Hughes Network Systems

Hughes Crypto Kernel

(Software Version 1.2 on Windows Server 2003;
Firmware Version 1.2 on VxWorks 5.4)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 1.0

Prepared for:

Hughes Network Systems
11717 Exploration Lane
Germantown, MD 20876
Phone: (301) 428-5500
Fax: (301) 428-1868
http://www.hughes.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2008-01-22	Xiaoyu Ruan	Release.

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 Crypto Kernel (software version 1.2 on Windows Server 2003; firmware version 1.2 on VxWorks 5.4) from Hughes Network Systems. This Security Policy describes how the Hughes Crypto Kernel (HCK) meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the US 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) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/index.html.

The Hughes Crypto Kernel is also referred to in this document as HCK 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:

- The Hughes Network Systems website (http://www.hughes.com/) contains information on the full line of products from Hughes.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to 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 Machine
- Installation Guides
- 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 Documentation is proprietary to Hughes and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Hughes.

2 Hughes Crypto Kernel Module

2.1 Overview

The HCK is packaged as a dynamic library, libhck.a or hck.dll, implemented in two different products. libhck.a is implemented in the Very Small Aperture Terminal (VSAT) which is a satellite based router running VxWorks 5.4. hck.dll is implemented in the Virtual Private Network (VPN) Internet Protocol (IP) gateway running on a general purpose computer (GPC) running Microsoft Windows Server 2003. The library provides the following basic functionalities:

- establish and teardown IP Security (IPsec) tunnels between two or more hosts
- create dynamically generated shared session keys using Internet Key Exchange (IKE)
- perform Advanced Encryption Standard (AES) 128-bit encryption on all data transfer within an IPsec tunnel
- ensure message authentication and integrity using Keyed-Hash Message Authentication Code (HMAC)-Secure Hash Algorithm (SHA)-1

2.2 Module Specification

The Hughes Crypto Kernel is a multi-chip standalone module that meets overall Level 1 FIPS 140-2 requirements. Based on the platform on which the HCK is running on, the module can be considered as either software or firmware, as detailed below.

- When the HCK source is compiled for use on a GPC running the Windows Server 2003 Operating System (OS) in single-user mode, the HCK is a software module. The server is placed in single-user mode by disabling all remote guest accounts in order to ensure that only one operator can log into the OS at a time. The services that are disabled are server services, terminal services, remote registry services, and remote desktop and remote assistance service. See Section 3.2.1 for details.
- When the HCK source is compiled for use on the Hughes Very Small Aperture Terminal (VSAT) satellite router (see Figure 1), the HCK is a firmware module. The VSAT satellite router is a custom hardware appliance running VxWorks 5.4 OS.

Figure 1 – Hughes VSAT Satellite Router

The module's physical cryptographic boundary on the GPC platform is defined by the metal enclosure over the GPC motherboard. The module supports the physical interfaces of a GPC. The physical ports include the computer keyboard port, optical drives, floppy-disk drive, mouse port, serial ports, parallel ports, networks ports, monitor port, and power plug (see Figure 2).

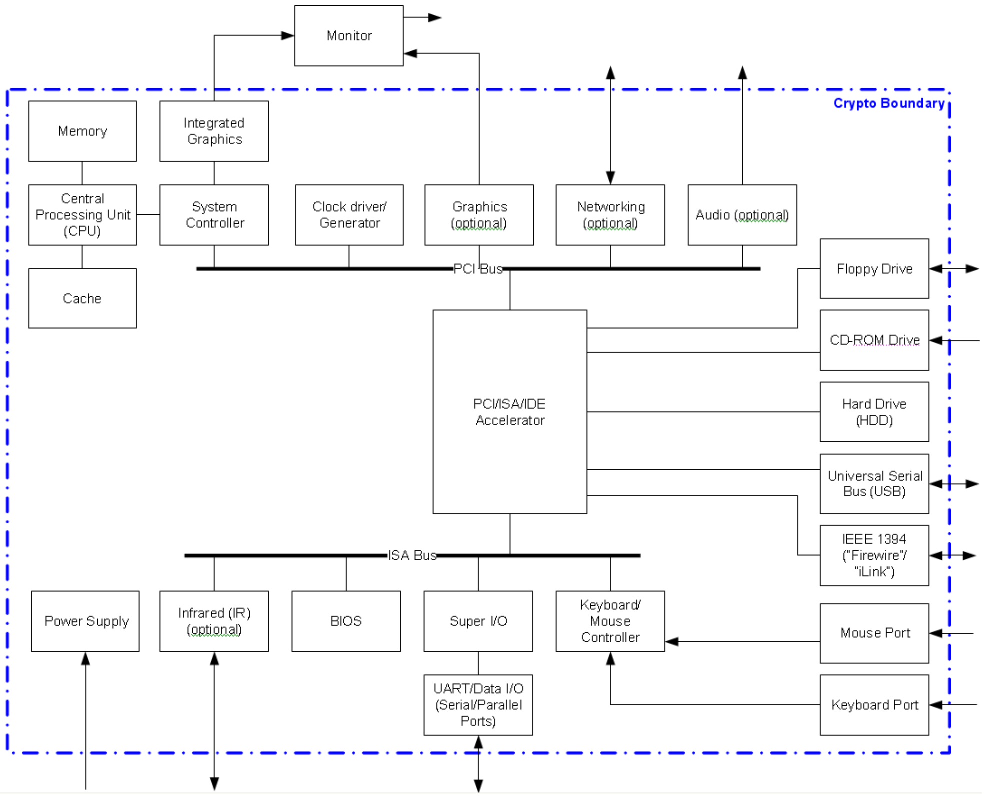

Figure 2 – Standard GPC Physical Block Diagram

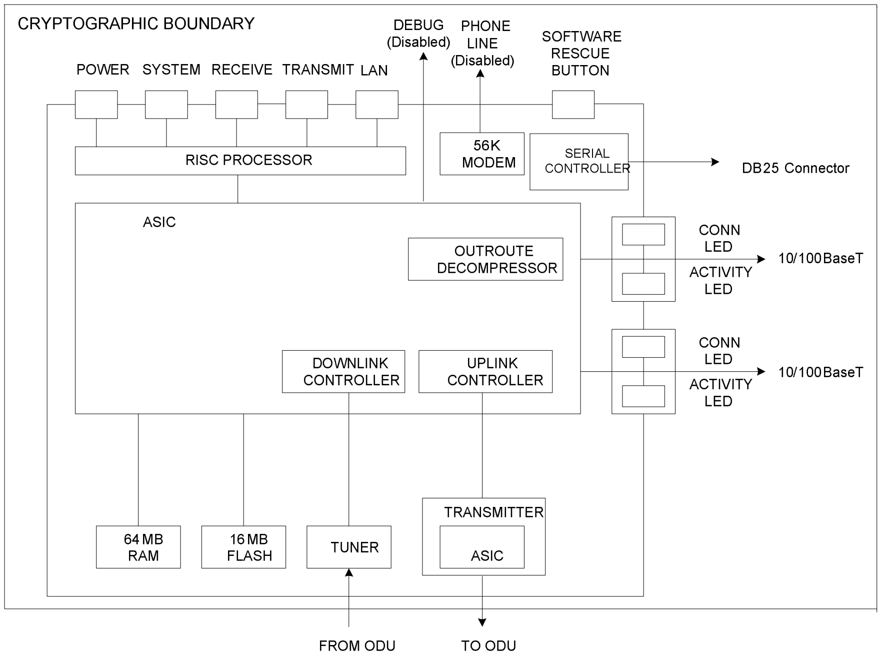

Figure 3 – Hughes VSAT Satellite Router Physical Block Diagram

The module's physical cryptographic boundary on the VSAT appliance is defined by the appliance's metal case, which physically encloses the complete set of hardware and firmware, including the operating system and the module. The module supports the following physical ports: Local Area Network (LAN), telephone, serial, power, and satellite in/out ports (see Figure 3).

The module is entirely encapsulated by the logical cryptographic boundary as shown in Figure 4. The module's logical cryptographic boundary is shown by the broken-line block marked "HUGHES Crypto Kernel". Notice that in this figure, CCI stands for Common Cryptographic Interface and GMP is the GNU Multiple Precision arithmetic library.

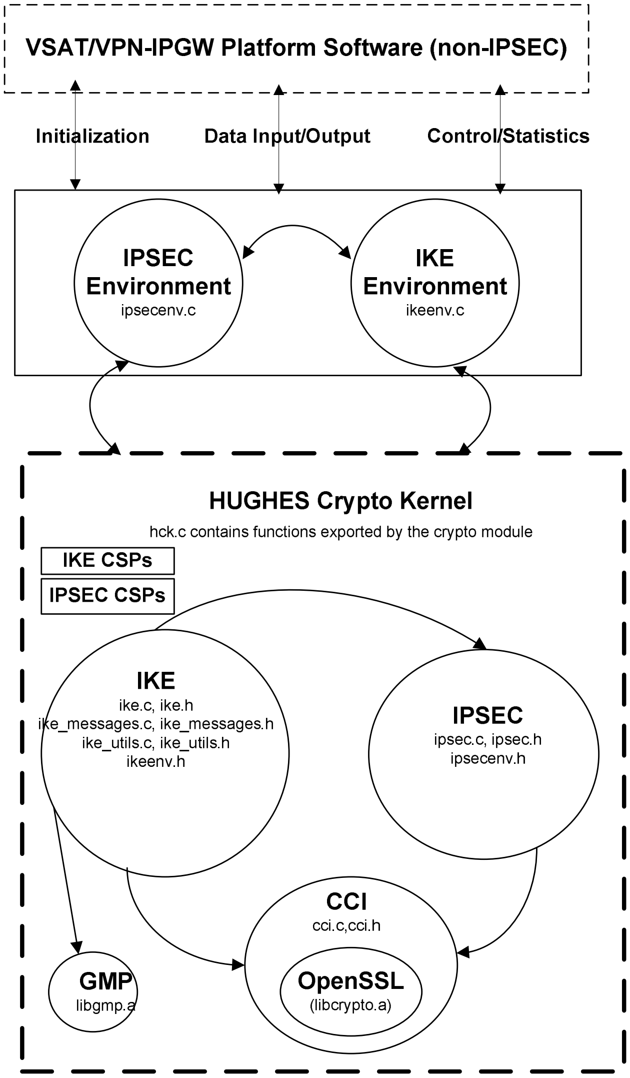

Figure 4 – Logical Cryptographic Boundary

The Hughes Crypto Kernel is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level (Software)	Level (Firmware)
1	Cryptographic Module Specification	1	1

Section	Section Title	Level (Software)	Level (Firmware)
2	Cryptographic Module Ports and Interfaces	1	1
3	Roles, Services, and Authentication	1	1
4	Finite State Model	1	1
5	Physical Security	N/A	1
6	Operational Environment	1	N/A
7	Cryptographic Key Management	1	1
8	Electromagnetic Interference (EMI)/ Electromagnetic Compatibility (EMC)	1	1
9	Self-tests	1	1
10	Design Assurance	1	1
11	Mitigation of Other Attacks	N/A	N/A

2.3 Module Interfaces

The functional module interface exists in the software/firmware. Physically, ports are considered to be those of the enclosure. The module provides Application Programming Interface (API) functions to interact with the components. Both the APIs and physical ports can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out Interface
- Data Control Interface
- Status Output Interface
- Power Interface

These logical interfaces (as defined by FIPS 140-2) map to the module's physical interfaces, as described in the following tables. The Debug port of the VSAT platform is disabled by not being linked to the firmware.

Table 2 – FIPS 140-2 Logical Interfaces (GPC Platform)

FIPS 140-2 Logical Interface	Hughes Crypto Kernel Interface	Physical Port
Data Input	Function input variables. It provides APIs to interact with the module.	Network port
Data Output	The API to the HCK library is the interface for data output. The data output can be in the form of function output variables or return values.	Network port
Control Input	The API to the HCK library provides control input to the module in the form of parameters to function calls.	Network port, serial port, keyboard port, mouse port, PC power button
Status Output	Certain function calls and return values for function calls are the interfaces for status output.	Light Emitting Diode (LED)s, Display monitor port, network port
Power	Not applicable	Power interface

Table 3 – FIPS 140-2 Logical Interfaces (VSAT Platform)

FIPS 140-2 Logical Interface	Hughes Crypto Kernel Interface	Physical Port
Data Input	Function input variables. It provides APIs to interact with the module.	Satellite port
Data Output	The API to the HCK library is the interface for data output. The data output can be in the form of function input/output variables or return values.	Satellite port
Control Input	The API to the HCK library provides control input to the module in the form of parameters to function calls.	Network port, serial port, power interface, telephone port
Status Output	Certain function calls and return values for function calls are the interfaces for status output.	Network port, serial port
Power	Not applicable	Power interface
--	Not applicable	Debug port

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 operator of the module must assume either of the roles based on the service being executed without any authentication.

When running on the Windows Server 2003 platform, operator spaces on the module are separated by the OS. The OS must be configured for single user mode in FIPS-approved mode of operation. See Section 3.2.1 of this document for details.

Both of the operator roles and their associated responsibilities are described below.

2.4.1 Crypto-Officer Role

The Crypto-Officer is expected to install and configure the module in the FIPS mode of operation. Please see Section 3, Secure Operation, for a complete list of the Crypto-Officer's responsibilities. Descriptions of the services available to the Crypto-Officer role, including the inputs, outputs, and Critical Security Parameters (CSPs), are provided in the table below.

Table 4 – Mapping of Crypto-Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP, Keys, and Type of Access
Installation	Installing the software /firmware module	Command	Result of installation	None
Uninstall	Uninstall the software/firmware module	Command	Module uninstalled	All CSPs – Delete
hck_init	Validates input parameters before performing power-on self-tests; Initializes configuration	Module configuration, module statistics, crypto environment functions	Parameter validation status indicator	Integrity Test Key – Read
hck_zeroize_csp	Zeroizes all CSPs except for the integrity test key	CSP to be zeroized, CSP type	Zeroization status	AES Key, HMAC Key, Diffie-Hellman Key – Zeroize

Service	Description	Input	Output	CSP, Keys, and Type of Access
hck_shutdown	Shuts down all crypto functionality	API call	None	AES Key, HMAC Key, Diffie-Hellman Key – Delete
hck_do_self_tests	Performs power-on self-tests	API call	Self-test status indicator	Integrity Test Key – Read
hck_get_status	Retrieves the crypto module status	API call	Crypto module status information	None
hck_get_name_and_version	Retrieves the module name and version number	API call	None	None
hck_get_version	Retrieves the module's major and minor version numbers	API call	None	None
hck_get_fips_mode	Determines whether or not FIPS mode has been enabled	API call	Mode indicator	None
hck_print_status	Prints module status variables and statistics to a display or log file	API call	none	None
hck_update_parms	Sets configuration parameters based on module's current mode of operation	API call	Module status indicator	AES Key, HMAC Key, Diffie-Hellman Key – Write, Read, Overwrite

2.4.2 User Role

While operating in the FIPS approved mode of operation, the User will be able to utilize the encryption and authentication functionality of the module. Descriptions of the services available to the User role are provided in the table below.

Table 5 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
hck_process_ike_event	Ensures that crypto module is active and validates input parameters before processing a received IKE packet or provides a timer event to the IKE state machine	IKE event, IKE peer	Validation status indicator	AES Key, HMAC Key, Diffie-Hellman Key – Read
hck_process_tx_pkt	Ensures that crypto module is active and validates input parameters before processing IPsec transmission packet	IPSec peer, ESP packet, number of bytes to add to ESP packet, authentication algorithm	Validation status indicator	AES Key, HMAC Key, Diffie-Hellman Key – Write, Read, Delete

Service	Description	Input	Output	CSP and Type of Access
hck_process_rx_pkt	Ensures that crypto module is active and validates input parameters before processing IPsec received packet	IPSec peer, ESP packet, ESP sequence number replay check indicator, authentication algorithm, IP header validation mode	Validation status indicator	AES Key, HMAC Key, Diffie-Hellman Key – Write, Read, Delete
hck_send_ike_msg	Ensures that crypto module is active and validates input parameters before invoking IKE transmit function	IKE message type, IKE peer message recipient	Validation status indicator	AES Key, HMAC Key, Diffie-Hellman Key – Read

2.5 Physical Security

When the module is running on Windows Server 2003, the physical security requirements do not apply to the module since it is software and does not implement any physical security mechanisms.

When the module is running on VxWorks 5.4 within the Hughes VSAT satellite router, it is firmware and the physical security requirements apply. The Hughes VSAT satellite router is a production-grade embodiment that includes a removable plastic case, which completely surrounds the module.

Both FIPS 140-2 test platforms (see Section 2.2) 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

When the module is running on VxWorks 5.4 within the Hughes VSAT satellite router, it is firmware. The operational environment requirements do not apply since VxWorks 5.4 within the Hughes VSAT satellite router is a non-modifiable operating system.

When the module is running on Windows Server 2003, it is software and the operational environment requirements apply. The module is installed as a shared library in its compiled form, hkc.dll. The operating system must be configured for single user mode per CMVP guidance for FIPS 140-2 compliance. All keys, intermediate values, and other CSPs remain in the process space of a single operator. The operating systems protect memory and process space from unauthorized access.

2.7 Cryptographic Key Management

The module implements the following FIPS-approved algorithms:

- AES - Cipher Block Chaining mode (AES CBC) – FIPS 197 (Certificate #616)
- SHA-1 (Byte-Oriented) – FIPS 180-2 (Certificate #664)
- HMAC-SHA-1 – FIPS 198 (Certificate #319)
- Digital Signature Algorithm (DSA) – 1024 bits, FIPS 186-2 (Certificate #239) for integrity test.
- Pseudo Random Number Generator (PRNG) – American National Standards Institute (ANSI) X9.31 Appendix A.2.4 with 128-bit AES (Certificate #351)

The module also implements the following non-FIPS approved algorithm:

- Diffie-Hellman – 1024-bit key agreement and key establishment providing 80 bits of encryption strength.

The module supports the following critical security parameters:

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

Key	Key Type	Generation / Input	Storage	Use
AES Key	128-bit AES CBC symmetric key	Generated using ANSI X9.31 PRNG	Plaintext in Random Access Memory (RAM)	Encrypt or decrypt IPsec Encapsulating Security Payload (ESP) packets
HMAC Key	160-bit HMAC key	Generated using ANSI X9.31 PRNG	Plaintext in RAM	Authenticate IPsec ESP packets
Diffie-Hellman key pair	1024-bit Diffie-Hellman keys	Generated using ANSI X9.31 PRNG	Plaintext in RAM	Establish key pairs for internet key exchange
Integrity Test Key	1024-bit DSA public key	Externally generated, hard coded in the module	Stored in hard-drive in plaintext with compiled software	Software/firmware integrity test
PRNG Seed	128-bit seed	Continually polled from various system resources to accrue entropy	Plaintext in RAM	Random number generation
PRNG Seed Key	128-bit seed key	Continually polled from various system resources to accrue entropy	Plaintext in RAM	Random number generation

All keys generated by the module are generated internally using a FIPS-approved PRNG, ANSI X9.31 Appendix A.2.4 PRNG. CSPs are never output from the module. All keys except the integrity test key are zeroized when the module enters an error state, upon reboot, or if the operator calls the hck_zeroize_csp function. The Integrity Test Key, which is a DSA public key used to verify the signature on the software/firmware image, is zeroized when the module is uninstalled. The PRNG seed is zeroized when new seed is generated. The zeroization of the CSPs is carried out by overwriting the storage area or memory location with zeros.

2.8 Self-Tests

The module is started by the application calling the hck_init function. Power-up self tests are executed automatically when hck_init is called. If these self-tests fail, then the module enters an error state and prevents all cryptographic processing and functionality. The Hughes Crypto Kernel performs the following power-up self-tests:

- Software/Firmware integrity test using a DSA public key
- Known Answer Tests (KATs)
  - AES KAT (encryption and decryption)
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - ANSI X9.31 PRNG KAT

In addition, the module performs a conditional PRNG self-test to ensure that the 128-bit random result is not equivalent to the previous result.

2.9 Mitigation of Other Attacks

The module does not mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

3 Secure Operation

The Hughes Crypto Kernel meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The Crypto-Officer role is responsible for ensuring that the module is installed on a platform as indicated in Section 2.2 of this document. The HCK implements a software/firmware integrity test that consists of a DSA signature computed over the image that comprises the library. During the power-up self-tests phase, the signature is verified over the stored HCK instance. If the stored signature is verified, then the test is passed. Otherwise, the test is failed and the module enters an error state where no cryptographic functionality is allowed.

3.2 Crypto-Officer Guidance

The Crypto-Officer is responsible for initialization, monitoring, and shutdown of the module.

3.2.1 Initialization

The Crypto-Officer role is responsible for ensuring that the module is operating in the FIPS approved mode of operation. The FIPS mode of the module is enabled through a parameter (*boolean fips_mode*, which must be set to True) passed to function hck_init. Notice that hck_init has to be called by the application (the VPN IP gateway software on Windows or the firmware on Hughes VSAT satellite router) first before other functions of the module are called. If a function is called without first calling hck_init, then the module will return a fatal error and be unloaded. A call to function hck_get_fips_mode will return a Boolean value showing the current FIPS mode setting of the module.

The functions exported by the module are not directly accessible by a Crypto-Officer. Instead, the API functions are invoked by the application using the module. On Windows Server 2003, the Crypto-Officer can place the module in the FIPS mode by configuring proper settings in the application. Please refer to the installation manuals of individual applications for details.

For the VSAT satellite router, the FIPS mode configuration is performed by Hughes in factory and cannot be changed by end-users. Before purchasing the VSAT router, the Crypto-Officer must request that the product be configured to the FIPS mode. To verify the VSAT router is indeed working in the FIPS mode, the Crypto-Officer should check the “HCK Stats” tag under the “IPSec/IKE” menu in the web browser interface and ensure that FIPS mode is indicated as “Enabled” under “HCK Status”.

When operated in the FIPS mode, on startup, the KATs and Integrity Test are executed before any cryptographic services are offered by the module. If any of the tests fail, then the module will be placed in an error state, and no crypto services are offered.

FIPS 140-2 mandates that a software cryptographic module at Security Level 1 shall be restricted to a single operator mode of operation. Prior to installing the module, the Crypto-Officer must ensure the GPC is actually running Windows Server 2003. To configure Windows Server 2003 for single user mode, the Crypto-Officer must ensure that all remote guest accounts are disabled in order to ensure that only one human operator can log into the Windows OS at a time. The services that need to be turned off for Windows are:

- Fast-user switching (irrelevant if server is a domain member)
- Terminal services
- Remote registry service
- Secondary logon service
- Telnet service
- Remote desktop and remote assistance service

On a Hughes VSAT satellite router running VxWorks 5.4, the module is installed as part of the firmware image. The Crypto-Officer is responsible for verifying the version of the module on the VSAT router before use. This can be done by accessing the router via a web browser and checking the “HCK About” tag under “IPsec/IKE”.

3.2.2 Management

The Crypto-Officer should monitor the module’s status regularly. If any irregular activity is noticed or the module is consistently reporting errors, then Hughes Network Systems customer support should be contacted.

3.2.3 Zeroization

All keys except the Integrity Test Key are zeroized when the module enters an error state, upon reboot, or if the Crypto-Officer calls the hck_zeroize_csp function. The Integrity Test Key, which is a DSA public key used to verify the signature on the software/firmware image, is zeroized when the module is uninstalled. See Section 2.7 of this document for details.

3.3 User Guidance

Only the module’s cryptographic functionalities are available to the User. 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 noticed.

The User must not modify the configuration of the module as established by the Crypto-Officer.

Acronyms

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CCI	Common Cryptographic Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GMP	GNU Multiple Precision
GPC	General Purpose Computer
GUI	Graphical User Interface
HCK	Hughes Crypto Kernel
HMAC	(Keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
SHA	Secure Hash Algorithm
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal