FIPS 140-2 SECURITY POLICY

RIDEWAY STATION FGC
Version: 5.0
FIPS Security Level: 2

Making Internet Security Easy

Table of Contents

1. Introduction

This security policy is a specification of the security rules under which RideWay Station FGC operates. This policy includes the security rules derived from the FIPS 140-2 standard requirements for Security Level 2 as well as additional security rules implemented by the ITServ. More specifically, this policy describes 1) the roles and services performed by the RideWay Station, 2) the physical security mechanisms implemented to protect RideWay Station and the actions to be taken to ensure that security is maintained, and 3) the security mechanisms implemented to mitigate attacks.

2. Purpose

There are two major reasons for developing and following a precise cryptographic module security policy:

- To provide a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, satisfies a stated security policy.
- To describe to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

3. Overview

RideWay Station is an integrated firewall, virtual private network (VPN) and IP-sharing appliance. It safeguards a computer network from outside intruders and attacks as well as allows secure remote access to the network and enables multiple offices to create a secure private network.

3.1. Cryptographic Module Definition

The cryptographic module consists of firmware that performs Network Address Translation (NAT), Firewall, and Virtual Private Networking (VPN). The firmware is stored in DRAM and flash memory disk, called the Disk on Module (DOM). The module works as a VPN as well as a Gateway device. The binary is stored on a DOM and includes a Linux kernel and other application level programs such as DHCP server and DNS server.

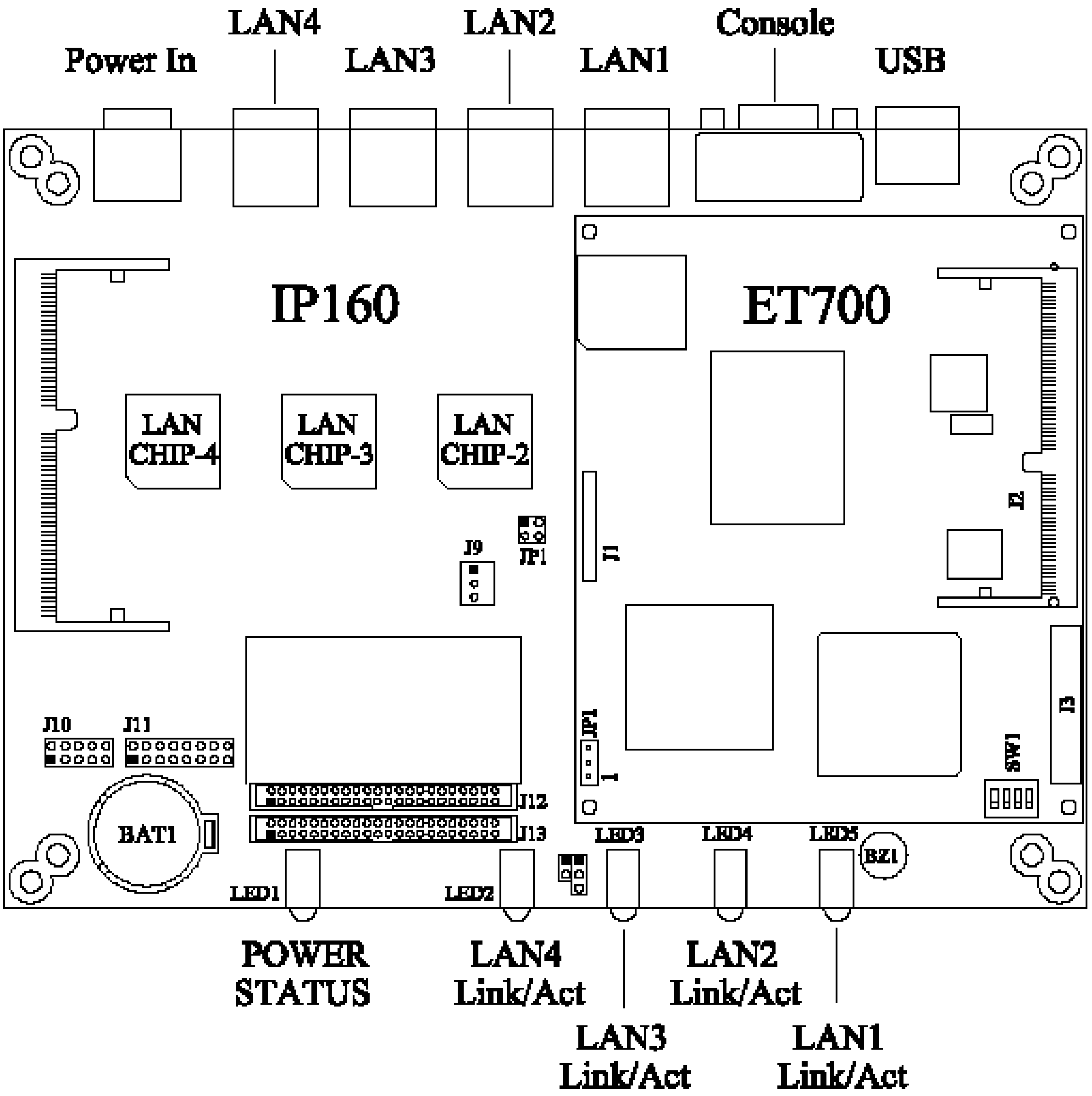
The cryptographic module contains the RideWay Station firmware and a copy of the Linux operating system. The firmware resides on the Disk-on-Module contained in the module and is protected via password-based authentication.

3.2. Hardware Description

The hardware cryptographic boundary consists of a physical enclosure, which is an aluminum box, with four Ethernet connectors, one console port connector, one USB port and a power cable for the DC input power supply.

Component Description

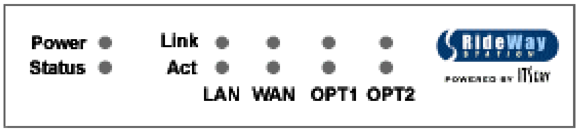
- Flash Memory Disk: program memory
- On-board Memory: the run-time memory for data and code execution
- CPU: Intel x86-based processor
- Ethernet Ports: LAN1 (OPT1 – used for DMZ), LAN2 (WAN), LAN 3 (LAN), LAN 4 (OPT2 - not used)
- Console Port: another port used for dial-up and administration connection
- USB Port: not being used



Hardware Diagram

RideWay Station has the following status indicator LEDs on its front panel:

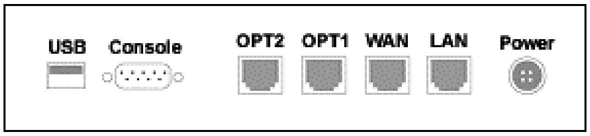
- Power LED: illuminates when RideWay Station is powered-on
- Status LED: illuminates once the RideWay Station successfully boots up.
- Link LED: indicates that the port is connected at 100 Mbps
    - LAN
    - WAN
    - OPT1 (DMZ)
    - OPT2 (not used)
- Act LED: indicates that packets are traversing through the port
    - LAN
    - WAN
    - OPT1 (DMZ)
    - OPT2 (not used)



RideWay Station Front Panel

RideWay Station has the following ports:

- USB: does not currently serve any functions relating to the cryptographic module. It is disabled by the firmware.
- Console: provides modem connection for dial-up users and administrative tasks.
- OPT2: does not currently serve any functions relating to the cryptographic module. It is disabled by the firmware.
- OPT1: provides the Ethernet connection for the De-militarized zone
- WAN: provides the Ethernet connection to the broadband/Internet network
- LAN: provides the Ethernet connection to the private network
- DC + 5V 4A: power plug. All power entering the cryptographic module must pass through this interface.



RideWay Station Rear Panel

4. Roles

The RideWay Station supports two roles:

- User: each user in this role must be set up by the crypto officer
- Crypto Officer: this is the general administration role of RideWay Station

4.1. User

A user can be identified as one of the following:

- Any person coming in through a host (standalone or as part of a remote network) that has an IPSec connection with the local network.
- Any person on the local network communicating with a host (standalone or as part of a remote network) that has an IPSec connection with the local network.

All authentication of users on the network is role-based. When a person logs into a PC that is on the network, that person is considered a user of the cryptographic module. If the communication is network to network (or LAN-to-LAN), the entire remote network can be considered a user.

Complementing policies must be created in both the remote host or network and the cryptographic module. Each endpoint must have the correct public and private IP address information of the other endpoint. In addition, each endpoint must agree on a pre-shared key (or password) that the cryptographic module will compare when the connection is established. For LAN-to-LAN connections, once the connection is up, if no other external authentication mechanisms are established, any user in the local and remote networks may use the tunnel to communicate.

To be in FIPS mode, the operator must access the network through an IPSec connection. The remote network and local network must be securely connected by an IPSec tunnel. In a LAN-to-LAN scenario, IPSec policies are set up by the administrators of the local and remote endpoints. Once the connection is up, if no other external authentication mechanisms are established, any user in the local and remote networks may use the tunnel to communicate. In a remote client to LAN scenario, the remote client policy is set up by the crypto-officer. The remote end connection is initiated by the user.

4.2. Crypto Officer

The crypto officer accesses RideWay Station's web-based configuration and management interface, known as the Control Center. The default (initial) username and password is "apadmin" and "ap/admin", respectively. The password can be and should be changed after the first login.

The crypto officer is able to perform cryptographic services such as set up IPSec policies and configure the module in FIPS-approved mode.

4.3. Maintenance

In FIPS-approved mode, maintenance can only be performed by an authorized ITServ technician. When the hardware malfunctions (e.g., the Ethernet port is not working), the unit can be returned to the factory for repair.

No maintenance interface or role exists in FIPS-approved mode.

4.4. Authentication

The following table details the roles supported by the RideWay Station and the authentication mechanism required for each role:

Role	Authentication Type	Authentication Data	Strength of Authentication
User	Role-based	Tunnel ID and pre-shared key	The pre-shared key has a minimum size of six characters. The characters must be alphanumeric and therefore can be 1 of 62 characters. Thus the probability of guessing the key is (1/62)^6, or 1 in 66800235584.
Crypto Officer	Role-based	Username and password	The password is obfuscated with CRYPT(3). Each digit can be 1 of 62 characters, and there are 6 digits minimum. Thus the probability of guessing the password is (1/62)^6, or 1 in 66800235584.

5. FIPS-Approved Mode of Operation

In the Approved mode of operation, the cryptographic module only uses the following cryptographic algorithms:

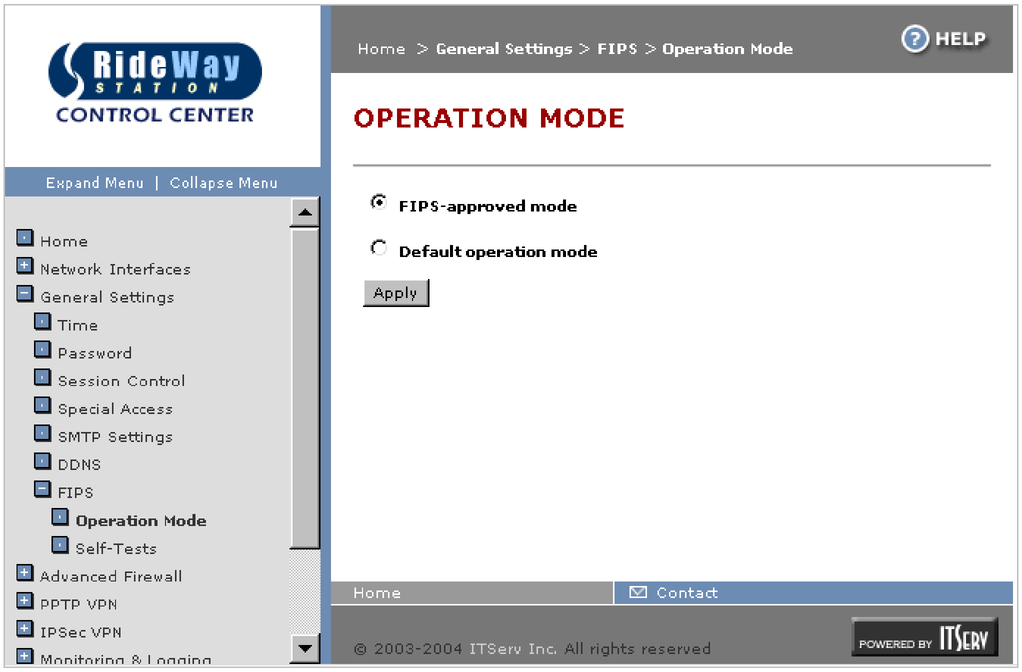
- Triple-DES: Certificate #247
- HMAC-SHA-1: Vendor affirmed, SHA-1 Certificate #186

In the RideWay Station Control Center, the Crypto-Officer is given the choice to perform non-Approved and Approved algorithms.

To invoke the Approved mode of operation in RideWay Station, the crypto-officer shall perform the following tasks:

- Login to the RideWay Station Control Center web page
- Select General Settings -> FIPS -> Operation Mode from the navigation bar.
- The Operation Mode page is displayed as in the figure below.

- Select "FIPS-approved mode" and click "Apply".



OPERATION MODE

● FIPS-approved mode

○ Default operation mode

RideWay Station Control Center

In FIPS-approved mode, the system disallows the following services:

- Initiate PPTP tunnel
- Transfer information through a PPTP tunnel (in other words, if a PPTP tunnel is active when the security mode is changed to FIPS-approved only mode, the tunnel will be deactivated)
- Running user services while crypto-officer service is occurring

6. Services

The following table lists the services provided by the module.

Service	Description
Transfer information through an IPSec tunnel (encryption/decryption)	Securely transfers information between the network and a remote network or client.
Initiate IPSec tunnel (authentication/key agreement)	Sets up the tunnel through which data will be securely transferred.
Manage IPSec policy	Sets up the parameters of an IPSec policy
Change Control Center Password	Change the password for logging in to the Control Center
Configure network settings	To configure the RideWay Station to operate in the network either by modifying individual settings or importing configurations from a local file.
Run self-tests	The module runs self-tests at power-up time and when algorithms are to be used to ensure that the algorithms are properly functioning. Self-tests can also be run manually.
Upgrade module	A key is entered into the module by the crypto-officer to activate options or add more user or VPN licenses.

Firmware update	The crypto-officer may download updates and patches to the firmware. Only affected objects are modified. Module requires a reboot after downloading new firmware. Firmware is protected by HMAC-SHA-1.
Factory reset	The module's configurations can be reset to the factory defaults by connecting a PC to the module via a console cable. The crypto-officer can then use the hyperterminal on the PC to reset the module.
Reboot the module	The crypto-officer can reboot the module from the Control Center.
Import/export configurations	The crypto-officer can export the module's configurations to a network location. The file will be obfuscated using a password inputted by the crypto-officer. Subsequently, the crypto-officer can import the configurations back into the module.

The following table lists the services that can be performed in each role.

Role	Service
User	Transfer information through an IPSec tunnel (encryption/decryption) Initiate IPSec tunnel (authentication/key agreement)
Crypto Officer	Manage IPSec tunnels (authentication/key agreement) Change Control Center Password Configure network settings Run self-tests Upgrade module Firmware update Factory reset Reboot the module Import/export configurations

In order for an IPSec tunnel to be created, both the local and remote location must set up corresponding IPSec policies in their respective RideWay Stations. The pre-shared keys in the local and remote policies must match in order for the tunnel to be activated.

RideWay Station also has an Access Control feature that allows the Crypto Officer to set access rules on top of RideWay Station's default Access Control Policy.

The following table lists the cryptographic keys used in each service and the type of access granted for each service.

Service	Cryptographic Keys, CSPs	Type(s) of Access
Transfer information through an IPSec tunnel (encryption/decryption)	IPSec session key	Read/Execute
Initiate IPSec tunnel (authentication/key agreement)	IPSec pre-shared key	Read
Manage IPSec tunnel (authentication/key agreement)	IPSec pre-shared key	Read/Write/Execute
Password Management	Crypto-officer key	Write
Configure network settings	None	N/A
Reset RideWay Station	None	N/A
Run self-tests	None	N/A
Upgrade module	Upgrade key	Read/Execute
Firmware update	None	N/A
Import configurations	Password	Read
Export configurations	Password	Write/Execute

7. Cryptographic Key Management

The cryptographic module employs the following FIPS-approved algorithms:

- Triple-DES
- HMAC-SHA-1
- SHA-1

The cryptographic module also employs the following non-FIPS-approved algorithms:

- RC4
- MD5
- Diffie-Hellman (key agreement)
- Crypt(3)

The following table describes the cryptographic keys used by the cryptographic module:

Key	Key Type	Generation	Storage	Use
IPSec pre-shared key	IKE pre-shared key	Created by the crypto officer through the management interface.	DOM	IKE authentication when an IPSec connection request is received.
IPSec session key	3DES (168-bit)	Negotiated during the IKE.	RAM	Secures IPSec traffic by encrypting and decrypting IPSec packets.
Import/export password	Non-FIPS approved algorithm	Created by the crypto officer through the management interface.	Not stored	Used to obfuscate configuration file during export and decrypt during import.

When an IPSec tunnel has been created, the system uses the IKE protocol to continually renegotiate the session key. Any data that is transferred in the IPSec tunnel is encrypted using 3DES encryption. The three key 3DES has 3 * 56 = 168 bits of key. However, against a "meet in the middle" attack, the key strength is equivalent to 112 bits.

The random number generator (RNG) used to generate the IPSec session keys is based on the requirements of ANSI X9.31 A.2.4. The ANSI X9.31 does not use a key but uses a seed (date and time) to create a random number to use in the Diffie-Hellman algorithm.

When exporting a configuration file, the crypto officer enters a password that is used to obfuscate the file itself. When the crypto officer imports the file back into the module, the password must be entered in order to decrypt the file. The password is never stored.

The cryptographic module utilizes a RAM-based disk interface to store all plaintext secrets. They are wiped out once the module is restarted. Session keys are zeroized by the IPSec module when they expire. The crypto-officer can zero out the pre-shared keys using the management interface. The module zeroizes the keys by overwriting the keys with zeroes.

The zeroization technique used by the cryptographic module for session keys is through the RAM-based disk interface, which can be wiped out completely in a very short period of time. The time it needs is not sufficient to compromise any plaintext pre-shared keys or any session keys. The zeroization technique used by the cryptographic module for the session keys works as such: when a key expires, the IPSec module removes it immediately. When the IPSec tunnel is not active or is disabled, no session keys exist. The pre-shared keys are zeroized when the crypto-officer zeroes them.

When the power to the module is turned off, all keys are zeroized automatically.

8. Self-Tests

The cryptographic module performs both power-up and conditional self-tests. Tests can also be manually initiated by an operator.

8.1. Power-Up Tests

When RideWay Station is first powered on, the system performs the following tests to ensure that the cryptographic module will function correctly:

- Standard power-up self-test
- Basic Input-Output System (BIOS) test
- Linux Operating System boot test
- Known answer test (w/ 3DES cryptographic algorithm test, HMAC-SHA-1, and RNG test)
- Software/firmware integrity test
- Critical functions test

The critical functions test includes the following tests:

- Licensing and model information function test: ensures that the environment of the cryptographic module is operating correctly.
- Key storage function test: ensures the integrity of any cryptographic key.

The following tests may be manually run by an operator:

- Known answer test (w/ 3DES cryptographic algorithm tests, HMAC-SHA-1, and RNG test)
- Continuous random number generation test
- Software/firmware load test
- Key storage integrity test

8.2. Conditional Tests

A continuous random number generation test is performed whenever a random number is generated by the ANSI x9.31 pseudo-random number generator, during module initialization and prior to cryptographic processing.

Whenever firmware patches are loaded onto the module, the system performs a software/firmware load test to verify the integrity of the firmware patch.

9. Physical Security Policy

If an error occurs on the power-up or during a self-test, the status LED will not illuminate. The Act LEDs will not illuminate because no traffic will be allowed to pass through.

There are no doors or buttons on the interface of the box.

The rear panel is connected to the rest of the shell by four screws. A vendor-supplied tamper-evident seal is placed on the rear panel such that if it is ever removed, the seal will be damaged.

10. Mitigation of Other Attacks Policy

This section specifies the security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

Potential attacks include:

- Denial-of-Service (DoS) attacks
- Port scanning
- Unauthorized access

RideWay Station has a built-in capability to monitor the incoming and outgoing traffic. It is able to detect and block the following DoS attacks from the Internet:

Other Attacks	Mitigation Mechanisms	Specific Limitations
DoS attacks: • Ping of Death • SYN Flood • IP Spoofing • Teardrop • LAN Attack	Monitors packets and detects attacks. When attacks are detected, packets associated with the attack are blocked.	None

The RideWay Station also protects the private local area network by blocking any unauthorized access into the LAN. The RideWay Station does not open any port or relay any access to those ports (other than PPTP Port 1723). Therefore, all unauthorized and illegal Internet accesses are stopped outside the private network.

As mentioned earlier, RideWay Station's Advanced Access Control feature enables the Crypto Officer to place further security measures on the RideWay Station. RideWay Station does not allow its default access control policy to be relaxed so the Crypto Officer does not need to worry about inadvertently opening up a vulnerability for attack.

If the Crypto Officer enables the logging mechanism, RideWay Station is able to log all accepted and blocked packets going to and from the LAN, Internet, DMZ, and VPN zones.

11. Acronyms

3DES	Triple Data Encryption Standard
CSP	Critical Security Parameter
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DNS	Domain Name Service
DoS	Denial of Service
DOM	Disk-on-Module
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
LAN	Local Area Network
LED	Light-Emitting Diode
NAT	Network Address Translation
PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
RNG	Random Number Generator
SHA-1	Secure Hash Algorithm
VPN	Virtual Private Networking
WAN	Wide Area Network