Hughes Network Systems, LLC
Hughes SPACEWAY Crypto Kernel
Firmware Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.6

Prepared for:

HUGHES®

Hughes Network Systems, LLC
11717 Exploration Lane,
Germantown, MD 20876
United States of America

Phone: +1 (301) 428-2762
http://www.hughes.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Hughes SPACEWAY Crypto Kernel (firmware version: 1.0) from Hughes Network Systems, LLC. This Security Policy describes how the Hughes SPACEWAY Crypto Kernel meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Hughes SPACEWAY Crypto Kernel is referred to in this document as the HSCK, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- Hughes corporate website (http://www.hughes.com) contains information on the full line of products from Hughes.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Validation Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Hughes. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Package is proprietary to Hughes and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Hughes.

2 Hughes SPACEWAY Crypto Kernel

2.1 Overview

Geostationary satellite coverage available via SPACEWAY 3 satellite from Hughes Network Systems, LLC provides the capability to deliver broadband internet service to individual consumers and businesses in the continental US (CONUS) coverage area. Optimized for broadband IP[1] services, Hughes SPACEWAY systems support a wide variety of applications, from high-speed Internet/intranet access to video conferencing. The Hughes SPACEWAY system is a broadband satellite system, designed and optimized for carrier-grade IP broadband networking and specialized for applications such as mobility and mesh networking. The system includes an economical access gateway earth station and high performance remote satellite terminals.

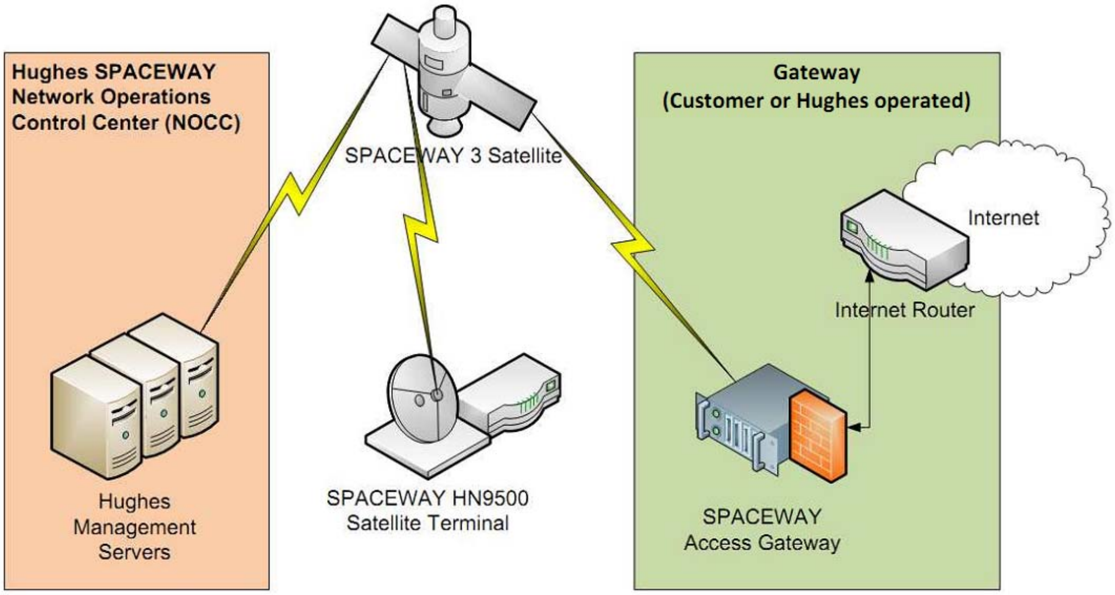
Hughes SPACEWAY Network Operations Control Center (NOCC)
SPACEWAY 3 Satellite
Gateway (Customer or Hughes operated)
Internet
Internet Router
Hughes Management Servers
SPACEWAY HN9500 Satellite Terminal
SPACEWAY Access Gateway

Figure 1 – Hughes SPACEWAY System Typical Deployment

The SPACEWAY system provides secure communication over an IPsec[2] protocol. The design of the SPACEWAY system includes the centralization of cryptographic functionality into a common cryptographic engine called the Hughes SPACEWAY Crypto Kernel (HSCK). The HSCK is used by the following components of the SPACEWAY systems for secure communications:

- SPACEWAY Access Gateway: A core component of a SPACEWAY System deployment is the Access Gateways (AGWs), where uplinks to the satellite and Internet infrastructure are available. The Access Gateway uses a proprietary SPACEWAY encoding protocol for the outbound channel received by all SPACEWAY Satellite Terminals (ST). STs utilize FDMA[3]/TDMA[4] channels to communicate back to the Access Gateway (when deployed in star mode) or to each other (when configured in mesh mode).

[1] IP – Internet Protocol
[2] IPsec – Internet Protocol Security
[3] FDMA – Frequency-Division Multiple Access
[4] TDMA – Time-Division Multiple Access

- HN9500 Satellite Router: The HN9500 is Hughes' high-performance satellite router that enables carrier-grade broadband IP services with enhanced security and selectable data rates to satisfy the most demanding bandwidth requirements. The HN9500 Satellite Router (Figure 2 below) is one of the available Satellite Terminals within the SPACEWAY system.

Figure 2 – HN9500 Satellite Router

HN9500 Satellite Routers are intended to be deployed in the field acting as the local access points to the satellite communication system and, ultimately to the network infrastructure. The HN9500 provides a broad array of standard networking functionality in a compact, high-performance package, allowing users to configure any combination of mesh and star topologies to create highly secure, broadband IP networks.

The HSCK provides the following basic functionalities:

- Creation of dynamically-generated shared session keys using Internet Key Exchange (IKE)
- Establishment and teardown of IPSec tunnels between two or more hosts
- Advanced Encryption Standard (AES) 128- or 256-bit encryption on all data transfer within an IPsec tunnel
- Message authentication and integrity using Keyed-Hash Message Authentication Code (HMAC) with SHA[5]1 or SHA256 as per the configuration

The module provides cryptographic and secure communication services for other applications developed by Hughes as described above. In this document, those applications will be collectively referred as a host application. The Hughes SPACEWAY Crypto Kernel is validated at the FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1

[5] SHA – Secure Hashing Algorithm

Section	Section Title	Level
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[6]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	1

2.2 Module Specification

The Hughes SPACEWAY Crypto Kernel is a firmware module with a multi-chip standalone embodiment. The overall security level of the module is 1. The physical cryptographic boundary of the Hughes SPACEWAY Crypto Kernel is the appliance upon which it runs; however, the module is in the form of a standalone binary object file. The HSCK module has been validated and tested for use on the custom-built Hughes HN9500 Satellite Terminal (ST) and the Access Gateway (AGW) appliances running the VxWorks 5.4 operating system.

The HSCK module comprises a single binary object file. This object file is used to provide a cryptographic Application Programming Interface (API) to the applications of the ST and AGW appliances. The HSCK module provides an API for invocation of FIPS-Approved cryptographic functions from host applications. The logical cryptographic boundary of the module is shown in Figure 3 and indicated with a dotted line.

[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

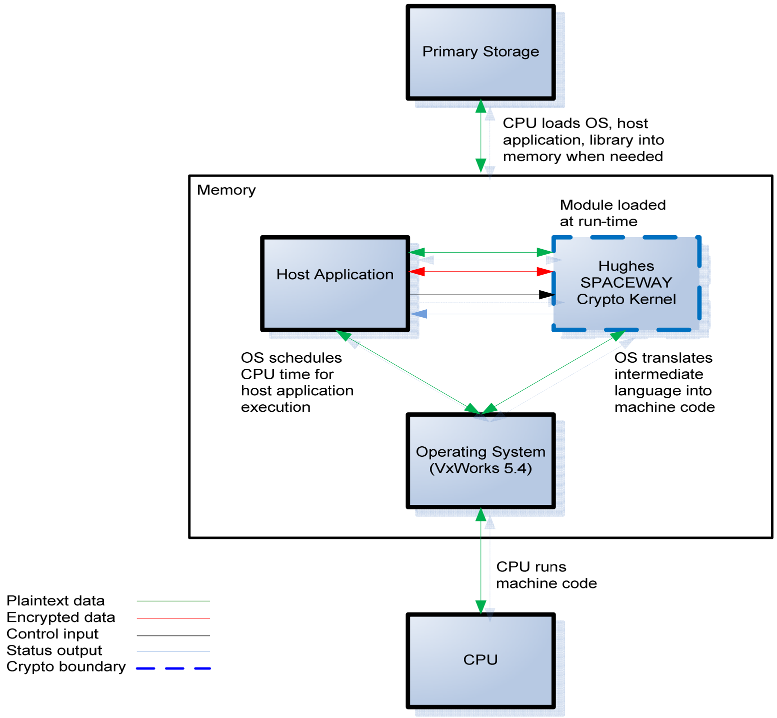
Primary Storage
CPU loads OS, host application, library into memory when needed
Memory
Module loaded at run-time
Host Application
Hughes SPACEWAY Crypto Kernel
OS schedules CPU time for host application execution
OS translates intermediate language into machine code
Operating System (VxWorks 5.4)
CPU runs machine code
Plaintext data
Encrypted data
Control input
Status output
Crypto boundary
CPU

Figure 3 – Hughes SPACEWAY Crypto Kernel Cryptographic Boundary

The module runs on a VxWorks 5.4 operating system on a custom-built Hughes HN9500 and a Commercial Off-The-Shelf (COTS) HP ProLiant DL320 Generation 2 and 5 servers (AGWs). Figure 4 and Figure 5 show the block diagrams of the HN9500 and AGW appliances.

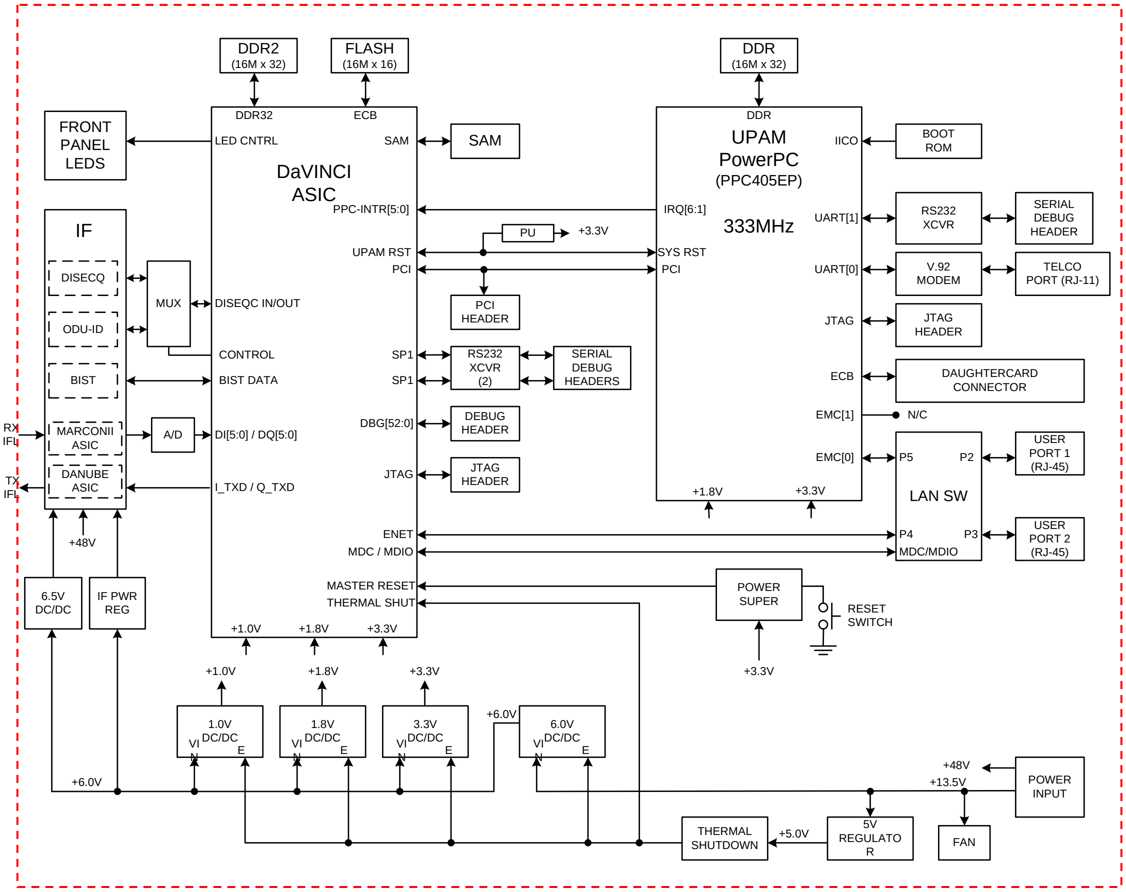

Figure 4 – Hardware Block Diagram for HN9500

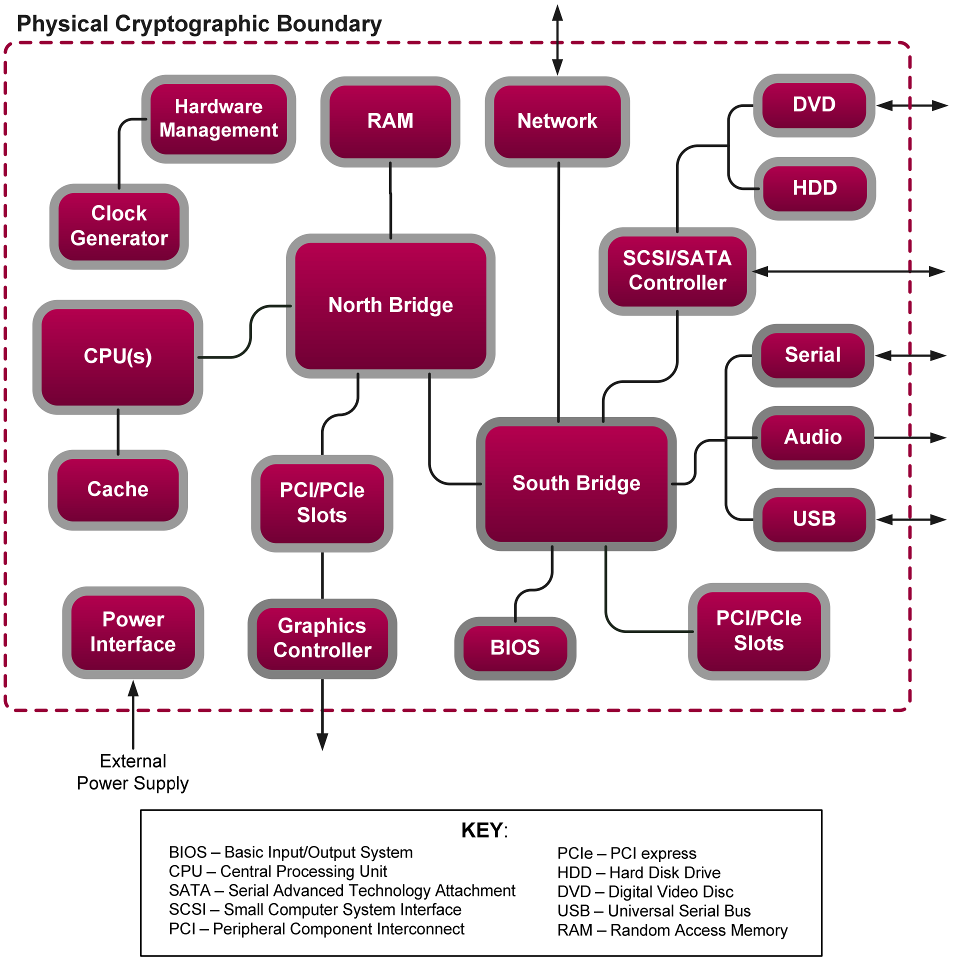

Figure 5 – Hardware Block Diagram for AGW

2.3 Module Interfaces

The HSCK implements distinct module interfaces in its firmware design. Physically, the module ports and interfaces are considered to be those of the host platform that the firmware runs upon. However, the firmware communicates through an Application Programming Interface (API), which allows a host application to access the module. Both the APIs and the physical ports/interfaces can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

These logical interfaces (as defined by FIPS 140-2) map to the platform's physical interfaces, as described in Table 2. All of these physical interfaces are separated into the logical interfaces required by FIPS 140-2 as described in Table 2.

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Physical Port/Interface		Hughes SPACEWAY Crypto Kernel Interface
	HN9500 Satellite Router	Access Gateway	
Data Input Interface	• Ethernet ports (2) • Serial port • Satellite IN port	• Ethernet ports (2) • Serial connector • Keyboard connector • Mouse connector • USB connectors (4)	Arguments for a function that takes the data to be used or processed by the module
Data Output Interface	• Ethernet ports (2) • Serial port • Satellite OUT port	• Ethernet ports (2) • Serial connector • Video connector • USB connectors (4)	Arguments for a function that specify where the result of the function is stored
Control Input Interface	• Ethernet ports (2) • Serial port • Satellite IN port	• Ethernet ports (2) • Serial port • iLO management port • Keyboard connector • Mouse connector • UID button • USB connectors (4) • Power button	Function arguments used to control the operation of the module
Status Output Interface	• Ethernet ports (2) • Serial port • Satellite IN port • LEDs	• Ethernet ports (2) • Serial connector • iLO management port • Video connector • USB connectors (4) • LEDs	Return values for function calls or function argument in 'hck_module_status_t' data structure
Power Interface	• Power interface • 48V, 13.5V external AC/DC power supply	• Power interface • 48V DC power supply	Not Applicable

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and a User role. The module does not support authentication mechanisms. Role assumption is implicit; operators assume their role based on the service selected for execution.

2.4.1 Crypto-Officer Role

The Crypto-Officer (CO) role is responsible for initializing the module, zeroizing keys and CSPs[7], performing self-tests, and monitoring status. Descriptions of the services available to the Crypto-Officer role are provided in Table 3. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read access: The CSP may be read.
- W – Write access: The CSP may be established, generated, modified, or zeroized.

[7] CSP – Critical Security Parameter

- X – Execute access: The CSP may be used within an Approved or Allowed security function or authentication mechanism.

Table 3 – Crypto-Officer Services

Service	Description	CSP and Type of Access
hck_init()	Validates input parameters before performing power-on self-tests; Initializes configuration	None
hck_initialize_csp()	Initializes the CSPs for a peer	IPsec Traffic key – W IPsec MAC key – W
hck_zeroize_csp()	Zeroizes IKE/IPsec ephemeral CSPs	IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W
hck_shutdown()	Shuts down all crypto functionality	None
hck_do_self_tests()	Performs power-on self-tests	None
hck_get_status()	Retrieves the crypto-module status	None
hck_get_name_and_version()	Retrieves the module name and version number	None
hck_get_version()	Retrieves the module's major and minor version numbers	None
hck_get_fips_mode()	Determines whether or not FIPS mode has been enabled	None
hck_print_status()	Prints module status variables and statistics to a display or log file	None
hck_update_parms()	Sets configuration parameters based on module's current mode of operation	None

2.4.2 User Role

The User role establishes IKE/IPsec sessions and utilizes secure communication functionality provided by the module. Descriptions of the services available to the User role are provided in Table 4. CSP access types (R, W, or X) are defined in Section 2.4.1 above.

Table 4 – User Services

Service	Description	CSP and Type of Access
hck_process_ike_event()	Ensures that the crypto-module is active and validates input parameters before processing a received IKE packet or provides a timer event to the IKE state machine	Preshared key – R, W, X IPsec Traffic key – W IPsec MAC key – W IKE Key Agreement key – W Entropy Input string – W, X DRBG seed – W, X
hck_process_tx_pkt()	Ensures that the crypto-module is active and validates input parameters before processing IPsec transmission packet	IPsec Traffic key – X IPsec MAC key – X Entropy Input string – W, X DRBG seed – W, X
hck_process_rx_pkt()	Ensures that the crypto-module is active and validates input parameters before processing IPsec received packet	IPsec Traffic key – X IPsec MAC key – X Entropy Input string – W, X DRBG seed – W, X
hck_send_ike_msg()	Ensures that the crypto-module is active and validates input parameters before invoking IKE transmit function	IKE Key Agreement key – R

2.5 Physical Security

Since this is a firmware module, the module relies on the host platform (a purpose-built Hughes appliance or a COTS HP ProLiant DL320 G5 server) to provide the mechanisms necessary to meet FIPS 140-2 physical security requirements. All components of the target platform are made of production-grade materials, and all integrated circuits are coated with commercial standard passivation.

The host platforms have been tested for and meet applicable Federal Communications Commission (FCC) Electromagnetic Interference and Electromagnetic Compatibility requirements for business use as defined in Subpart B of FCC Part 15.

2.6 Operational Environment

On the host platforms, Hughes employs VxWorks 5.4, a non-modifiable OS. Hence, the operational environment requirements do not apply to the firmware module.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES CBC[8] (128-, 256-bit key)	1788
SHA-1, SHA-256	1570
HMAC SHA-1, HMAC SHA-256	1053
HMAC-based SP800-90 DRBG	126

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementations:

- MD5[9] - used for the firmware integrity test
- Diffie-Hellman - key agreement mechanism (caveat: 1024-bit or 2048-bit Diffie-Hellman key agreement protocol provides 80 or 112 bits of encryption strength)

The module supports the CSPs listed below in Table 6.

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key Type	Generation / Input	Output	Storage	Zeroization	Use
Pre-shared key	Generated externally, enters the module in plaintext	Never exits the module	Resides in plaintext on volatile memory	Reboot	Generation of the IPsec Traffic key and internal IKE authentication
IKE Key Agreement key	Generated internally during IKE Phase 1 negotiation	Never exits the module	Plaintext in volatile memory	Reboot or on key derivation completion	Exchange of shared secret during IKE
IKE Session key	Generated internally during IKE Phase 1 negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp()' function	Encryption or decryption of IKE sessions
IKE MAC key	Generated internally during IKE Phase 1 negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp()' function	Data authentication during IKE sessions
IPsec Traffic key	Generated internally during IKE Phase 2 negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp()' function	Encryption or decryption of IPsec ESP packets
IPsec MAC key	Generated internally during IKE Phase 2 negotiation	Never exits the module	Plaintext in volatile memory	Reboot, session termination, or by calling to 'hck_zeroize_csp()' function	Authentication of IPsec ESP packets

[8] CBC – Cipher Block Chaining
[9] MD5 – Message Digest 5

Key Type	Generation / Input	Output	Storage	Zeroization	Use
DH public key	Generated internally	Exits the module in plaintext	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key and IPsec session key
DH private key	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key and IPsec Session key
Entropy Input string	Continually polled from various system resources to accrue entropy	Never exits the module	Plaintext in volatile memory	Reboot	Random number generation
DRBG seed	Generated internally using nonce and personalization string along with entropy input	Never exits the module	Plaintext in volatile memory	Reboot	Random number generation

2.8 Self-Tests

The HSCK performs a set of self-tests upon power-up and conditionally as required in FIPS 140-2.

2.8.1 Power-Up Self-Tests

Power-up self tests are executed automatically when the module is loaded into memory space. If any one of the self-tests fail, the module enters an error state and prevents all cryptographic data processing and functionality. The Hughes SPACEWAY Crypto Kernel performs the following power-up self-tests:

- Firmware integrity test using an Error Detection Code (MD5 hash)
- Known Answer Tests (KATs)
  - AES KAT (encryption and decryption)
  - SHA-1 and SHA-256 KATs
  - HMAC SHA-1 and HMAC SHA-256 KATs
  - SP800-90 HMAC-based DRBG KAT

2.8.2 Conditional Self-Tests

The module performs a Continuous RNG Test (CRNGT) for the Approved DRBG to ensure that the 256-bit random result is not equivalent to the previous result. Upon reseed, the CRNGT for the reseed also verifies that the next seed value is not equivalent to the previous seed value.

2.8.3 Critical Functions Self-Tests

At the power-up, the module also tests for the following:

- Minimum available memory on the host platform
- Operating system version

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any additional attacks in its FIPS-Approved mode of operation.

3 Secure Operation

The Hughes SPACEWAY Crypto Kernel meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-Approved mode of operation. Section 3.1 below provides guidance to the Crypto-Officer for managing the module.

3.1 Secure Management

The Hughes SPACEWAY Crypto Kernel is distributed by Hughes installed on a custom appliance as part of a single monolithic binary image containing the Hughes' HN9500 and AGW system applications, and is not distributed as a separate binary. Thus, module operators are not required to perform any steps to ensure that the module is running in its FIPS-Approved mode of operation.

Host applications must first call the function hck_install() to load and initialize the module. This function call is the entry point to the module, and ensures that all necessary power-up self-tests are called. When properly initialized, the HSCK will only operate in its defined FIPS-Approved mode of operation. Any use of the module without proper initialization will result in the module operating in a non-Approved manner.

3.1.1 Initialization

On host platforms, VxWorks 5.4 is a non-modifiable operating system; hence, it does not require to be configured for single user mode. The module itself checks for the OS version and available memory on the platform at startup.

3.1.2 Management

The Crypto-Officer should monitor the module's status regularly and make sure only the services listed in Table 3 and Table 4 are being used. If any irregular activity is noticed or the module is consistently reporting errors, then Hughes Network Systems customer support should be contacted.

3.1.3 Zeroization

The module does not persistently store any key or CSPs. All ephemeral keys used by the module are zeroized upon reboot, or session termination. The Crypto-Officer can also zeroize keys by calling the hck_shutdown() function.

3.2 User Guidance

Only the module's cryptographic functionalities are available to the User. Users are responsible to use only the services that are listed in Table 4. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is observed.

4 Acronyms

This section lists acronyms used in the document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CCI	Common Cryptographic Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
COTS	Commercial Off-the-Shelf
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DC	Direct Current
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FDMA	Frequency-Division Multiple Access
FIPS	Federal Information Processing Standard
HSCK	Hughes SPACEWAY Crypto Kernel
HMAC	(Keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPGW	Internet Protocol Gateway
IPsec	Internet Protocol Security
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest
NIST	National Institute of Standards and Technology
NOCC	Network Operations Control Center
OS	Operating System

PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
SHA	Secure Hash Algorithm
TDMA	Time-Division Multiple Access

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com