RedCreek Personal Ravlin Cryptographic Module Security Policy for the Federal Information Processing Standards Publication (FIPS Pub) 140-1

1.0 Introduction

1.1 Purpose

This Cryptographic Module Security Policy is for the FIPS 140-1 Level 2 certification of the RedCreek Personal Ravlin. The Personal Ravlin is an Internet Engineering Task Force (IETF) IP Security (IPSec) Standard based product that enables secure data communications. This security policy describes how the Personal Ravlin meets the FIPS 140-1 Level 2 requirements and how it can be securely operated.

1.2 References

Additional information regarding the RedCreek suite of network security solutions for data communications can be found at the http://www.redcreek.com web site.

Additional information regarding the IETF IPSec standard for encryption, authentication, key management, ad anti-replay services can be found at the http://ww.ietf.org web site.

Additional information regarding the Security Requirements for Cryptographic Modules, FIPS 140-1, can be found at the http://csrc.nist.gov/cryptval web site.

2.0 Personal Ravlin Description

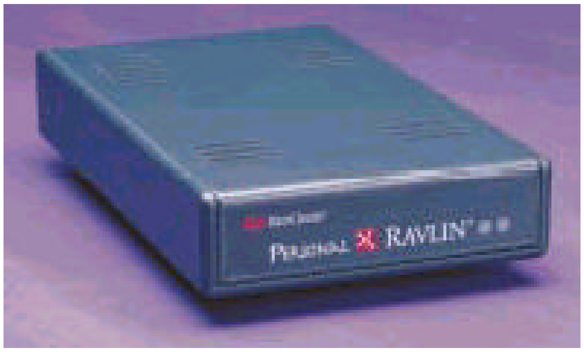


Figure 1 – Personal Ravlin Front View

The RedCreek Personal Ravlin, shown in Figure 1, is a cost-effective network security solution that performs encryption and decryption with a throughput of 4 Mbps. The Personal Ravlin provides data privacy using industry standard 40-bit/56-bit Data Encryption Standard (DES) and 168-bit Triple DES encryption. Authentication and access control are provided using the Digital Signature Standard (DSS), Secure Hash Algorithm (SHA1), Diffie-Hellman key exchange, X.509 v.3 digital certificates, and ISAKMP/Oakley key management. ISAKMP is defined as Internet Security Association and Key Management Protocol in the IPSec standards. The Personal Ravlin maintains the 4 Mbps throughput through the use of the RedCreek CryptoCore™ technology.

2.1 Cryptographic Module

The Personal Ravlin is composed of a printed circuit (PC) board in a sealed plastic case. The unit weight is 5.9 oz, and the dimensions are 1" H x 6" D x 4" W. The amber and green front panel indicator LEDs provides helpful information regarding the status of the Personal Ravlin. The power and two Ethernet connectors are mounted on the printed circuit board, and are accessible through the back panel. A permanent printed label with the unit's unique characteristics is attached to the bottom of the unit: the Ethernet MAC (media access control) hardware address and the security identification number (or Security ID).

The Security ID is a representation of the unit's DSA public/private key pair. The unit's DSA X.509 v.3 digital certificate's distinguished name would be its Security ID. The RedCreek Certificate Authority (CA) signs the digital certificate as part of the unit's manufacturing process. The unit's DSA key pair, the unit's digital certificate, and the RedCreek CA public key are stored in flash memory. The CryptoCore™ is a multi-chip implementation of a DES engine and a random number generator.

2.2 Module interfaces

The module has two 10BaseT Ethernet ports. Logically, the module has the following interfaces:

Local Port
Remote Port
Configuration: Network

The Local and Remote Ports are for sending and receiving Ethernet packets, and serve as the unit's data input and data output interfaces. If the received Ethernet packets are addressed specifically to the Ravlin unit, then they are forwarded to the Network Port. Module interface Level 2 requirements permit the sharing of the ports for data input/output and for critical security parameters. The control-input interface is the Network Port. The status output interface is the Network Port, while the amber (yellow) and green front panel indicator LEDs provides helpful information regarding the status of the Personal Ravlin. There is a single DC power interface, and no maintenance access interface.

When AC power is applied to the unit, the green and yellow LEDs on the front panel of the Personal Ravlin should flash, and the green LED should remain on.**{**xe "front-panel lights"**}**

REDCREEK
RAVLIN™ 4

Amber	Steady Blink	IP Address Not Set No Secure Associations Established
	Off	IP Address Set No Secure Associations Established
	On	IP Address Set Secure Association(s) Established
	Flicker	Network Activity for All States
Green	On	Power On
	Off	Power Off

2.3 Roles and Services

RedCreek Communications manufactures the Ravlin hardware unit. The manufacturing process initializes the unit's security parameters with specialized manufacturing firmware. The unit's public key pair is generated in the Ravlin unit. The unit's public key is formatted into a X.509 v3 digital certificate, and transferred to and signed by the RedCreek Certificate Authority. The unit's private key, digital certificate, and RedCreek public key are stored in the unit's flash memory. The unit's real time clock, Security ID, Ethernet MAC addresses are initialized, and the password, IP address, subnet mask, and operational mode are assigned default values. The manufacturing firmware is then replaced with the product firmware, which doesn't include the capability to generate new DSA public key pairs.

The Ravlin network administrator or security manager would be referred to as the Crypto Officer in FIPS 140-1 terminology. RedCreek recommends that the network administrator be responsible for receiving and distributing the Ravlin hardware units. The network administrator would then log the incoming unit's Security ID, set the unit's new password, and assign the unit's IP address.

The Crypto Officer would be responsible for assigning the unit's name, password, IP address, and subnet mask, and for setting them up on the network. RedCreek recommends that the password be at least 8 digits (0-9) in length, and can be up to 16 digits. The Crypto Officer would be responsible for setting up which units may establish virtual private network (VPN) security associations (SA) and their modes. The Ravlin product implements role-based authentication, as defined in FIPS 140-1, meets the Level 2 operator authentication requirements.

In IPSec terminology, a security association is established between the Ravlin product and any other Ravlin suite or other IPSec compliant product when information traffic must be exchanged. The traffic between the Ravlin units can be configured to be authenticated or confidential, or both. The security of the traffic is determined by the policy data entries in each Ravlin unit, as configured by the Crypto Officer. The Ravlin product will only allowed the security association if the request is permitted by the configured security policy. The policy data entries include key management information and protocol information. If the security association were allowed, the Ravlin units would authenticate themselves and exchange session keys using the ISAKMP protocol. Thus, the Ravlin units would be considered Users in FIPS 140-1 terminology.

The process of creating of a policy entry consists of three basic steps:

1. **Create at least one entry in the {** XE "Key Management table" **}Key Management table.**

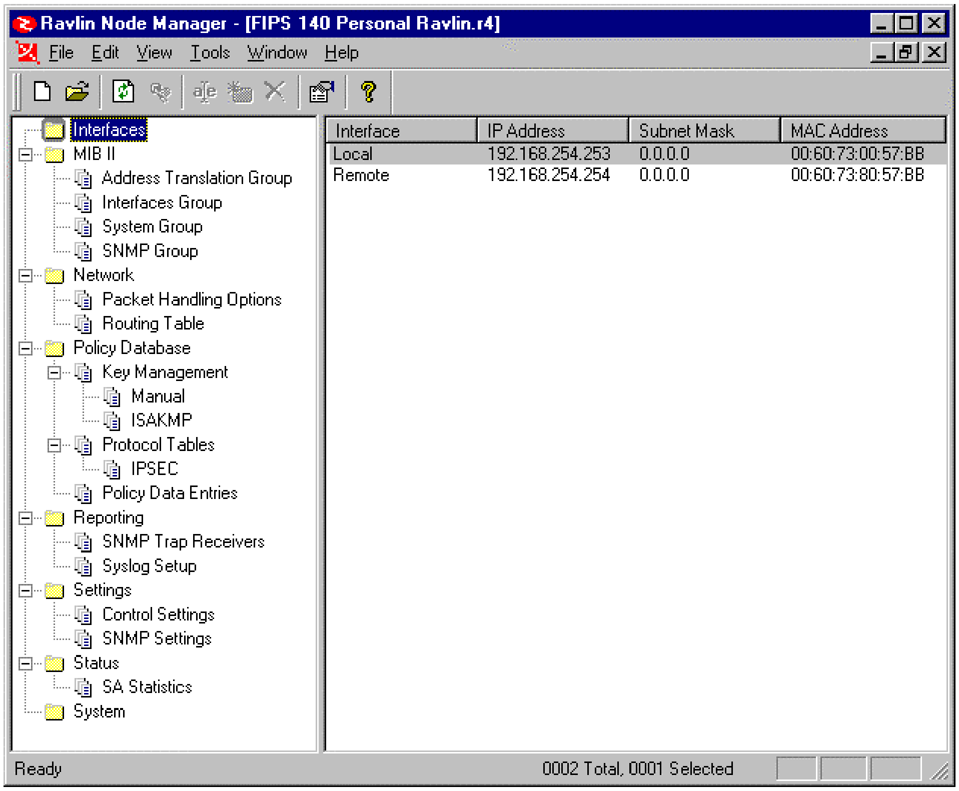
   Each Key Management entry is a profile that describes the kind of key to use when establishing an **{** XE "SA" **}**SA, the type of hashing to use, and the kind of encryption to perform during the SA. An entry in the Key Management table has no *direct* effect when the Ravlin unit builds an SA. It only contains *possible* settings for a policy entry.

2. **Create at least one entry in the {** XE "Protocol table" **}Protocol table.**

   Each Protocol Table entry is a profile that determines which IPSEC protocol to use (Authenticated Headers, Encapsulating Security Payload, or Encryption In Place). As with Key Management table entries, an entry in the Protocol Table has no *direct* effect when the Ravlin unit builds an SA. It only contains *possible* settings for a policy entry.

3. **Create a policy entry in the Policy table. {** XE "Policy table" **}**

   A policy entry is a specification the Ravlin unit uses to build an SA. Because the Ravlin unit can establish and run multiple SAs simultaneously, more than one such entry may be created.



Interface	IP Address	Subnet Mask	MAC Address
Local	192.168.254.253	0.0.0.0	00:60:73:00:57:BB
Remote	192.168.254.254	0.0.0.0	00:60:73:80:57:BB

Ready

0002 Total, 0001 Selected

The Key Management table has two types of subcomponents:

- **{ XE "manual key" }Manual** (to specify a pre-arranged, manual key)
- **ISAKMP** (for generating a session key using ISAKMP and the Diffie-Hellman algorithm).

The Manual Key Information has the following options to support entry of pre-arranged values:

Under **Encryption Key**:

- **Inbound** - The key used for decrypting IP packets received *from* the peer Ravlin unit
- **Outbound** - The key used for encrypting IP packets for transmission *to* the peer Ravlin unit

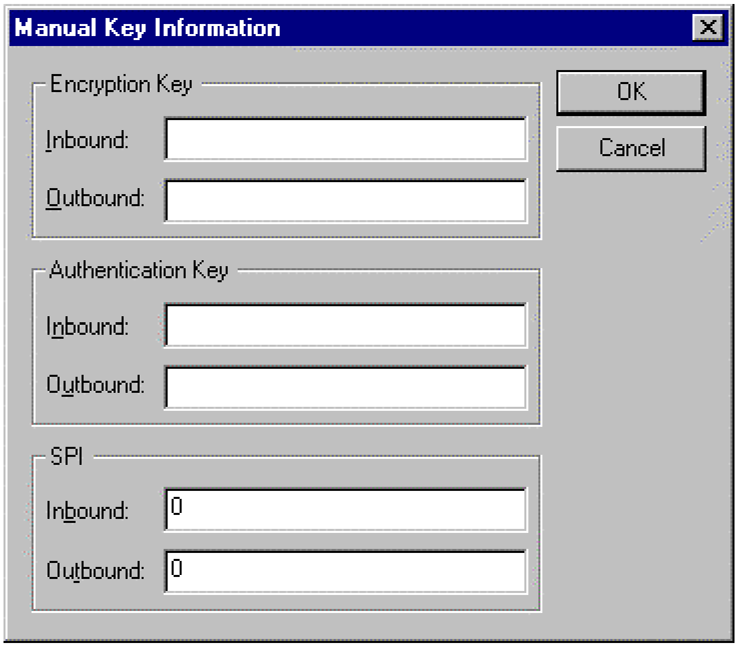
Under **Authentication Key**:

- **Inbound** - The hashing key used for authenticating IP packets received *from* the peer Ravlin unit.
- **Outbound** - The hashing key used for authenticating IP packets sent *to* the peer Ravlin unit.

Under **SPI**:

The **{** XE "SPI" **}**SPI (Security Parameter Index**{** XE "Security Parameter Index" \t "*See* SPI" **}**) is a 32-bit integer value that identifies the SA to which an IP packet belongs. This value resides in the **{** XE "ESP header" **}**ESP header of each packet sent and received by the Ravlin unit.

- **Inbound** - The SPI that identifies the SA for IP packets received *from* the peer Ravlin unit.
- **Outbound** - The SPI that identifies the SA for IP packets sent *to* the peer Ravlin unit.



Encryption Key

Inbound:

Outbound:

Authentication Key

Inbound:

Outbound:

SPI

Inbound: 0

Outbound: 0

The Crypto Officer may configure the following security parameters in the protocol table for security associations:

- While running in the **{** XE "AH" **}{** XE "Authenticated Headers" \t "*See* AH" **}Authentication Headers** (AH) security mode, the Ravlin unit provides integrity and authentication without confidentiality. AH ensures proper authentication by inserting an authentication header in the packet between the IP header and the payload. Because neither the packet's payload nor its IP address is encrypted, AH mode is widely acceptable even where the export, import, or use of encryption is regulated or prohibited.

  While running in the **AH Tunneling** security mode, the Ravlin unit encapsulates the original IP packet and attaches an AH header and a new IP header. As with normal AH mode, no encryption takes place.

- While running in the **{** XE "ESP" **}Encapsulated Security Payload** (ESP) security mode, the Ravlin unit encrypts the entire IP packet, authenticates it, encapsulates it, and gives it a new IP header. When two Ravlin units establish a security association in ESP mode, the communication link between the units is referred to as an *ESP tunnel*. Because ESP tunnel mode encapsulates and encrypts the original IP header along with the payload, intruders cannot capture routing information and use it to attack the system.

  While running in **ESP Transport** security mode, the card encrypts only the payload and ESP trailer. It does not encrypt the source IP address. Because of low overhead, ESP Transport mode usually gives high performance.

- While running in **{** XE "EIP" **}RedCreek Proprietary (EIP)** security mode, the Ravlin unit encrypts the IP packet's payload only, without encrypting the packet header. Because EIP ("Encryption In Place") does not require encryption of the IP header or encapsulation of the IP packet, overhead is lower and performance enhanced.

The Control Settings configuration parameters determine how the Ravlin unit operates in the VPN environment.

ARP Cache Cleanup Interval**{** XE "ARP Cache	Determines if the Ravlin unit performs automatic ARP cache cleanups, and specifies the interval between such

Cleanup" **}**	cleanups.
Operational Mode**{** XE "operational modes" **}**	Specifies the default action to take when the Ravlin unit detects an IP packet. The possible settings are: • Pass all traffic The Ravlin unit passes all IP traffic in the clear. • Block all traffic The Ravlin unit blocks all IP traffic. • Virtual Private Network The Ravlin unit encrypts, blocks, or passes IP traffic according to the entries in the policy database. **{** XE "IP packets" **}**
Inactive Client Timeout**{** XE "timeout" **}{** XE "Inactive Client Timeout" **}**	Determines how long the Ravlin unit waits before terminating a security association between the Ravlin unit and an inactive RavlinSoft client.
Password	Determines the password required to access this Ravlin unit's configuration parameters with the RavlinNodeManager. The password consists of 2–16 digits (0 through 9). Passwords of at least 8 characters are recommended. As you enter the password, it appears as a sequence of asterisk (*) symbols for security. The default password**{** XE "default password" **}{** XE "password:default" **}** for all Ravlin units is “1234.”

2.4 Physical Security

The Personal Ravlin would be considered a multi-chip standalone module meeting Level 2 physical security requirements. The production grade integrated circuits are assembled on a printed circuit board. The PC board is installed into an opaque enclosure. The enclosure is seal by gluing the back panel. Any attempt to access the physical components would require damaging the seal, enclosure, and/or back panel.

2.5 Key Management

The unit's DSA key pair, the unit's digital certificate, and the RedCreek CA public key are stored in flash memory. The firmware does not include the capability of generating new DSA key pairs, and thus cannot change the unit's DSA key pair. The session keys are exchanged using the Diffie-Hellman algorithm, thus they are never exposed outside the unit. The session keys are stored in DRAM, and are zeroized after power off or rekey. The firmware does not support the exporting of any of the session keys nor of the unit's DSA private key.

2.6 Electromagnetic Interference/Electromagnetic Compatibility

The Personal Ravlin was tested and found to be fully compliant with FCC/CISPR 22/85 Class B, EN 5022B Class B, and EN50082-1 (1992). CKC Laboratories, Inc. performed the test, and the report number is FB97-041 & CE97-125. Their DAR Registration Number is DAT-P-051/95-00. According to FCC Part 15 Section 15.107, paragraph (e) and Section 109, paragraph (g), these tests meet the requirements of FCC Part 15, Subpart B, Class B.

3.0 Ravlin Operation

The Personal Ravlin and RavlinNodeManager User Guides outline the steps for the secure operation of the Personal Ravlin.

A. Install the RavlinNodeManager on a workstation in the network.
B. Install the Ravlin units on the network
C. Logically add the Ravlin units to the RavlinNodeManager
D. Establish the Key Management Table, Protocol Table, and Policy Data Entries.
E. Specify the operational parameters.

The following information may form the basis for an Appendix or Release Note regarding FIPS 140-1 Rules of Operation in addition to the standard User Guides.

3.1 Password Length

The password may consist of 2-16 digits (0 through 9). RedCreek recommends that the password be at least 8 digits in length

3.2 Manual Keys

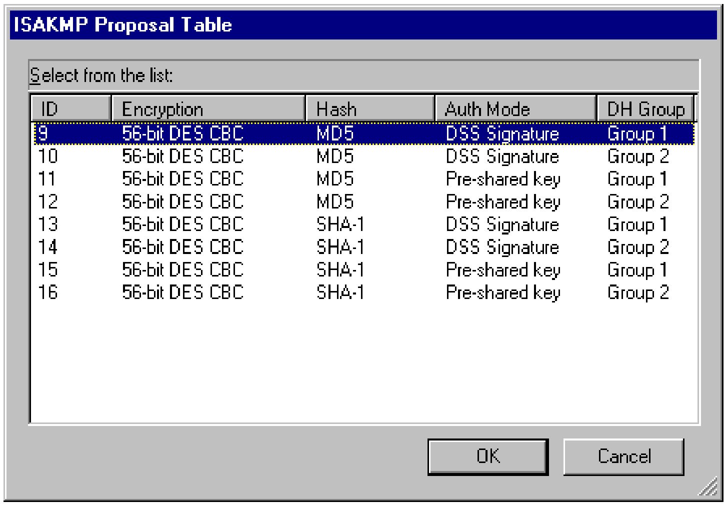
The Encryption Key entered into the manual key field may be either a string or a hex value. If a hex value is to be entered, then it must be preceded by "0x". The string may be up to 24 bytes long. The Ravlin unit will load the string, and will zero out any bytes not provided. The Crypto Officer is reminded to use all of the available resources, and to enter quality encryption keys.

The Authentication Key entered into the manual key field may be either a string or a hex value. If a hex value is to be entered, then it must be preceded by "0x". The string may be up to 20 bytes long. The Ravlin unit will load the string, and will zero out any bytes not provided. The Crypto Officer is reminded to use all of the available resources, and to enter quality authentication keys.

The Security Parameter Index entered into the manual key field must be a 32-bit integer from 256 to 4,294,967,295.

3.3 ISAKMP Proposal Table Selection

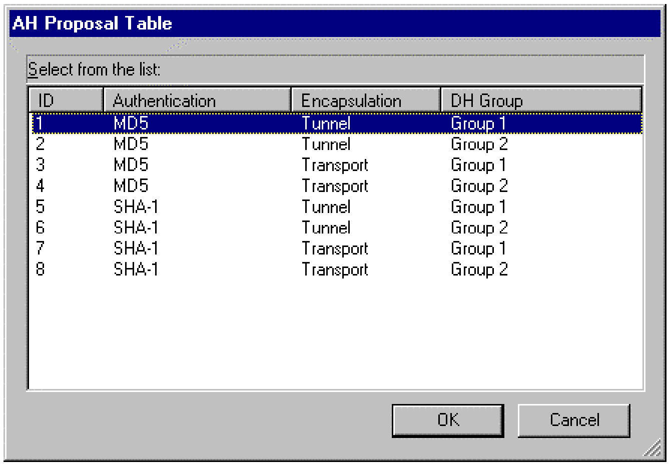
Only FIPS approved cryptographic algorithms should be selected for FIP 140-1 operations. The FIPS approved algorithms include DES, SHA-1, and DSS. Pre-shared key authentication mode may also be selected.



ID	Encryption	Hash	Auth Mode	DH Group
9	56-bit DES CBC	MD5	DSS Signature	Group 1
10	56-bit DES CBC	MD5	DSS Signature	Group 2
11	56-bit DES CBC	MD5	Pre-shared key	Group 1
12	56-bit DES CBC	MD5	Pre-shared key	Group 2
13	56-bit DES CBC	SHA-1	DSS Signature	Group 1
14	56-bit DES CBC	SHA-1	DSS Signature	Group 2
15	56-bit DES CBC	SHA-1	Pre-shared key	Group 1
16	56-bit DES CBC	SHA-1	Pre-shared key	Group 2

3.4 AH Proposal Table Selection

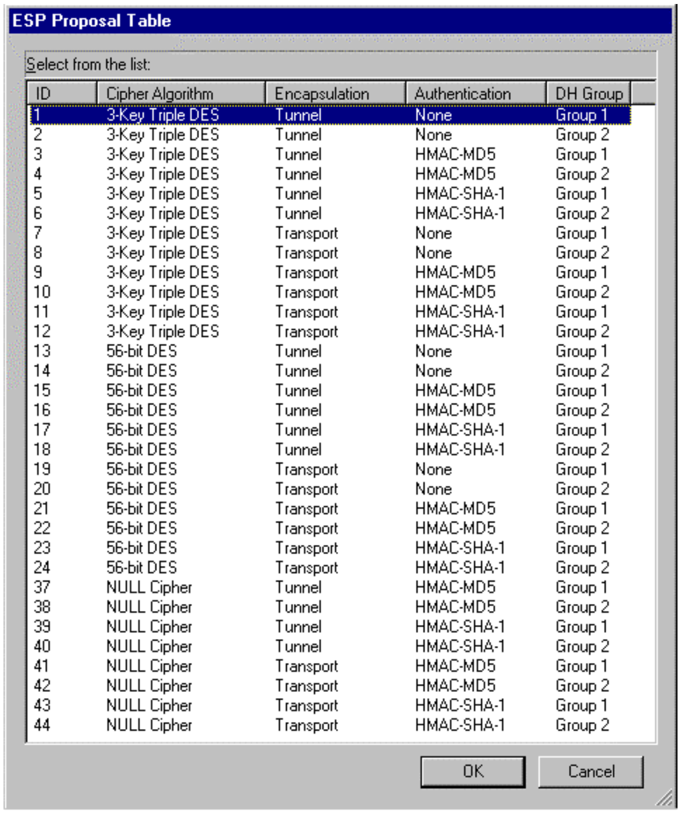
Only FIPS approved cryptographic algorithms should be selected for FIP 140-1 operations. The FIPS approved algorithm include SHA-1. Only the tunnel encapsulation should be selected for VPN security associations between Ravlin units.



ID	Authentication	Encapsulation	DH Group
1	MD5	Tunnel	Group 1
2	MD5	Tunnel	Group 2
3	MD5	Transport	Group 1
4	MD5	Transport	Group 2
5	SHA-1	Tunnel	Group 1
6	SHA-1	Tunnel	Group 2
7	SHA-1	Transport	Group 1
8	SHA-1	Transport	Group 2

3.5 ESP Proposal Table Selection

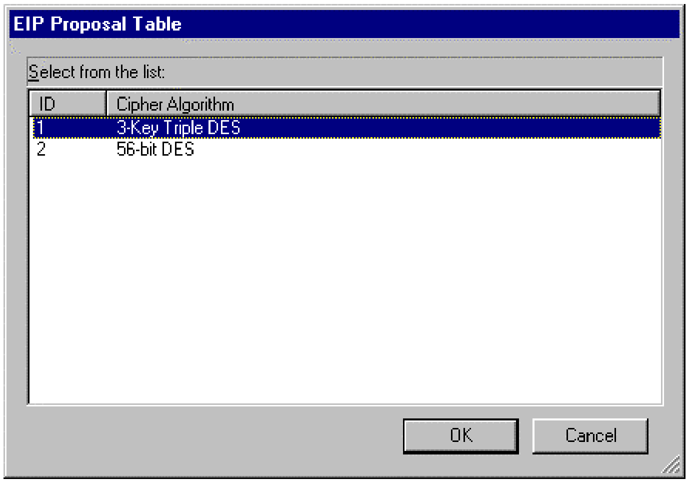
Only FIPS approved cryptographic algorithms should be selected for FIP 140-1 operations. The FIPS approved algorithms include DES, and SHA-1. The 3-Key Triple DES is also approved for US and Canadian Government usage. Only the “Tunnel” encapsulation should be selected for VPN security associations between Ravlin units. “None” is shown as an alternative for Authentication, but this should not be selected when operating in a FIPS environment.



ID	Cipher Algorithm	Encapsulation	Authentication	DH Group
1	3-Key Triple DES	Tunnel	None	Group 1
2	3-Key Triple DES	Tunnel	None	Group 2
3	3-Key Triple DES	Tunnel	HMAC-MD5	Group 1
4	3-Key Triple DES	Tunnel	HMAC-MD5	Group 2
5	3-Key Triple DES	Tunnel	HMAC-SHA-1	Group 1
6	3-Key Triple DES	Tunnel	HMAC-SHA-1	Group 2
7	3-Key Triple DES	Transport	None	Group 1
8	3-Key Triple DES	Transport	None	Group 2
9	3-Key Triple DES	Transport	HMAC-MD5	Group 1
10	3-Key Triple DES	Transport	HMAC-MD5	Group 2
11	3-Key Triple DES	Transport	HMAC-SHA-1	Group 1
12	3-Key Triple DES	Transport	HMAC-SHA-1	Group 2
13	56-bit DES	Tunnel	None	Group 1
14	56-bit DES	Tunnel	None	Group 2
15	56-bit DES	Tunnel	HMAC-MD5	Group 1
16	56-bit DES	Tunnel	HMAC-MD5	Group 2
17	56-bit DES	Tunnel	HMAC-SHA-1	Group 1
18	56-bit DES	Tunnel	HMAC-SHA-1	Group 2
19	56-bit DES	Transport	None	Group 1
20	56-bit DES	Transport	None	Group 2
21	56-bit DES	Transport	HMAC-MD5	Group 1
22	56-bit DES	Transport	HMAC-MD5	Group 2
23	56-bit DES	Transport	HMAC-SHA-1	Group 1
24	56-bit DES	Transport	HMAC-SHA-1	Group 2
37	NULL Cipher	Tunnel	HMAC-MD5	Group 1
38	NULL Cipher	Tunnel	HMAC-MD5	Group 2
39	NULL Cipher	Tunnel	HMAC-SHA-1	Group 1
40	NULL Cipher	Tunnel	HMAC-SHA-1	Group 2
41	NULL Cipher	Transport	HMAC-MD5	Group 1
42	NULL Cipher	Transport	HMAC-MD5	Group 2
43	NULL Cipher	Transport	HMAC-SHA-1	Group 1
44	NULL Cipher	Transport	HMAC-SHA-1	Group 2

3.6 EIP Proposal Table Selection

Only FIPS approved cryptographic algorithms should be selected for FIP 140-1 operations. The FIPS approved algorithm includes DES. The 3-Key Triple DES is also approved for US and Canadian Government usage.



EIP Proposal Table

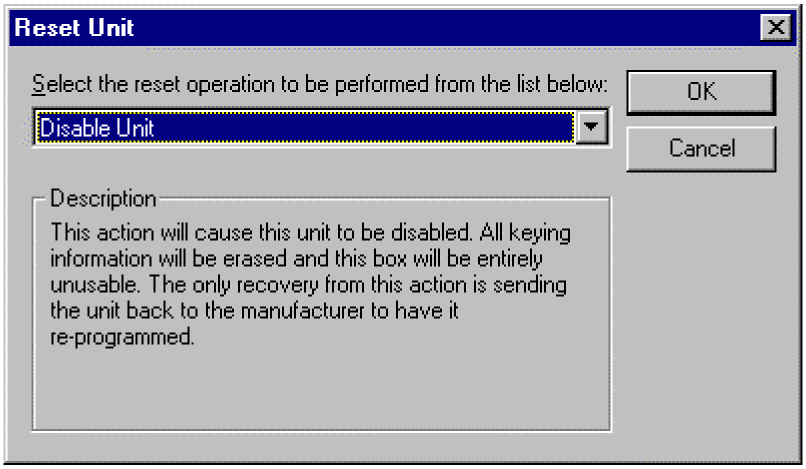
Select from the list:

ID	Cipher Algorithm
1	3-Key Triple DES
2	56-bit DES

3.7 Ravlin Unit Disposal

Part of the FIPS 140-1 cryptographic module security requirements is concerned with the entire life cycle management of cryptographic keys. Even after the Ravlin unit is reset to factory defaults, the FIPS 140-1 require an implementation to zeroize all internal plaintext cryptographic keys. These internal cryptographic keys are the unit's DSA key pair, the unit's X.509 v3 certificate, and the RedCreek Certificate Authority public key. These keys cannot be used to unprotect previously protected data since the Diffie-Hellman key exchange algorithm used provides perfectly forwarded secrecy.

In any event, the Ravlin unit should be disabled before the unit is disposed. Go to “Tools” menu, and select “Reset Unit”. From the Reset Unit dialogue box, select “Disable Unit”. Only Ravlin units with firmware version 3.3 or greater support the Disable Unit function. The RavlinNodeManager will only display that Reset Unit option for the supported Ravlin units. There will be three confirmation screens since zeroizing the Ravlin unit will completely disable unit, and the operation is not recoverable. However, the Ravlin unit may be sent back to RedCreek Communications to be re-manufactured, for a fee.



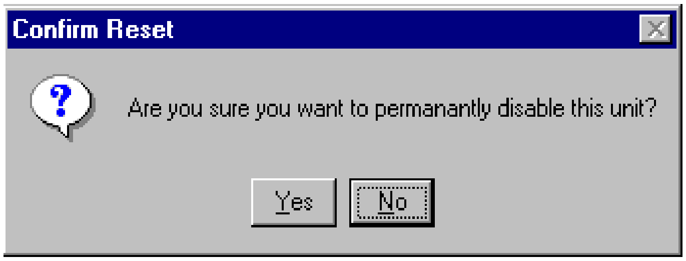
Reset Unit

Select the reset operation to be performed from the list below: Disable Unit

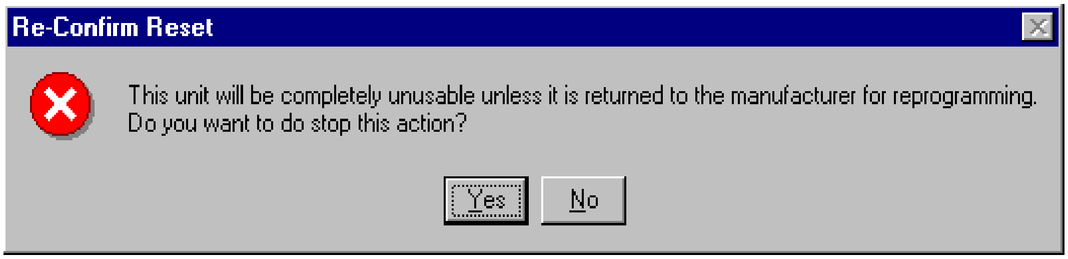
Description

This action will cause this unit to be disabled. All keying information will be erased and this box will be entirely unusable. The only recovery from this action is sending the unit back to the manufacturer to have it re-programmed.

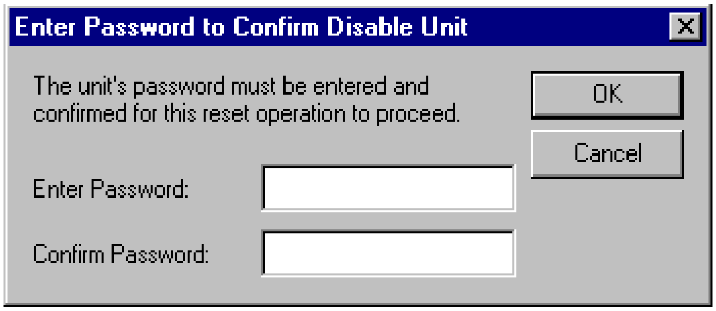
The confirmation screens button defaults are designed to prevent accidental disabling of the unit by hitting a series of returns or by clicking on the same spot on the screen; in case the wrong reset operation was selected. In addition, the unit's password is separately requested before the disable command is sent along with the entered password to the Ravlin unit.


Confirm Reset

Are you sure you want to permanantly disable this unit?


Re-Confirm Reset

This unit will be completely unusable unless it is returned to the manufacturer for reprogramming.
Do you want to do stop this action?


Enter Password to Confirm Disable Unit

The unit's password must be entered and confirmed for this reset operation to proceed.

Enter Password:

Confirm Password:

If the same password are not entered, then the RavlinNodeManager will display an 'Invalid Key' dialog box. If the request operation was successful, the RavlinNodeManager will display a 'Reset Complete' dialog box.

3.8 Power-On Self-Test (POST)

The Personal Ravlin executes a series of power-on self-tests after power is applied to the unit. If there were no errors, then the yellow LED on the front panel will be off. If there were a power-on self-test failure, then the yellow LED on the front panel will blink the number of the failed test. The corresponding failed test number would be the following:

Power-On Self-Test	Failed Test Number
FIPS Bypass Test	3
Test Real Time Clock	5
Test Random Numbers	7
Test Crypto-Core Gate Array (DES encrypt and decrypt)	2
SHA Hash Algorithm Test	9
DSA Signature Test	10

3.9 Firmware Upgrade

Ravlin units with firmware version 3.31 or greater require that all firmware downloaded be digitally signed (DSA) by RedCreek Communications. If the firmware downloaded to the Ravlin unit is not properly signed, the Unknown error code 319 will occur. The RedCreek DSA private key used to sign the firmware is separate from the RedCreek Certificate Authority DSA private key used to sign Ravlin unit certificates.