Bluesocket® WG-5000 Wireless Gateway

(Hardware Versions: 870-500FF-002, 870-500FT-002, 870-500TF-002, and 870-500TT-002,
and Firmware Version 4.1.0.11.fips.7)

FIPS 140-2 Non-proprietary Security Policy

Level 2 Validation

Part Number: 870-50000-S01
Revision: 1.3

September 2006

Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Hardware Versions: 870-500FF-002, 870-500FT-002, 870-500TF-002, and 870-500TT-002, and Firmware Version 4.1.0.11.fips.7 of the WG-5000 Wireless Gateway from Bluesocket, Incorporated.

This security policy describes how the WG-5000 meets the security requirements of FIPS 140-2, and how to operate the WG-5000 in a secure FIPS 140-2-compliant mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Bluesocket WG-5000.

This document is non-proprietary, and may be copied in its entirety and without modification. All copies must include the copyright notice on the front page.

FIPS 140-2 (*Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Modules*) 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 NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

Refer to the Bluesocket, Incorporated website at http://www.bluesocket.com for complete details about the entire line of Bluesocket Wireless Gateways.

You can find specific information about the Bluesocket WG-5000 Wireless Gateway at http://www.bluesocket.com/solutions/WG-5000.pdf.

1.3 Terminology

In this document, the terms *Bluesocket WG-5000* and *WG-5000* refer to version 4.1.0.11.fips.7 of the Bluesocket WG-5000 Wireless Gateway.

1.4 Document Organization

This Security Policy document is one document in a FIPS 140-2 Submission Package.

In addition to this document, the Submission Package includes:

- Proprietary security policy
- Vendor evidence document
- Finite state machine
- Module firmware listing
- Other supporting documentation as additional references

This Security Policy and other Validation Submission Documentation was produced by Bluesocket, Incorporated. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Bluesocket, Incorporated.

This document provides an overview of the Bluesocket WG-5000 and explains the secure configuration and operation of the module. This introductory section is followed by Section 2, which details the general features and functionality of the Bluesocket WG-5000 and describes how the WG-5000 meets all Level 2 FIPS 140-2 requirements. Section 3 specifically addresses the required configuration for the FIPS 140-2-compliant operation. Section 4 defines the acronyms and abbreviations used in this document.

2 The Bluesocket WG-5000

The Bluesocket WG-5000 Wireless Gateway provides a single scalable solution to the security, quality of service (QoS), and management issues facing institutions, enterprises, and service providers who deploy 802.11 and Bluetooth-based wireless networks.

The WG-5000 resides between the wireless LAN access points and the wired LAN as shown in Figure 1, and requires no changes to the existing wired LAN or user client software.

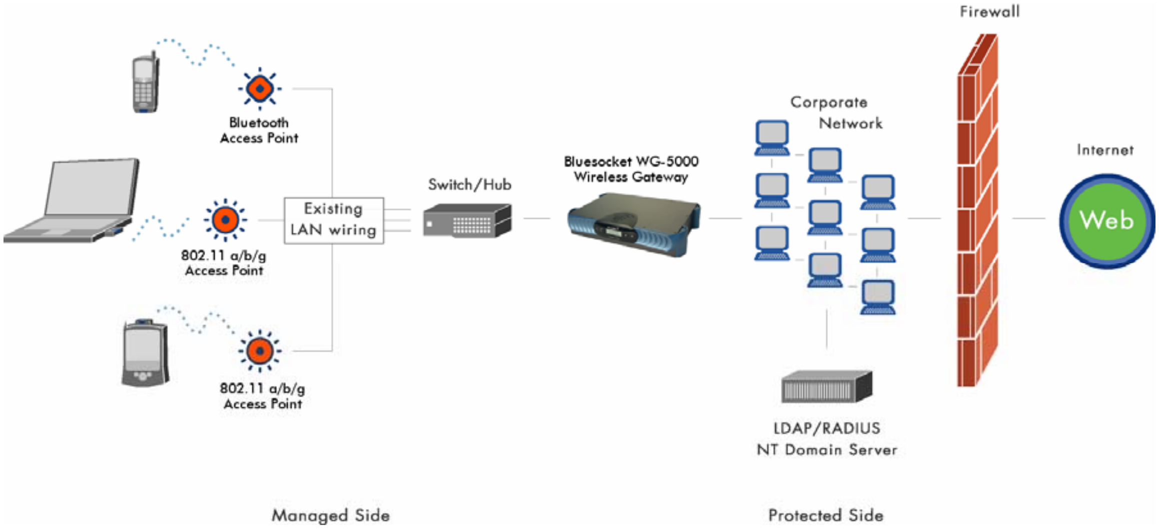
Firewall
Bluetooth Access Point
Corporate Network
Internet
Bluesocket WG-5000 Wireless Gateway
Switch/Hub
Existing LAN wiring
Web
802.11 a/b/g Access Point
802.11 a/b/g Access Point
LDAP/RADIUS NT Domain Server
Managed Side
Protected Side

Figure 1: The Role of the Bluesocket WG-5000 in a Wireless LAN

The WG-5000 mediates access between the wireless access points (the *managed side* of the network) and the enterprise network or Internet (the *protected side* of the network).

Two WG-5000s may be coupled to provide a hot failover capability, and multiple WG-5000s may be installed for large sites with higher data density requirements.

To verify the identity of a user, the WG-5000 uses authentication. The user submits a username and password, or other credential from his or her wireless device. The WG-

5000 first checks its internal user database (for stand-alone use) and then an external RADIUS or LDAP/Active Directory server in turn for a valid match.

If a match is found, the WG-5000 grants the user access to the network. If the WG-5000 cannot authenticate the user, the user is denied access.

After the user is authenticated, the WG-5000 defines which network resources and destinations in the enterprise the user can access, the bandwidth they can use. The Crypto-officer implements authorization by defining a role and assigning it to the user.

2.1 FIPS 140-2 Applicability

The Bluesocket WG-5000 is classified as a multi-chip standalone module as defined in the *Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules*.

The Bluesocket WG-5000 meets all the Level 2 requirements for FIPS 140-2 as summarized in Table 1.

Table 1: Bluesocket WG-5000 FIPS 140-2 Security Levels

FIPS 140-2 Security Requirements Section	Security Level
1. Cryptographic Module Specification	2
2. Module Ports and Interfaces	2
3. Roles, Services, and Authentication	2
4. Finite State Model	2
5. Physical Security	2
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	3
9. Self Tests	2
10. Design Assurance	2
11. Mitigation of Other Attacks	N/A

2.2 Cryptographic Module Specification

The Bluesocket WG-5000 operates in a FIPS 140-2-compliant mode.

The cryptographic boundary for the WG-5000 is the defined as the metal case enclosing all of the hardware and firmware system components as shown in Figure 2.

The WG-5000 cryptographic module consists of the following generic components:

- A commercially available general-purpose hardware computing platform based on the Intel Pentium IV CPU and the Intel E7210 Chipset. A Block Diagram is provided in Figure 1.
- A customized Linux OS running on the hardware platform. WG-5000 FIPS 140-2 compliance was tested on Linux OS version 2.4.18.
- Bluesocket/AdmitOne IPSec engine, running on the above platform under the operating system in Kernel Space.
- Bluesocket/AdmitOne IKE service running on the above platform, under the above OS in User Space memory.
- Bluesocket Application code running on the above platform, under the above OS in User Space memory.

Figure 2 shows a block diagram of the WG-5000 cryptographic module.

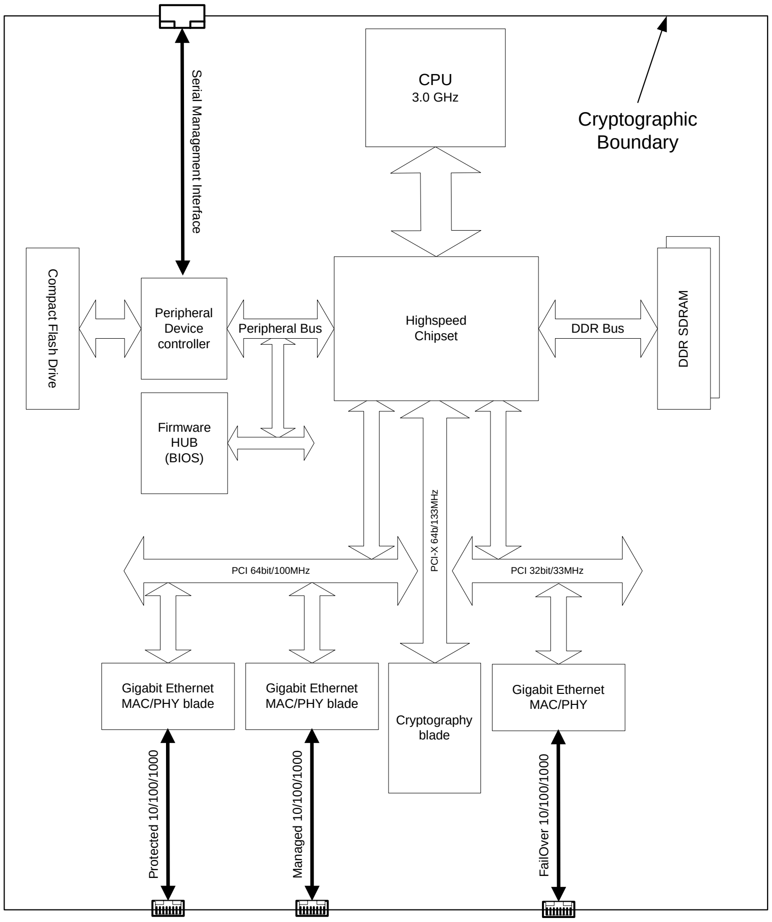

Figure 2: WG-5000 Cryptographic Module Block Diagram

Figure 3 shows a block diagram representing the WG-5000 major firmware components.

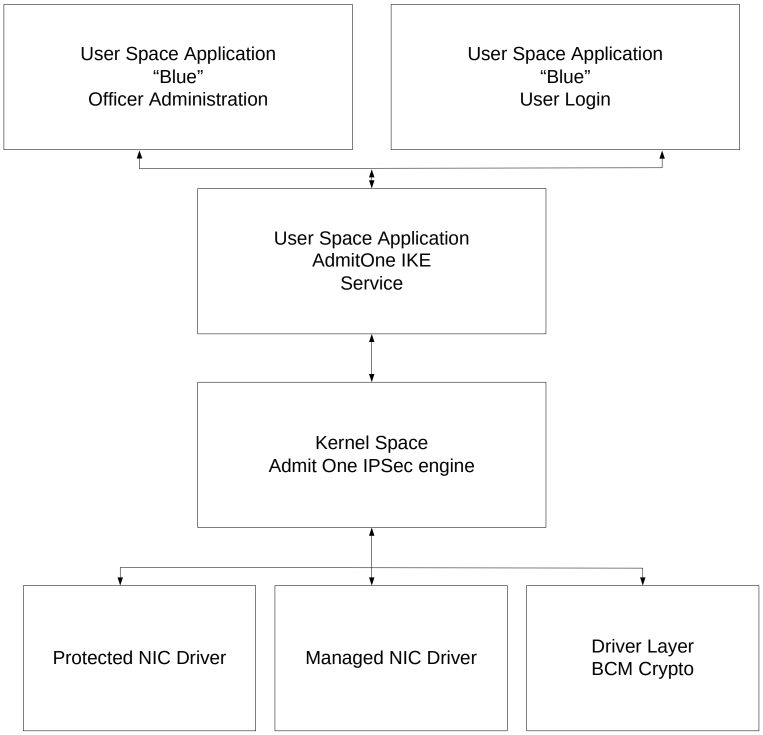

Figure 3: WG-5000 Firmware Layer Block Diagram

2.3 Cryptographic Module Interfaces

The WG-5000 cryptographic module is accessible only through well-defined physical ports including: two standard copper 10/100/1000 Mbps Ethernet ports (or optional 1000 Based-SX fiber ports) for network connectivity, a single copper 10/100/1000 Mbps Ethernet port for failover connectivity to another WG-5000, a serial port for local console management of the WG-5000, front-panel Power and Reset controls, front-panel LEDs and LCD for status, and an AC power plug and switch.

Additionally, the module has a video port.

The LEDs and LCD on the front of the module provide status information. The Power and Reset controls provide the ability to power down and rest the module. The AC power switch and power connector provide the ability to connect and disconnect the module from source power. The network connectors provide the ability to connect and disconnect the module from the network.

The physical ports to the units are described as follows:

- The Video port may monitor activity at boot time to ensure the WG-5000 boots properly. The Video port is used for status output only and does not accept user input.
- The Failover Port (Ethernet Port 2) is used to provide stateful information to a redundant unit for high-availability purposes.

- The Managed Port (Ethernet Port 1) provides Ethernet access to the managed clients. This port may be used to provide an IPSec tunnel to clients secured by IPSec.
- The Protected Port (Ethernet Port 0) provides an Ethernet link to the physically secured LAN. Packets are transmitted in the clear to and from this interface.
- The Serial port is RS232 compliant and provides a minimal set of management capabilities.

Table 2 maps the logical interfaces described by the FIPS 140-2 standard to physical ports on the WG-5000.

Table 2: FIPS Logical Interfaces Mapped to WG-5000 Physical Ports

FIPS 140-2 Logical Interface	WG-5000 Physical Port
Data Input Interface	Managed Port (Ethernet Port 0) Protected Port (Ethernet Port 1) Failover Port (Ethernet Port 2)
Data Output Interface	Managed Port Protected Port Failover Port
Control Input Interface	Managed Port Protected Port Serial Port Power Control Reset Control
Status Output Interface	Front Panel LCD Front Panel LEDs Serial Port Video Port
Power Interface	Power Plug Power Switch

2.4 Roles and Services

The WG-5000 supports role-based authentication. There are three roles in the module that operators may assume: a Local Crypto-Officer role, a Crypto-Officer role, and a User role.

The Local Crypto-Officer accesses the module using a command line interface (CLI) over the serial port. The Local Crypto-Officer authenticates with a password and is able to perform minimal configuration and management of the module.

The Crypto-Officer accesses the module through an Ethernet port over a TLS link to the Bluesocket Administration page served by the WG-5000 Web Server Application. The

Crypto-Officer authenticates with a User ID and password. The Crypto-Officer has the ability to fully configure and manage the module.

The User role accesses the module through the Managed Interface Ethernet port to pass IPSec-secured data or plaintext through the WG-5000.

To pass IPSec traffic through the module, the User must authenticate with a pre-shared key or by presenting a digital certificate for mutual authentication against the module's own digital certificate.

To transfer packets through the module in plaintext, without IPSec processing, the User authenticates with a User ID and password. Transfer of packets in plaintext through the module is not allowed in FIPS approved mode of operation.

2.4.1 Local Crypto-Officer Role

The Local Crypto-Officer is able to perform a limited set of WG-5000 configuration and management tasks. These tasks include resetting the WG-5000 internal database, rebooting and restarting the WG-5000, displaying a variety of status information.

Generally, the Local Crypto-Officer performs management tasks via the WG-5000 serial port only in the rare event that Crypto-Officer access to the WG-5000 is lost.

Table 3 details the Local Crypto-Officer's set of services in FIPS mode.

Table 3: Local Crypto-Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output
dbinit	Restore all database settings to their default value	Command	Command status
ifconfig	Show interface settings for Protected, Managed, and Failover interfaces	Command	Command status
processes	Show a list of all running processes	Command	Command status
restart	Restart the WG-5000	Command	Command status
switch	Switch to the alternate firmware image	Command	Command status
reboot	Reboot the WG-5000	Command	Command status
clean	Delete event logs	Command	Command status
exit	Exit the CLI	Command	Command status
interface	Set protected interface address	Command	Command status

Service	Description	Input	Output
self-tests	Invoke the WG-5000 self tests	Command or Cycle power to the WG-5000	Self-test status

2.4.2 Crypto-Officer Role

The Crypto-Officer role, accesses the module over a TLS session. The Crypto-Officer has the ability to fully configure and manage the module.

Table 4 details the Crypto-Officer's set of services in FIPS mode.

Table 4: Crypto-Officer Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output
IPSec SA configuration for Users	Install IPSec SAs on the module	Command and IPSec SA information over TLS session	Status of command over TLS session
TLS	Access the crypto-module via an TLS session over an https link	Password over a secured link	Access to HTML-based configuration interface
IPSec SA deletion	Delete IPSec SAs on the module	Command and IPSec SA information over TLS session	Status of command over TLS session
Network configuration of the module	Configure the network settings of the module	Command and network settings over TLS session	New network configuration for the module and status of command over TLS session
QoS configuration	Configure the QoS settings of the module	Command and OoS settings over TLS session	New QoS configuration for the module and status of command over TLS session
Device Administration	Modify port forwarding and address translation settings on the module	Command and administration settings over TLS session	Modified device administration settings for the module and status of command over TLS session
Module Logging configuration	Configure the logging settings of the module	Command and logging settings over TLS session	New logging configuration for the module and status of command over TLS session
Administer User accounts	Add, delete, or edit User account settings	Command and User account settings over TLS session	Modified User account settings for the module and status of command over TLS session

Service	Description	Input	Output
reboot	Reboot the WG-5000	Command over TLS session	Command status over TLS session
restart	Restart the WG-5000.	Command over TLS session	Command status over TLS session
shutdown	Shut down the WG-5000	Command over TLS session	Command status over TLS session
self-tests	Initiate the WG-5000 self tests	Cycle power to the WG-5000	Self-test status

2.4.3 User Role

The User role accesses the module through the Managed Interface Ethernet port to pass IPSec-secured data or plaintext through the WG-5000. Transfer of plaintext traffic through the module is not allowed in FIPS approved mode of operation.

To pass IPSec traffic through the module, the User must authenticate with a pre-shared key or by presenting a digital certificate for mutual authentication against the module's own digital certificate. User and data security are provided by a combination of SHA-1 and one of the following cryptographic protocols, DES (transitional phase only - valid until May 19, 2007), 3DES, or AES.

To transfer packets through the module in plaintext, without IPSec processing, the User authenticates with a User ID and password but this is not allowed in FIPS mode.

Table 5 details the User role's set of services in FIPS mode.

Table 5: User Services, Descriptions, Inputs, and Outputs

Service	Description	Input	Output
IPSec	Access the module's IPSec services to secure communications between the User and the module	IPSec inputs, commands, and data	IPSec outputs, status, and data

2.4.4 Authentication Mechanisms

The module implements password-based authentication and digital certificate/RSA-based authentication as summarized in Table 6.

Table 6: WG-5000 Authentication Methods

Authentication Type	Use/Strength
Password-based authentication	Local Crypto-Officer password is a fixed seven-character password configured at the factory. Considering only the alphanumeric character set, the number of potential passwords is 62^7.

	Crypto-Officer password must be at least eight characters in length and may be any combination of alphanumeric characters. Considering only the alphanumeric character set, the number of potential passwords is 62^8. User passwords must be at least eight characters in length and may be any combination of alphanumeric characters. Considering only the alphanumeric character set, the number of potential passwords is 62^8. IPSec Pre-shared Secret must be at least eight characters in length and may be any combination of alphanumeric characters. Considering only the alphanumeric character set, the number of potential passwords is 62^8.
Digital Certificate/RSA-based Authentication	Authenticate User to pass IPSec-encrypted data. Certificate is secured by RSA. RSA is used by the Crypto-Officer to initially authenticate to the module using a TLS handshake. The mechanism, using a 1024-bit key size, provides a work factor of roughly 2^{80} (cryptographic strength provided by 1024-bit RSA).

2.4.5 Unauthenticated Services

N/A—the module does not provide any unauthenticated services.

2.4.6 Finite State Machine Model

The WG-5000 is designed around a Finite State Machine (FSM), which is detailed in a Bluesocket proprietary document (FIPS 140-2 Proprietary Finite State Machine). Parties interested in reviewing this document should contact Bluesocket through the sources listed in Section 1.2.

2.5 Physical Security

The Bluesocket WG-5000 is housed in a FIPS 140-2 Level 2-compliant case. The WG-5000 housing is made of a two-piece, tamper-resistant metal shell with a front-panel polycarbonate bezel. The WG-5000 case is fitted with an inner louvered metal shield that renders the case opaque and resistant to probing. The only components exposed from the case are the front-panel LCD, LEDs, Power Switch and Reset Switch, and the rear-panel AC power receptacle, network interface connectors, serial port connector, and video port connector.

Tamper-evident labels are placed across the WG-2100's top cover and case, and on the back panel at the factory as shown in Figure 4.

Any attempt to access the WG-2100's internal components will result in the tamper-evident labels being damaged.

2.6 Operational Environment

FIPS 140-2 operational environment requirements do not apply to the Bluesocket WG-5000 Wireless Gateway as the WG-5000 is characterized as having a non-modifiable operational environment.

2.7 Electromagnetic Compatibility (EMI/EMC)

The WG-5000 has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, (Class B for home use).

2.8 Cryptographic Algorithms and Protocols

The WG-5000 implements the following approved cryptographic algorithms:

- SHA-1 (Certificate #228, #329) – per FIPS PUB 180-1
- HMAC-SHA-1 (Certificate #12, #63) – per FIPS-198
- Triple-DES-ECB, CBC (Certificate #335) and Triple-DES-CBC (Certificate #250) – per FIPS PUB 46-3
- DES-ECB, CBC, CFB8, CFB64, OFB (transitional phase only - valid until May 19, 2007) (Certificate #313) – per FIPS PUB 46-3
- AES-CFB128 (Certificate #76, #254) – per FIPS PUB 197
- RSA Digital Signatures (Generation/Verification) – per PKCS#1, RSA Key generation (ANSI X9.31) Mod Sizes 1024/1536/2048/3072/4096 (Certificate #14)
- RNG (FIPS 186-2, Appendix 3.1, Change Notice 1) (Certificate #16)

The module implements the following non-FIPS 140-2-approved algorithms:

- MD5
- HMAC-MD5
- Diffie-Hellman (Key agreement) – Permitted for use in a FIPS 140-2-approved mode of operation. The Diffie-Hellman implementation uses a 160-bit private key and 1024/1536 bit public key.
- RSA Key Transport – as per PKCS#1 during TLS – Permitted for use in a FIPS 140-2 approved mode of operation. The RSA Key Transport implementation uses a 1024-bit key length.

The Key establishment methodology provides 80-bits of encryption strength.

The module supports the following protocols for use in an approved mode of operation:

- IPSec
- TLS

These cryptographic algorithms are implemented in firmware for TLS and implemented in both hardware and firmware for IPSec.

The WG-5000 uses a FIPS 186-2 Appendix 3.1 change notice 1-compliant random number generator.

2.9 Cryptographic Key Management

This section describes cryptographic keys and other critical security parameters (CSPs) contained in the WG-5000.

2.9.1 Local Crypto-Officer Password

The Local Crypto-Officer access password is a pre-configured factory-default value that cannot be modified. The password is stored in the WG-5000 module EEPROM and is used to authenticate the Local Crypto-Officer.

Type	Fixed seven-character password
Use	Authenticate Local Crypto-Officer
Storage	In non-volatile EEPROM (plaintext)
Applicable Service	All Local Crypto-Officer Commands
Access by Role*	Local Crypto-Officer - R
Generation	Factory-default
Destruction	Crypto-Officer overwrites EEPROM

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.2 Crypto-Officer Password

The Crypto-Officer access password is used to authenticate the Crypto-Officer over a TLS connection. The password is created by and may be modified the Crypto-Officer. The password is stored in the WG-5000 module EEPROM.

Type	Eight-character password
Use	Authenticate Crypto-Officer
Storage	In non-volatile EEPROM (plaintext)
Applicable Service	All Crypto-Officer Services
Access by Role*	Crypto-Officer – W, R, D
Generation	Outside of module (input by Crypto-Officer)
Destruction	Reset module to factory default values

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.3 User Access Password

The User access password is used to authenticate a user for plaintext data transfer through the module. The password is created by and may be modified the Crypto-Officer. The user access password is stored in the WG-5000 module EEPROM.

Note: Plaintext data transfer through the module is not allowed in FIPS mode.

Type	Eight-character password
Use	Authenticate User for Plaintext Traffic
Storage	In non-volatile EEPROM (plaintext)
Applicable Service	Plaintext Traffic
Access by Role*	Crypto-Officer – W, R, D; User - R
Generation	Outside of module (input by Crypto-Officer)
Destruction	Reset module to factory default values

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.4 IPSec Pre-Shared Secret

The WG-5000 uses the IKE protocol (RFC-2409) for key establishment. IKE authentication of a User can be done with digital certificates using the RSA signature algorithm or a pre-shared secret.

The IPSec Pre-shared Secret is used to authenticate a User to pass IPSec encrypted data through the module. The password is created by and may be modified the Crypto-Officer. The IPSec Pre-shared Secret is stored in the WG-5000 module EEPROM.

Type	Eight-character password
Use	Authenticate User for IPSec Traffic
Storage	In non-volatile EEPROM (plaintext)
Applicable Service	IPSec
Access by Role	Crypto-Officer – W, R, D; User - R
Generation	Outside of module (input by Crypto-Officer)
Destruction	Reset module to factory default values

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.5 IPSec Server Certificate

The WG-5000 uses the IKE protocol (RFC-2409) for key establishment. IKE authentication of a User can be done with digital certificates using the RSA signature algorithm or a pre-shared secret.

The WG-5000 uses a certificate protected with a private key to authenticate the IPSec Server running on the WG-5000. The certificate is stored in RAM, in non-volatile EEPROM, and in the WG-5000 database. The IPSec Server Certificate is deleted from EEPROM on restart and is deleted from the WG-5000 database upon administrator command.

Type	Digital Certificate with RSA signature
Use	Authenticate IPSec Server running on WG-5000
Storage	In volatile memory, in non-volatile EEPROM in X.509 certificate, and in WG-5000 Database
Applicable Service	IPSec
Access by Role*	Crypto-Officer – W, R, D; User - R
Generation	Outside of module (X.509 specification)
Destruction	Deleted from EEPROM on restart, and deleted from WG-5000 database upon Crypto-Officer command

***** - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.6 Enrollment CA Certificate

The WG-5000 uses the IKE protocol (RFC-2409) for key establishment. IKE authentication of a User can be done with digital certificates using the RSA signature algorithm or a pre-shared secret.

The trusted Bluesocket CA public key certificate is loaded on the module by the manufacturer at production and is not generated by the module. This certificate is used to sign IPSec client requests.

Type	Digital Certificate with RSA signature
Use	Sign IPSec client certificate requests
Storage	In non-volatile EEPROM in X.509 certificate and in WG-5000 Database
Applicable Service	IPSec
Access by Role*	Crypto-Officer – R; User - R
Generation	Outside of module (X.509 specification)
Destruction	Deleted from EEPROM upon restart and from WG-5000 Database upon Crypto-Officer command

***** - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.7 IPSec Diffie-Hellman Key Pairs

The WG-5000 uses the IKE protocol (RFC-2409) for key establishment. During IKE Phase 1 negotiation, the WG-5000 establishes a Security Association (SA) with a User that defines methods for protecting future communications. The Diffie-Hellman method is used to generate key material to encrypt and authenticate further IKE negotiations, and to generate keying material for User IPSec services.

Type	Diffie-Hellman
Use	Encrypt and authenticate IKE negotiations
Storage	RAM
Applicable Service	IPSec
Access by Role	User - R
Generation	Generated using the PRNG specified in FIPS 186-2 Appendix 3.1 change notice 1.
Destruction	Deleted from memory by restarting the module

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.8 IPSec Session Keys

The WG-5000 uses the IKE protocol (RFC-2409) for key establishment. IPSec session keys are generated during IKE Phase 2 negotiations. The session keys are derived from the keying material established with the Diffie-Hellman exchange in Phase 1. If the Crypto-Officer has configured the WG-5000 to use IKE perfect secrecy mode, the session keys are established using a Diffie-Hellman exchange.

The Crypto-Officer can configure a lifetime for the IPSec session keys. When the configured lifetime expires, new session keys are negotiated.

Type	3DES, DES (transitional phase only - valid until May 19, 2007), or AES/HMAC-SHA-1 key
Use	Encrypt IPSec Traffic
Storage	In volatile memory
Applicable Service	IPSec
Access by Role*	User - R
Generation	Oakley algorithms using Diffie-Hellman groups 1 to 3
Destruction	Deleted from memory by restarting the module

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.9 TLS Server Certificate

The WG-5000 uses TLS to protect data during administration of the WG-5000 by the Crypto-Officer over HTTPS.

The WG-5000 uses a certificate protected with a private key to provide server authentication. The WG-5000 also uses the RSA private key to decrypt the pre-master secret from the TLS client during TLS handshaking. The WG-5000 uses the RSA key transport for key establishment during TLS.

The TLS Server Private Key is generated using standard Open TLS commands and is stored in RAM and in non-volatile EEPROM. The TLS Server Private Key is zeroized in memory after the TLS session has terminated.

Type	RSA private key
Use	TLS Server Certificate is used to Authenticate the server and the RSA private key is used to decrypt the pre-master secret from the TLS client
Storage	In volatile memory and in non-volatile EEPROM
Applicable Service	TLS
Access by Role*	Crypto-Officer - R
Generation	Generated using the PRNG specified in FIPS 186-2 Appendix 3.1 change notice 1.
Destruction	Crypto-Officer overwrites EEPROM

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.10 TLS Write Key

The WG-5000 uses TLS to protect data during administration of the WG-5000 by the Crypto-Officer over HTTPS.

The WG-5000 uses a symmetric secret key to encrypt TLS application data for each TLS connection. The TLS Write Key is generated using a TLS standard algorithm and is stored in RAM. The TLS Write Key is zeroized after the TLS session has terminated.

Type	3DES
Use	To encrypt TLS Application data for each TLS connection
Storage	In volatile memory
Applicable Service	TLS
Access by Role	Crypto-Officer - R
Generation	Via standard TLS algorithm
Destruction	Zeroized after the TLS session has terminated

* - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.11 TLS MAC Secret

The WG-5000 uses TLS to protect data during administration of the WG-5000 by the Crypto-Officer over HTTPS.

The WG-5000 uses a message authentication code (MAC) key to secure TLS application data for each TLS connection. The TLS MAC Secret Key is generated using a TLS standard algorithm and is stored in RAM. The key is zeroized after the TLS session has terminated.

Type	HMAC-SHA-1
Use	Secure TLS application data
Storage	In volatile memory
Applicable Service	TLS
Access by Role	Crypto-Officer –R
Generation	Via standard TLS algorithm
Destruction	Zeroized after the TLS session has terminated

***** - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.12 Configuration Files

The configuration files store the WG-5000's settings for network configuration, QoS configuration, device administration, module logging, user accounts, and other module configurations. The configuration files are created by the Crypto-Officer and are stored in the module's non-volatile EEPROM.

Type	Plaintext files
Use	Define QoS, device administration, and other module settings.
Storage	In non-volatile memory
Applicable Service	Device administration and configuration
Access by Role	Crypto-Officer – W, R, D; User - R
Generation	Outside of module (Input by Crypto-Officer)
Destruction	Reset module to factory default values

***** - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.9.13 HMAC-SHA-1 Key

The WG-5000 verifies the integrity of its system firmware upon power up using an HMAC-SHA-1 checksum.

Type HMAC-SHA-1 Key

Use Verify integrity of WG-5000 system firmware.

Storage In non-volatile memory

Applicable Service Firmware integrity power-up self test

Access by Role Crypto-Officer – W, R, D

Generation HMAC-SHA-1 algorithm

Destruction Deleted from EEPROM on restart

- - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

Table 8 lists the Critical Security Parameters employed by the Bluesocket WG-5000 Wireless Gateway Cryptographic Module.

Table 8: Critical Security Parameters Employed by the Bluesocket WG-5000

Key	Key Type	Key Generation	Storage Location	Key usage	Applicable Service	Access by Role*
IPSec Pre-shared secret	8-character Password	Outside of module	Stored in plain text in non-volatile EEPROM	Authenticate user for IPSec traffic	IPSec	CO-W, R, D User- R
IPSec server certificate	Digital Certificate with RSA Signature	Outside of module (X.509 specification)	Stored in memory, in non-volatile EEPROM in X.509 certificate and in WG-5000 database	Authenticate IPSec Server running on WG-5000	IPSec	CO-W, R, D User- R
Enrollment CA Certificate	Digital Certificate with RSA signature	Outside of module (X.509 specification)	Stored in non-volatile EEPROM in X.509 certificate and in WG-5000 Database	Sign IPSec client certificate requests	IPSec	CO- R User- R
IPSec Diffie-Hellman Key pairs	Diffie-Hellman Private/public Key pair	Generated using the FIPS-186.2 Appendix 3.1 (Change Notice	Stored in plain text in RAM	Encrypt and authenticate IKE negotiations	IPSec	User- R

Key	Key Type	Key Generation	Storage Location	Key usage	Applicable Service	Access by Role*
		1) PRNG				
IPSec Session Keys	TDES, DES, AES/ HMAC-SHA-1 Key	Oakley algorithms using DH groups 1 to 3	Stored in plain text in volatile memory	Encrypt IPSec traffic	IPSec	User- R
TLS Server Certificate	RSA Key pair	Generated using the FIPS-186.2 Appendix 3.1 (Change Notice 1) PRNG	Stored in plaintext in volatile memory and in non-volatile EEPROM	TLS server certificate is used to Authenticate the server and the RSA private key is used to decrypt the pre-master secret from the TLS client	TLS	CO- R
TLS Write Key	TDES	Via standard TLS algorithms	Stored in plain text in volatile memory	To encrypt TLS application data for each TLS connection	TLS	CO- R
TLS MAC Secret	HMAC-SHA-1 Key	Via standard TLS algorithm	Stored in plain text in volatile memory	Secure TLS application data	TLS	CO -R
Firmware Integrity Key	HMAC-SHA-1 Key	HMAC-SHA-1 Algorithm	Stored in plain text in non-volatile EEPROM	Verify integrity of WG-5000 system firmware	Firmware Integrity Power-up self test	CO- W, R, D
Configuration Files	Plain text files	Outside of module	Stored in plain text in non-volatile memory	Define QoS, Device administration and other module settings	Device administration & Configuration	CO-W, R, D User- R
Local Crypto-Officer Password	Fixed 7-character password	Factory Default	Stored in plain text in non-volatile EEPROM	Authenticate Local Crypto-Officer	All Local Crypto officer services	Local CO- R

Key	Key Type	Key Generation	Storage Location	Key usage	Applicable Service	Access by Role*
Crypto-Officer Password	8-character password	Outside of module	Stored in plaintext in non-volatile EEPROM	Authenticate Crypto-Officer	All Crypto-officer services	CO-W, R, D
User Access Password	8-character password	Outside of module	Stored in plain text in non-volatile EEPROM	Authenticate User for Plaintext traffic	Plain text traffic	CO-W, R, D User- R

- * - W – Write (input or generate) key or CSP, R – Read (use) key or CSP, D – Delete (zeroize) key or CSP

2.10 Self-Tests

As required by FIPS 140-2, the WG-5000 performs a number of startup and conditional self-tests to ensure proper operation. Self-tests include integrity checks over each binary component, cryptographic algorithm tests, and a continuous random number generator test that monitors output from the module's FIPS-approved and non-approved random number generators.

The Local Crypto-Officer and the Crypto-Officer can initiate the WG-5000's self-tests by power-cycling the WG-5000.

2.10.1 Power On Self Tests

The WG-5000 executes several power-on-self-tests including:

- Triple-DES Known Answer Test (KAT)
- DES KAT *
- AES KAT
- SHA-1 KAT
- RSA KAT for key transport and authentication
- System Firmware Integrity Check Using HMAC-SHA-1
- Critical Functions Test
  - Hardware Integrity check

The WG-5000 performs the Cryptographic Algorithm tests on all the implementations of the FIPS-approved algorithms used by the module.

* DES is used for transitional phase only - valid until May 19, 2007.

2.10.2 Conditional Self Tests

The WG-5000 executes the following conditional self-test:

- Continuous RNG Test on both the FIPS-approved PRNG and the non-deterministic RNG used to the seed the PRNG
- RSA Pair-wise Consistency Test for key transport and authentication

2.11 Design Assurance

The development process for the Bluesocket WG-5000 Wireless Gateway includes a configuration management (CM) system. The system in use is CVS and Bluesocket employs a branching methodology for release management. The CVS tagging mechanism is utilized to mark reproducible states in the source tree. CVS also handles all versioning of the various source code files and documentation for the WG-5000.

2.12 Mitigation of Other Attacks

The module does not implement mechanisms to mitigate any other specific attacks.

3 Secure Operation of the WG-5000

The Bluesocket WG-5000 is classified as a multi-chip standalone module as defined in the Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules*. The cryptographic boundary for the WG-5000 is the defined as the metal case enclosing all of the hardware and firmware system components.

This section provides guidance information to ensure FIPS 140-2-compliant operation of the WG-5000 and includes:

- Physically Securing the WG-5000
- Crypto-Officer Guidance
- User Guidance

3.1 Physically Securing the WG-5000

Periodically, the Crypto-Operator should inspect the WG-5000 to verify that its chassis has not been tampered with and the device is physically secure. This chapter provides information about verifying the physical security of the WG-5000 and includes:

- WG-5000 Tamper-evident Labels
- Inspecting the WG-5000 Chassis

3.1.1 WG-5000 Tamper-evident Labels

The Bluesocket WG-5000 is housed in a FIPS 140-2 Level 2-compliant case and is shipped from the factory in a secure condition.

The WG-5000 housing is made of a two-piece, tamper-resistant metal shell with a front-panel polycarbonate bezel. The WG-5000 case is fitted with an inner louvered metal shield that renders the case opaque and resistant to probing. The only components exposed from the case are the front-panel LCD, LEDs, Power Switch and Reset Switch, and the rear-panel AC power receptacle, network interface connectors, serial port connector, and video port connector. Access to the WG-5000's internal components can only be gained by removing the WG-5000's top cover.

Tamper-evident labels are placed across the WG-5000's top cover and case, and on the back panel at the factory as shown in Figure 4.

Any attempt to access the WG-5000's internal components will result in the tamper-evident labels being damaged.

3.1.2 Inspecting the WG-5000 Chassis

The WG-5000 is not FIPS 140-2-compliant if its internal components have been modified in any way.

The Crypto-Officer should regularly inspect the WG-5000 chassis for signs of tampering, including deep scratches on the surface, cracks, and any physical damage to the appearance of the module, especially around the power and port connectors.

Verify that the tamper-evident labels are fully intact. If evidence of tampering is discovered, the Crypto-Officer should power off the WG-5000 and contact Bluesocket, Inc.

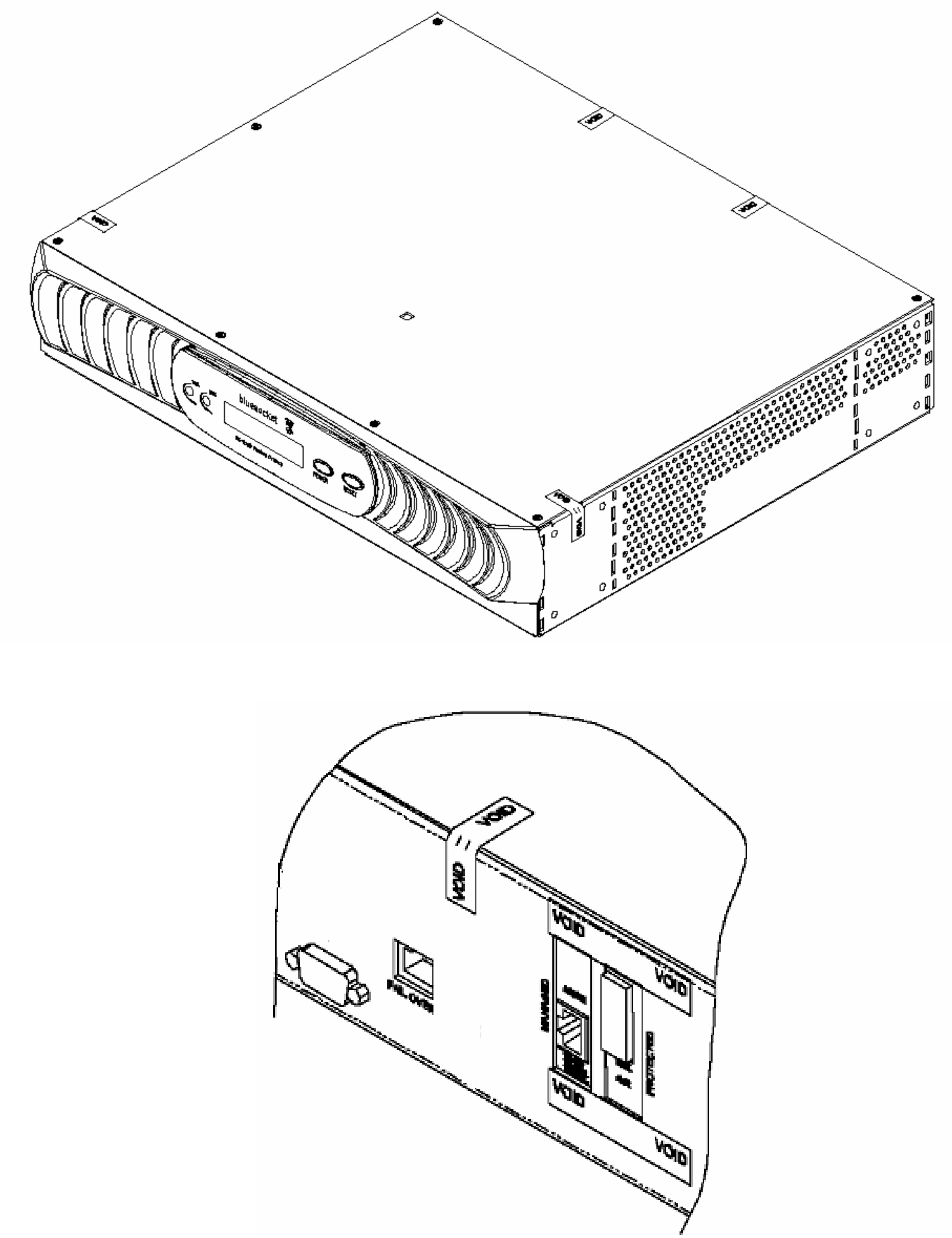

Figure 4: Location of the Tamper-evident Labels on the WG-5000 Case

3.2 Crypto-Officer Guidance

In addition to verifying the physical security of the WG-5000 (as described in Section 3.1), the Crypto-Officer is responsible for initialization of the module, configuration and management of the module, and termination (shutdown) of the module. Detailed information for the Local Crypto-Officer and Crypto-Officer services can be found in the *Bluesocket WG-5000 Wireless Gateway Crypto-Officer's Guide* and the *Bluesocket Wireless Gateway Setup and Administration Guide*.

3.2.1 Initialization

The operator(s) assuming the Crypto-Officer role receives the module from Bluesocket via a secure delivery mechanism. The Crypto-Officer can either pick the module up directly from a Bluesocket facility, or the module can be securely shipped to the Crypto-Officer using a bonded courier. The module is shipped in a box sealed with tape.

If the module is shipped to the Crypto-Officer, the Crypto-Officer should examine the box and tape used to seal the box for evidence of tampering. Additionally, the Crypto-Officer should carefully examine the shipping container containing the module for signs of tampering, which can include tears, scratches, and other irregularities in packaging.

Before the initial configuration of the module, there is no access control provided by the module. The Crypto-Officer must maintain control of the module and restrict any access to the module until configuration is completed and the module is fully initialized for FIPS 140-2-compliant operations.

Once the WG-5000 is unpacked, the Crypto-Officer must follow Bluesocket guidance for setting up the module. These steps include assuming the Crypto-Officer role to set the access control password for the module and configure the module's network settings.

After this process is complete, an operator can assume full Crypto-Officer responsibilities and begin managing the module via its HTML-based administrator interface and can configure it for use by Users.

3.2.2 Management

Once the initial configuration has been completed, the Crypto-Officer role is responsible for configuring the WG-5000 to operate in a FIPS 140-2-compliant mode by completing these steps:

1. Access the WG-5000 HTML-based administrator interface.
2. Verify that the FIPS 140-2-compliant system firmware image has been installed the WG-5000.
3. Disable the WG-5000 SSH capabilities.
4. Disable the WG-5000 PPTP capabilities.
5. Disable the WG-5000 L2TP capabilities.

6. Configure IPSEC to use only FIPS 140-2-compliant encryption algorithms (AES, DES (used for transitional phase only - valid until May 19, 2007), 3DES, or SHA-1).
7. Deactivate any IPSEC configurations using algorithms that are not FIPS 140-2-compliant.
8. Configure the WG-5000 such that plaintext data transfer through the module is not allowed.
9. Restart the WG-5000 to effect the configuration changes that have been made.

Refer to the *Bluesocket WG-5000 Wireless Gateway Crypto-Officer's Guide* for detailed procedures to complete the steps above.

Additionally, the Crypto-Officer is responsible for deletion of IPSec SAs for the Crypto-Officer and Users, changing the module's settings as appropriate, and monitoring the module's status logs. The Crypto-Officer is responsible for keeping track of the module, and this includes viewing the log entries for any suspicious activities.

The Crypto-Officer is required to routinely check the module's tamper-evident labels for signs of tampering. Such indications include warping or tearing, of the label. If strange activity or damage to labels is found, the Crypto-Officer should take the module offline and investigate.

If the module consistently malfunctions or otherwise repeatedly enters an error state, the manufacturer should be contacted.

3.2.3 Termination

When use of the WG-5000 has been completed, the Crypto-Officer should delete all IPSec SAs, and fully power down the module to delete all remaining keys in volatile memory.

3.3 User Guidance

The User accesses the module's User services as configured by the Crypto-Officer. The User should be careful not to provide his or her IPSec session keys or access passwords to other parties.

4 Acronym and Abbreviation List

Table 8 lists the acronyms and abbreviations are used in this document.

Table 8: Acronyms and Abbreviations Used in this Document

Acronym/Abbreviation	Definition
3DES	Triple DES (*see DES*)
API	Application Programming Interface
CA	Certification Authority
CO	Crypto Officer

Acronym/Abbreviation	Definition
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FSM	Finite State Machine
FTP	File Transfer Protocol
HMAC	Hashing Message Authentication Cryptography
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transmission Protocol, Secure
IKE	Internet Key Exchange
IPSec	IP Secure
KEK	Key Encryption Keys
LCD	Liquid Crystal Dial
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MD5	Message Digest Algorithm
NIST	National Institute of Standards and Technology
NTLM	NT LanMan
OS	Operating System
PC	Personal Computer
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
RSA Encryption	A public-key cryptosystem for both encryption and authentication
SHA-1	Secure Hash Algorithm
SSH	Secure SHell
SSL	Secure Sockets Layer
TLS	Transport Layer Security Protocol
VPN	Virtual Private Network