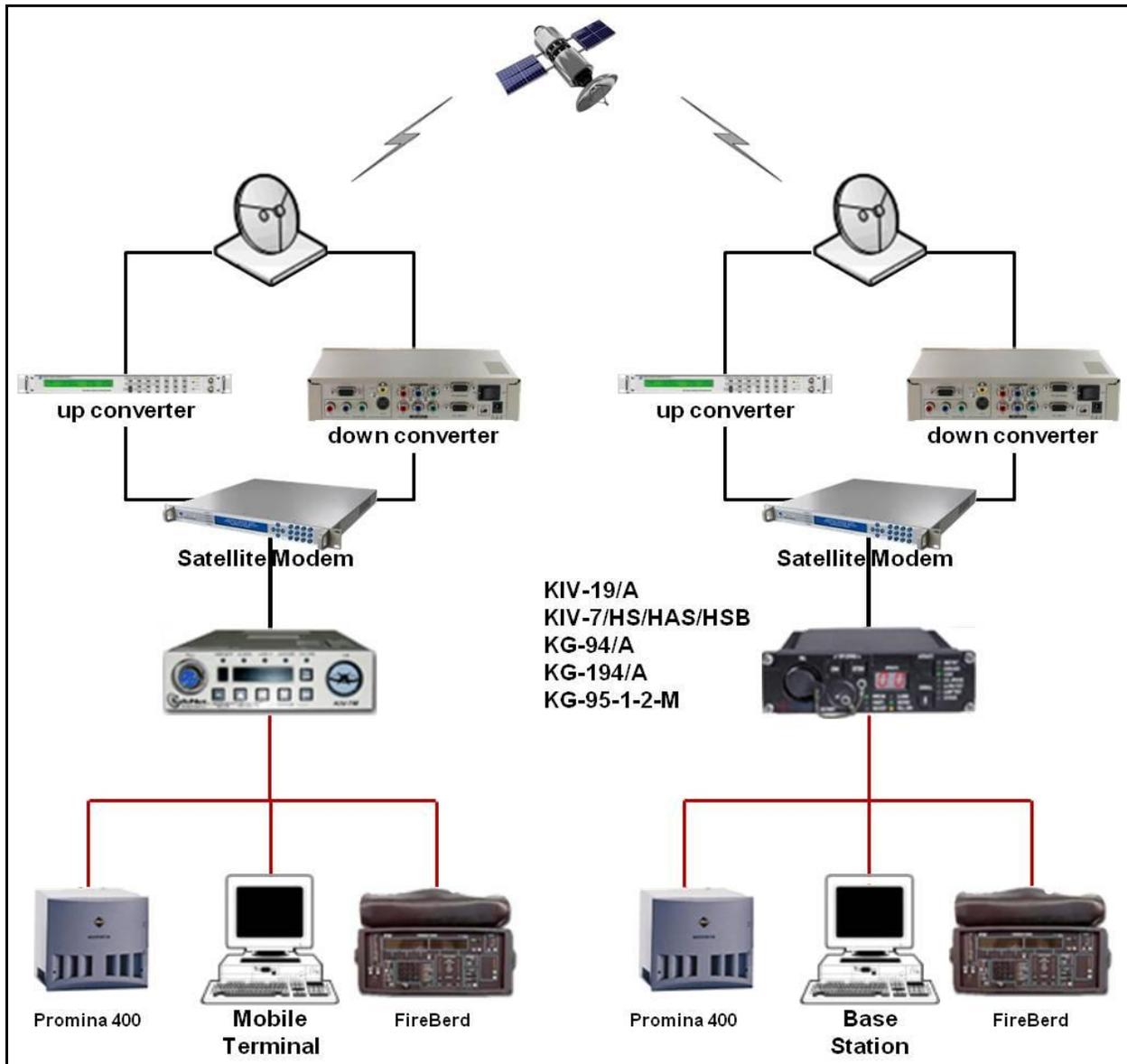


Figure 12.2-3. LEF Application Example

12.2.3 Secure Communications Interoperability Protocol

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.

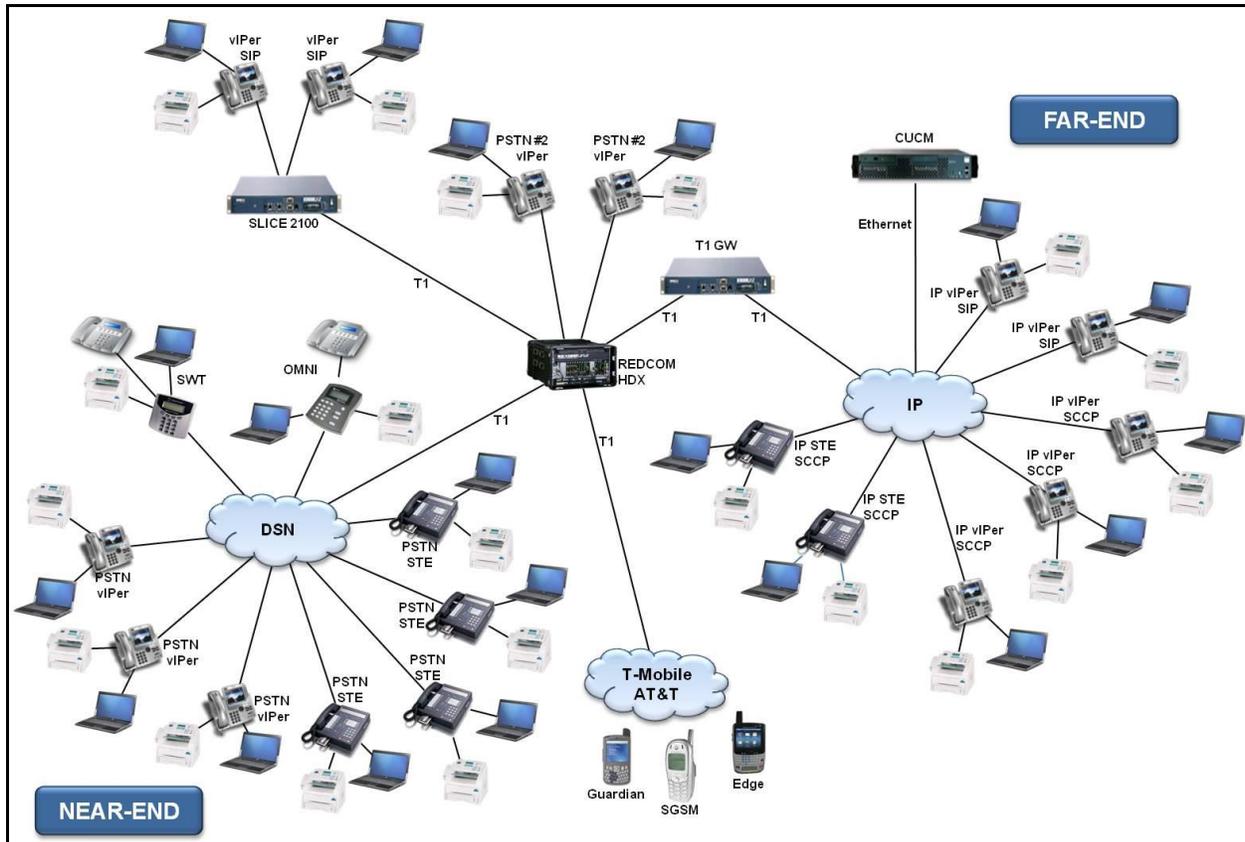


Figure 12.2-4. SCIP Network Example 1

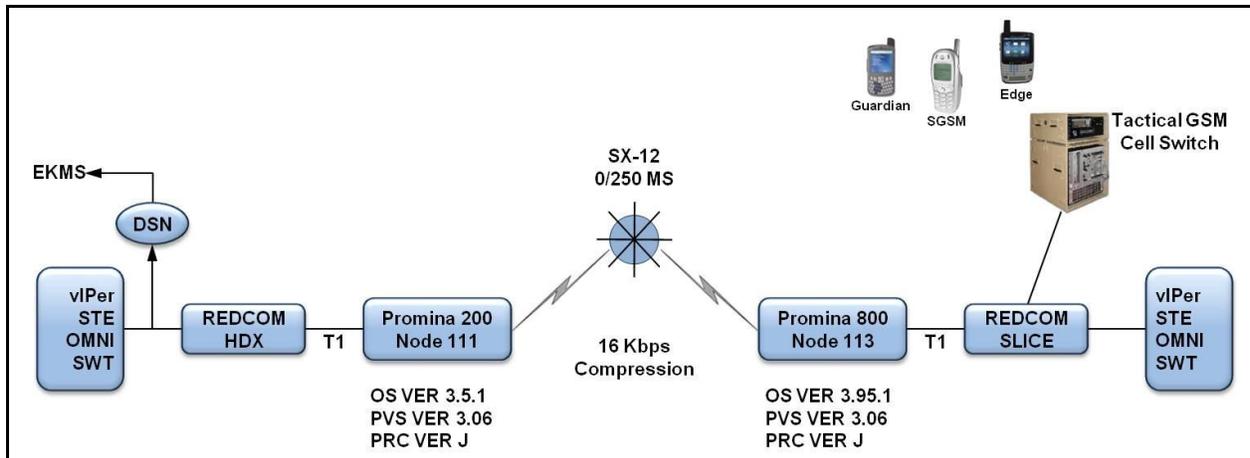


Figure 12.2.5. SCIP Network Example 2

12.3 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 Change (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, 128, 256, 512, 1024, 1280, and 1400).
- 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 on the Fly

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.

The Configuration Changes test should be used as an evaluation tool to determine when the device must be taken offline. Using the test results, an assessment is made on the device, based on the overall effect of configuration changes on In-line Network Encryptor (INE) availability. 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.” This is required to be performed in the field or at a forward repair facility.

The test evaluates the UUT’s procedures and tools [(e.g., tamper recovery crypto ignition key (CIK)] available for tamper recovery in the field or at a forward repair facility.

12.3.1.5 Loss of Physical Medium

The plaintext interface connection of the UUT is a wired interface connection. Sudden and abrupt loss of communication links is common and has the possibility of disrupting hardware. Further, the UUT can lose power temporarily. These two events are induced and observed. Here, the following severed links are evaluated:

- The UUT’s physical communications medium is severed; on reconnection, the UUT’s restoration of active security associations, and the time the UUT needs to accomplish this, is evaluated.
- The UUT’s power is cut during operation; when power is restored, the UUT’s need for new security associations, and the time the UUT needs to recover, is evaluated.

There is no pass or fail criteria for the Loss of Physical Communication Medium test. The test is used as an evaluation tool to determine device reactions to physical changes and device recovery time from power outages.

Using the test results, an assessment is made on the device's recovery time, based on the overall effect of configuration changes to the INE:

Poor 1:	Recovery time	\geq	2 minutes.
Fair 2:	1 minute	\leq	Recovery time < 2 minutes.
Good 3:	30 seconds	\leq	Recovery time < 1 minute.
Excellent 4:	Recovery time	<	30 seconds.

12.3.1.6 Line Impairment

INEs are not always used in areas with ideal or even adequate network conditions. The Line Impairment test shall verify that the device recovers secure communications after or during the interruptions. The device is tested to examine performance by altering the quality of the transmission line.

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. The term "latency" refers to any of several kinds of delays typically incurred in the processing of network data.

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 shall 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. The CM software can run on a number of operating systems or interfaces.

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, 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 type of devices:

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

12.3.2.1 Legacy Devices

All devices below are legacy devices and should be tested using legacy (HAIPE IS v1.3.5) algorithms/transforms for both PPK (Baton-48) and Firefly (Medley-8).

1. General Dynamics Tactical Local Area Network Encryptor (TACLANE) KG-175 Classic.
The KG-175 Classic is limited to 10-Half Duplex Speeds.
2. General Dynamics TACLANE KG-175 E100.
The KG-175 E100 is capable of 10/100-Full Duplex Speeds.
3. General Dynamics TACLANE KG-175A (GigE).
The KG-175A is capable of 10/100/1000-Full Duplex Speeds.
4. General Dynamics TACLANE KG-175B (Mini).

The KG-175B is capable of 10/100-Full Duplex Speeds..

5. General Dynamics Sectera KG-235.

The KG-235 is capable of 10-Half Duplex Speeds.

6. Altasec KG-255.

The KG-255 is capable of 10/100/1000-Full Duplex Speeds.

7. L-3 Communications KOV-26 (Talon).

The KOV-26 (Talon) is capable of approximately 10-Full Duplex Speeds.

8. Harris KIV-54 (SecNet 54).

The KIV-54 is capable of 10/100-Full Duplex Speeds.

9. Safenet KIV-7MIP.

The KIV-7MIP is capable of 10/100-Full Duplex Speeds.

12.3.2.2 Modern Devices

These are modern devices and should be tested using modern (HAIPE IS 3.x) algorithms/transforms for both PPK and Firefly (Medley-4).

1. General Dynamics TACLANE KG-175D (Micro).

The KG-175D is capable of 10/100-Full Duplex Speeds.

2. L-3 Communications KG-245A.

The KG-245A is capable of 10/100/1000-Full Duplex Speeds.

3. L-3 Communications KG-240A.

The KG-240A is capable of 10/100-Full Duplex Speeds.

4. L-3 Communications KG-245X.

The KG-245X is capable of 10 Gigabit-Full Duplex Speeds.

5. Altasec KG-250.

The KG-250 is capable of 10/100-Full Duplex Speeds.

6. Altasec KG-250X.

The KG-250X is capable of 10/100-Full Duplex Speeds.

12.3.2.3 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 (CHVPs). 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).

1. General Dynamics TACLANE KG-175D (Micro).

The KG-175D is capable of 10/100-Full Duplex Speeds.

2. L-3 Communications KG-245A.

The KG-245A is capable of 10/100/1000-Full Duplex Speeds.

3. L-3 Communications KG-240A.

The KG-240A is capable of 10/100-Full Duplex Speeds.

4. Altasec KG-250.

The KG-250 is capable of 10/100-Full Duplex Speeds.

5. Altasec KG-250X.

The KG-250X is capable of 10/100-Full Duplex Speeds.

6. Altasec IPS-250.

This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.

7. General Dynamics C-100.

This CHVP, Suite B only product is capable of 10/100-Full Duplex Speeds.

12.3.2.4 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 will also be tested in various timed intervals after a stress test of operations. These intervals will 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.

Asynchronous data communication is used throughout many older Army systems. It is a vital part of the KG-84A/C operation. Table B-1 lists the different modes of operation of an LEF device. The UUT must communicate with the reference encryptors in all modes.

The UUT must also operate in the Suite A and Suite B personalities, using the equivalent asynchronous options.

12.4.3.1 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.

Table B-2 lists the synchronous modes supported by current LEF devices. The LEF encryptor UUT is tested against all supported modes within the matrix. In each mode, data rates from 50 bps to the maximum data rate supported by that algorithm are tested. There are 25 random data rates chosen between the maximum and minimum data rates for this test, ensuring that the UUT can operate at a variety of data rates.

12.4.3.2 Modern Link Encryption Interoperability and Interchangeability

Modern link encryptors must be interoperable so that different systems can choose different encryptors and operate without error. Interchangeability is equally important so that a system can use whatever encryptor is available. This interchangeability also increases the options available to a system for choosing an encryptor.

To test interoperability, the UUT is 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. Devices labeled with an “M” in Table B-3 must fulfill the requirement for modern testing.

To test interchangeability, the UUT is replaced by other modern-link encryptors. The procedure, cables, racks, and other ancillaries are noted; conversion instructions are created as necessary. These instructions detail the cost and work required for the conversion and alert users of any issues. The UUT is then used to replace all other modern-link encryptors. Conversion instructions are created for this procedure.

12.4.4 Reliability

To test reliability, a log is kept of any unit errors that occur during test conduct. This includes the cold startup and reboots time of each configuration and test. Any defects are noted. A defect is defined as the inability to initialize, pass traffic as specified, or report status. Based on this information, an observed Mean Time Between Failures (MTBF) is derived from the CM Branch’s laboratory testing. Results are compared to the vendors specified 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).

The observed MTBF is combined with Mean Time To Repair (MTTR) (it does not include configuration or rekey time) to determine network availability.

12.4.5 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 Key Management Interface

The Communications-Electronics Research, Development and Engineering Center (CERDEC) conducts tests on all applicable End Cryptographic Devices that are supported or interact with the Army Key Management System and the Key Management Fill Device being tested.

12.4.6.1 Key Loading

The UUT is tested 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 will receive a FAIL.

12.4.7 Network Management

The UUT must be manageable via Ethernet port by a remote system. This will satisfy the net-centric requirement. The UUT is tested using human manual interaction and computer automated HyperText Transfer Protocol, Secure (HTTPS) requests/posts to verify the robustness and viability of the UUT human-computer interface (HCI) (see [Table 12.4-1](#)). To pass, the UUT must properly process all requests. If the UUT has a buffer feature in which consecutive requests are given during long processes, then it is acceptable if the UUT ignores or rejects those requests. At no time should the UUT suffer a system failure when it enters an alarm state.

Table 12.4-1. Network Management Test Criteria

RANK	GRADE	CRITERIA
Failure	0	No Ethernet port
Poor	1	Poor configuration of HCI

RANK	GRADE	CRITERIA
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 Ease of Software Loading

Instructions for software loading and upgrading are followed verbatim, using a combination of original equipment manufacturer (OEM) documentation provided with the firmware upgrade and the latest operator's manual. It is graded on whether the instructions available are lacking or sufficient. Test conduct evaluates the ease of use and the capability of using commercial off-the-shelf (COTS) equipment (see [Table 12.4-2](#)).

Table 12.4-2. Ease of Software Loading 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

Also, the procedure evaluates the UUT for mass updating capabilities and single-button operation updates. This process consists of loading a single file through the management port. The ability to connect multiple units to a network is preferable in an update environment. Additionally, the length of time and the skill required are reported in logistical support analysis.

12.4.9 Degraded Network Capability and Robustness

During test conduct, network delays and bit errors are added to evaluate the LEF encryptor's operational thresholds. These values are compared to legacy LEF devices to evaluate whether or not the LEF encryptor under test is a suitable replacement device. The standard for the thresholds is the highest threshold measured among legacy devices for each test case (see [Table 12.4-3](#)). If there are no legacy devices available for reference, then the test case reverts to similar legacy configurations to generate the threshold number.

Table 12.4-3. Clarity of Threshold Levels

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 ($<10^{-5}$)

RANK	GRADE	CRITERIA
Good	3	Device passes test with intermediate delay and error (<10<3)
Excellent	4	Device passes test with extreme delay and error (>=10^3)

LEF devices must accept a wide variety of network timing and variable speeds. Standard LEF test speeds range from 50 bits per second (bps) to 50 megabits per second (Mbps). Even though the test cases outline specific speeds within the 50 bps to 50 Mbps, tests are conducted at selected rates within the range. Test conduct proceeds with both extremes of data rate to include low and high rates as well as test conduct at regular step intervals as test equipment permits.

Clock sources are provided from the BLACK and RED sides. The UUT is tested in both configurations with either the BLACK or the RED timing is provided. When the UUT does not support the RED-side clock, the standard Defense Information Systems Agency (DISA) W11 Transmission Security (TRANSEC) cable is used so that the RED-side clock can be compared, even if the UUT does not directly support it.

The UUT is tested in applications of random cable lengths up to 150 feet. If the UUT fails at 150-foot lengths, the distance is reduced by 10-foot segments until the UUT operates properly. The distance is recorded if the UUT fails at the 150-foot length.

12.4.10 Required Ancillaries Devices

Interface connections are established and verified for each swapped 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 are 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 is tested for its supported control signals. Any signals not supported are noted as deficiencies because the UUT will not be able to fully replace them.

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						

ALGORITHM	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
	A	B	W	S	A	B	W	S	S	S	S	S	S	S	W	W	W	W	W	W
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 UUT 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

ALGORITHM	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	
	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	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

This section describes the requirements that will be 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 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 UC SIP 2013, Section 2.14.10, MG Support for ISDN PRI Trunks, for PRI, and Section 4, SIP Requirements for UC SIP Signaling Appliances and UC SIP EIs, for the UC SIP.

3. Call Completion Rate.

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

4. Multiple SCIP Modes.

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.

5. Latency.

The DSCD shall operate in a network that has an end-to-end (E2E) latency of up to 600 milliseconds.

6. Voice Quality.

The DSCD shall achieve and maintain a secure voice connection with a minimum mean opinion score (MOS) of 3.0.

7. Rekey.

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.

8. 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.

9. Minimum Data Rate.

The DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.