



*3e Technologies International, Inc.*  
**FIPS 140-2**  
**Non-Proprietary Security Policy**  
**Level 2 Validation**

**Version 2.0**

February 27, 2003

Copyright ©2003 by 3e Technologies International.  
This document may freely be reproduced and distributed in its entirety.



**GLOSSARY OF TERMS.....3**

**1. INTRODUCTION .....4**

1.1. PURPOSE .....4

1.2. DEFINITION .....4

1.3. SCOPE .....5

**2. ROLES, SERVICES, AND AUTHENTICATION .....5**

2.1.1. *Roles and Services* .....5

2.1.2. *Authentication Mechanisms and Strength*.....9

**3. SECURE OPERATION AND SECURITY RULES .....10**

3.1. SECURITY RULES .....10

3.2. PHYSICAL SECURITY RULES .....10

3.3. SECURE OPERATION INITIALIZATION .....14

3.3.1. *System Configuration*.....15

3.3.2. *Wireless Configuration*.....17

3.3.3. *Services Settings* .....19

3.3.4. *Firewall*.....19

3.3.5. *User Management*.....21

3.3.6. *System Administration* .....22

**4. SECURITY RELEVANT DATA ITEMS.....24**

4.1. CRYPTOGRAPHIC ALGORITHMS .....24

4.2. CRYPTOGRAPHIC KEYS AND SRDIS .....24

4.3. ACCESS CONTROL POLICY.....25

## **Glossary of terms**

<b>AP</b>	Access Point
<b>CO</b>	Cryptographic Officer
<b>DH</b>	Diffie Hellman
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMG</b>	Dual Mode Gateway
<b>DMZ</b>	De-Militarized Zone
<b>IP</b>	Internet Protocol
<b>EAP</b>	Extensible Authentication Protocol
<b>FIPS</b>	Federal Information Processing Standard
<b>HTTPS</b>	Secure Hyper Text Transport Protocol
<b>LAN</b>	Local Area Network
<b>MAC</b>	Medium Access Control
<b>NAT</b>	Network Address Translation
<b>PRNG</b>	Pseudo Random Number Generator
<b>RSA</b>	Rivest, Shamir, Adleman
<b>SHA</b>	Secure Hash Algorithm
<b>SRDI</b>	Security Relevant Data Item
<b>SSID</b>	Service Set Identifier
<b>TLS</b>	Transport Layer Security
<b>WAN</b>	Wide Area Network
<b>WLAN</b>	Wireless Local Area Network

## 1. Introduction

### 1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International 's wireless gateway products, the *3e-521NP*, *3e-522FIPS* and *3e-530NP Wireless Gateways* (HW P/Ns 3e-521NP, 3e-522FIPS and 3e-530NP, FW Version 2.0), hereafter known as the 3e-DMG (Dual Mode Gateway). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This document defines 3eTI's security policy and explains how the 3e-DMG Wireless Gateways meet the FIPS 140-2 security requirements.

The figures below show the 3e-521NP and 3e-522FIPS Gateways. The 521NP and 530NP look identical and so only one picture is included.



Figure A 3e 521NP Gateway

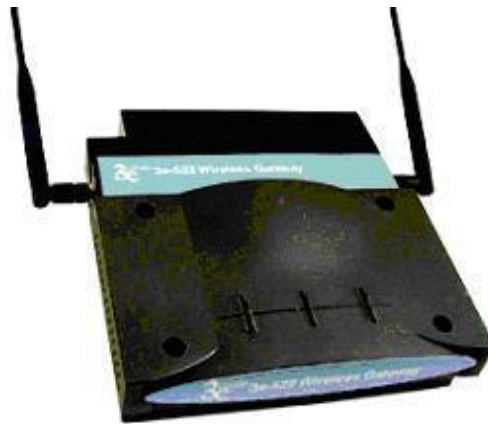


Figure B 3e-522FIPS Gateway

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at <http://csrc.nist.gov/cryptval/>.

### 1.2. Definition

The 3e-DMG Wireless Gateway is a device which consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-DMG gateway operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-DMG Gateway is defined to be the entire enclosure of the Gateway. The 3e-DMG is physically bound by the mechanical enclosure which is protected by tamper evident tape.

3eTI Gateway software provides the following major services:

- Wireless 802.11b Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11b Gateway Network Address Translation (NAT) routing functionality (routing from the uplink LAN to the wireless LAN).
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface. In Gateway mode, the local LAN includes the wireless LAN. In Access Point mode, only the local wired LAN includes DHCP service).

The only difference between the 3e-521NP and 3e-530NP is the outer enclosure of the gateway. The 3e-521NP uses a steel enclosure and the 3e-530NP employs an aluminum enclosure.

### ***1.3. Scope***

This document will cover the secure operation of the 3e-DMG including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

## **2. Roles, Services, and Authentication**

The 3e-DMG supports four separate roles. The set of services available to each role is defined in this section. The 3e-DMG authenticates an operator's role by verifying his PIN or access to a shared secret.

### **2.1.1. Roles and Services**

The 3eTI gateway supports the following authorized roles for operators:

*Crypto Officer Role:* The Crypto officer role performs all security functions provided by the Gateway. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, and audit functions). The Crypto officer is also responsible for managing the Administrator users and configuring the Gateway firewall rules. The Crypto officer must operate within the Security Rules and Physical Security Rules specified in Sections 3.1 and 3.2. The Crypto officer uses a secure web-based HTTPS connection to configure the Gateway. Only one Crypto Officer is defined in the Gateway. The Crypto Officer authenticates to the Gateway using a username and password.

The following functionalities are provided to the Crypto Officer role.

	Features	Access Point						Gateway					
		Show <sup>1</sup>	Set <sup>2</sup>	Add <sup>3</sup>	Delete <sup>4</sup>	Zeroize <sup>5</sup>	Default Reset <sup>6</sup>	Show	Set	Add	Delete	Zeroize	Default Reset
<b>System Configuration</b>													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
• LAN	IP address/Subnet mask	X	X				X	X	X				X
• Operating Mode	Gateway/AP mode	X	X				X	X	X				X
<b>Wireless Configuration</b>													
• General	MAC address, SSID, Channel No.	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X	X	X				X
	3DES	X	X			X	X	X	X			X	X
	AES (128-/192-256-bit)	X	X			X	X	X	X			X	X
• MAC Address Filtering	Enable/Disable, Add/Delete entry	X	X	X	X		X	X	X	X	X		X
• Misc. Settings		X	X				X	X	X				X
<b>Service Settings</b>													
• DHCP Server	Enable/Disable												
	Starting/Ending IP address						NA	X	X		X		X
								X	X				X
<b>Firewall</b>													
• Content Filtering								X	X	X	X		X
• IP Filtering								X	X	X	X		X
• Port Filtering								X	X	X	X		X
• Virtual Server								X	X	X	X		X
• DMZ								X	X				X
<b>User Management</b>													
• List All Users		X	X	X	X		X	X	X	X	X		X
• Add New User		X	X	X	X		X	X	X	X	X		X
<b>Monitoring/Reports</b>													
• Web Logging		X					X	X					X
• Wireless	Client Info (IP address, MAC address, Signal strength, channel number, and bandwidth usage)	X					X	X					X
• Device Status	MAC address,	X					X	X					X

<sup>1</sup> The operator can view this setting

<sup>2</sup> The operator can change this setting

<sup>3</sup> The operator can add a required input. For example: Adding an entry to the MAC address filtering table

<sup>4</sup> The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table

<sup>5</sup> The operator can zeroize these keys.

<sup>6</sup> The operator can reset this setting to its factory default value. This is done by performing a zeroize



	WAN IP address, Subnet mask, Default gateway	X					X	X					X
	LAN IP address, Subnet mask, Default gateway	X					X	X					X
• Routing Table		X					X	X					X
<b>System Administration</b>													
• Firmware Upgrade			X				X		X				X
• Restore Defaults			X				X		X				X
• Zeroize			X						X				
• Reboot			X						X				
• Self-Test		X	X					X	X				

*Administrator Role:* This role performs general Gateway configuration such as defining firewall rules, defining the WLAN, LAN and DHCP settings, performing self-tests and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator can also reboot the Gateway if deemed necessary.

The Administrator must operate within the Security Rules a specified in Section 3.1 and always uses a secure web-based HTTPS connection to configure the Gateway. The Administrator authenticates to the Gateway using a username and password. Up to 5 operators who can assume the Administrator role can be defined. All Administrators are identical i.e. they have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The following functionalities are provided to the Administrator role.

	Features	Access Point						Gateway					
		Show	Set	Add	Delete	Zeroize	Default Reset	Show	Set	Add	Delete	Zeroize	Default Reset
<b>System Configuration</b>													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
• LAN	IP address/Subnet mask	X	X				X	X	X				X
• Operating Mode	Gateway/AP mode	X	X				X	X	X				X
<b>Wireless Configuration</b>													
• General	MAC address, SSID, Channel No.	X	X				X	X	X				X
• Encryption	No Encryption	X					X	X					X



	3DES	X						X	X						X	
	AES (128-/192-256-bit)	X						X	X						X	
•	MAC Address Filtering	Enable/Disable, Add/Delete entry	X					X	X						X	
•	Misc. Settings		X	X				X	X	X					X	
<b>Service Settings</b>																
•	DHCP Server	Enable/Disable Starting/Ending IP address	NA						X	X		X				X
			NA						X	X						X
<b>Firewall</b>			NA													
•	Content Filtering		NA						X	X	X	X				X
•	IP Filtering		NA						X	X	X	X				X
•	Port Filtering		NA						X	X	X	X				X
•	Virtual Server		NA						X	X	X	X				X
•	DMZ		NA						X	X						X
<b>User Management</b>																
•	List All Users		X					X	X						X	
•	Add New User							X							X	
<b>Monitoring/Reports</b>																
•	Web Logging		X					X	X						X	
•	Wireless	Client Info (IP address, MAC address, Signal strength, channel number, and bandwidth usage)	X					X	X						X	
•	Device Status	MAC address,	X					X	X						X	
		WAN IP address, Subnet mask,	X					X	X						X	
		Default gateway														
		LAN IP address, Subnet mask,	X					X	X						X	
		Default gateway														
•	Routing Table		X					X	X						X	
<b>System Administration</b>																
•	Firmware Upgrade															
•	Restore Defaults															
•	Zeroize															
•	Reboot			X						X						
•	Self-Test		X	X						X	X					

*User Role:* This role is assumed by the wireless client workstation that uses static or dynamic key AES or 3DES encryption to communicate wirelessly with the Gateway AP. Authentication is implicitly selected by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed and the client uses its public key certificate to authenticate itself. The static key (TDES or AES key) is configured on the Gateway by the Crypto officer. The static key must be pre-shared between the Gateway and User. The Gateway supports 128 Users (client workstations) if MAC address filtering is disabled. If MAC address filtering is enabled, only 60 Users are allowed.

The only service available to the User role is the ability to send data to and through the 3e-DMG. All data is sent in the form of 802.11b wireless packets. All wireless communication is encrypted using either 3DES or AES encryption (based upon Gateway configuration). In bypass mode plaintext packets can also be sent to the Gateway



*Security Server Role:* This role is assumed by the authentication server, which is a self-contained workstation connected to the Gateway over the Ethernet Uplink WAN port. The security server is employed for authentication of wireless clients and key management activities. The Security Server is used only during dynamic key exchange. The Security Server authenticates using a shared secret which is used as an HMAC-SHA1 key to sign messages sent to the Gateway during dynamic key exchange. The Security Server IP address and password are configured on the Gateway by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

- a) Authenticate wireless clients for the Gateway
- b) Perform a DH key exchange with the Gateway to negotiate an AES key
- c) Send unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

**2.1.2. Authentication Mechanisms and Strength**

The following table summarizes the four roles and the type of authentication supported for each role:

<b>Role</b>	<b>Type of Authentication</b>	<b>Authentication Data</b>
Crypto Officer	Identity-based	Userid and password
Administrator	Identity-based	Userid and password
User	Role-based	Static Key (TDES or AES)
User	Role-based	CA signature
User	Role-based	MAC address and CRC
Security Server	Role-based	HMAC SHA1 (Shared secret)

The following table identifies the strength of authentication for each authentication mechanism supported:

<b>Authentication Mechanism</b>	<b>Strength of Mechanism</b>
Userid and password	Minimum 6 characters => $72^6 = 1.39E11$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 6 characters => $72^6 = 1.39E11$
CA signature	128-bit
MAC address (6 bytes) and CRC (4 bytes)	10 bytes (80-bits).

### 3. Secure Operation and Security Rules

In order to operate the 3e-DMG securely, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

#### 3.1. Security Rules

The following 3e-DMG security rules must be followed by the operator in order to ensure secure operation:

1. Every operator (Crypto Officer or Administrator) has a user-id on the 3e-DMG. No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 3e-DMG with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-DMG with any other operator or entity.
4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-DMG.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the Gateway.
6. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. A compromised tape reveals message “OPENED” with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
7. The Crypto Officer should change the default password when configuring the Gateway for the first time. The default password should not be used.

#### 3.2. Physical Security Rules

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the Gateway enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

**Tools:**

Wire Cutters (wire seal removal)

**Materials:**

Gateway, 3eTI – Quantity: 1

Seal, Tape, Tamper-evident – Quantity: 3

Isopropyl Alcohol Swab

3M Adhesive Remover (citrus or petroleum based solvent)

#### Installation – Tamper-evident tape

1. Locate on Gateway the placement locations of tamper-evident tape seals. (3 locations as shown in Figure 1, 2, and 3 for the 3e-521NP and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522FIPS).
2. Thoroughly clean area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 3e-521NP and 3e-530NP Gateways as shown in Figures 1, 2, and 3. For the 3e-522FIPS Gateway seals must be applied as shown in Figures 4, 5, and 6. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the Gateway, apply pressure to verify that adequate adhesion has taken place.

### Removal – Tamper-evident tape

1. Locate on Gateway locations of tamper-evident tape seals. (3 locations as shown in Figures 1, 2, and 3 for the 3e-521NP and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522FIPS)
2. Record tracking numbers from existing tamper-evident tape seal and verify physical condition as not tampered or destroyed after installation.
3. Cut tape along seam of Gateway to allow opening of enclosure.
4. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (three locations as shown in Figures 1, 2, and 3 for the 3e-521NP and 3e-530NP and 4 locations as shown in Figures 4, 5, and 6 for the 3e-522NP)

This picture shows the physical interface side of the 3e-521NP and 3e-530NP Gateway enclosure with tamper-evident seal.



Figure 1

Side-view of the 3e-521NP and 3e-530NP Gateway with tamper-evident seal:



Figure 2

End-view of the 3e-521NP and 3e-530NP Gateway showing WLAN port and tamper-evident seal:

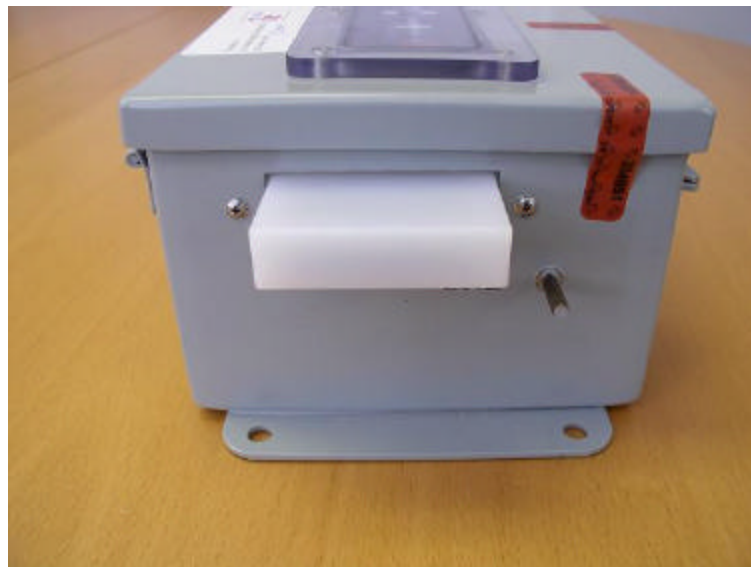


Figure 3

This picture shows the bottom view of the 3e-522FIPS Gateway, with tamper-evident tape covering the wall-hanging openings to prevent access to any internal circuitry.



**Figure 4**

This picture shows the top right side of the 3e-522FIPS Gateway with tamper-evident tape securing the outer enclosure.



**Figure 5**

This picture shows the top left side of the 3e-522FIPS Gateway with tamper-evident tape securing the outer enclosure.



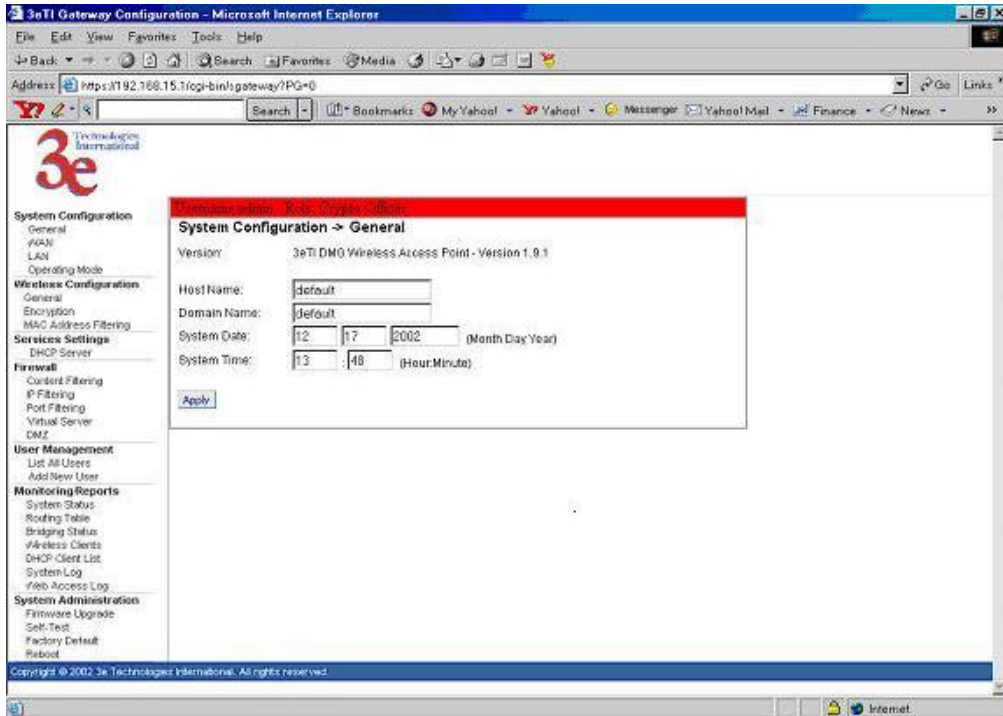
Figure 6

### ***3.3. Secure Operation Initialization***

There is a default Crypto Officer password which can be used to access the configuration pages using HTTPS from any browser. The LAN port by default is configured with the IP address 192.168.15.1.

Using any browser, open the page <https://192.168.15.1> to access the Gateway configuration.

The main configuration page is shown below:



### 3.3.1. System Configuration

#### 3.3.1.1. WAN Configuration

The IP address of the WAN interface can be configured with Static IP address or by using DHCP to obtain an IP address.



Username: admin Role: Crypto Officer

**System Configuration -> WAN**

Using DHCP to get an IP address

IP Address: 192.168.204.149  
 Subnet Mask: 255.255.255.0  
 Default Gateway: 192.168.204.1  
 DNS 1: 192.168.202.10  
 DNS 2:

Specify a static IP address

IP Address:      
 Subnet Mask:      
 Default Gateway:      
 DNS 1:      
 DNS 2:

### 3.3.1.2. LAN Configuration

The IP address of the LAN interface can be configured with a static IP address, by using the link under System Configuration.

Username: admin Role: Crypto Officer


**System Configuration -> LAN**

IP Address: 192.168.15.1

### 3.3.1.3. Operating Mode

The gateway can be configured in *Gateway* or *Wireless Access Point mode* by using the Operating Mode link. It is important to note that the unit will be reset to factory default when the Operating mode is changed.





Username admin Role: Crypto Officer

**System Configuration → Operating Mode**

Gateway Mode  
 Wireless Access Point Mode

Apply

### 3.3.2. Wireless Configuration

#### 3.3.2.1. General

This screen can be used to configure the SSID and the channel number.



Username admin Role: Crypto Officer

**Wireless Configuratoion → General**

MAC Address: 00:02:78:E1:17:35

SSID:

Channel No:

Apply

#### 3.3.2.2. Encryption

##### No Data Encryption

Factory default sets the encryption to “*No Data Encryption*”. This results in all wireless traffic being sent in plaintext form.

##### Dynamic Key Management

Using this configuration, the Crypto Officer can set per session keys dynamically.

The configuration entails the following:

##### **Gateway Configuration:**

- Configure the IP address of the radius server in the *Security Server IP Address* box.
- Configure the Radius Server password.
- Select the type of key. The options available are:

- AES 128-bit key
- AES 192-bit key
- AES 256-bit key
- 3DES key

### **Static 3DES Key**

The Crypto Officer can also use static 3DES key to associate with the Gateway/Access Point.

### **Static AES Key**

The Crypto Officer can also use static AES keys to associate with the Gateway/Access Point. The following AES keys can be configured:

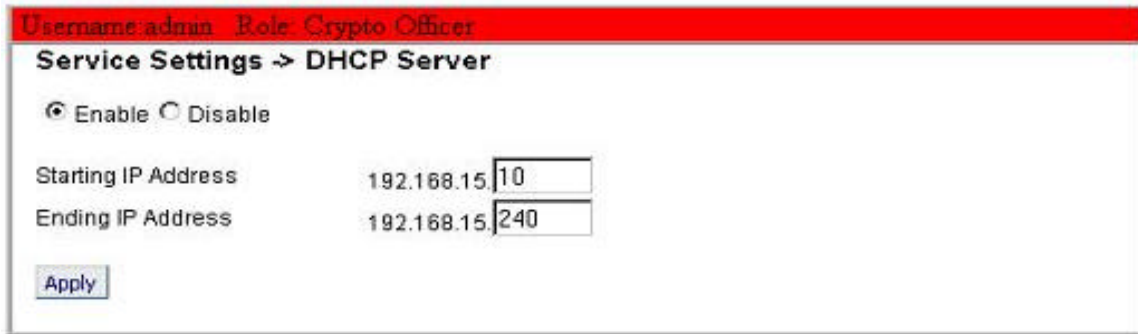
- AES 128-bit key
- AES 192-bit key
- AES 256-bit key

The screenshot shows a web interface for configuring encryption. At the top, a red header bar displays 'Username: admin Role: Crypto Officer'. Below this, the page title is 'Wireless Configuration -> Encryption'. There are three main radio button options: 'Off - No Data Encryption' (which is selected), 'Dynamic Key Management', and 'Static 3DES Key / Open System Authentication'. The 'Dynamic Key Management' section includes fields for 'Security Server IP Address', 'Password', and a 'Key Type' dropdown menu currently set to '128-bit AES key'. The 'Static 3DES Key / Open System Authentication' section has a note 'Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F)' and two input fields labeled '192-bit Key' and 'Type again'. The 'Static AES Key / Open System Authentication' section has three radio button options: '128-bit', '192-bit', and '256-bit', each followed by a 'Type again' label and an input field. An 'Apply' button is located at the bottom left of the form area.

### 3.3.3. Services Settings

Using this link, the DHCP server for the LAN port can be configured.

- The DHCP server can be enabled or disabled.
- The IP address range can be configured.



### 3.3.4. Firewall

This option is valid only in Gateway mode. The following options can be configured:

- Content Filtering
- IP Filtering
- Port Filtering
- Virtual Server
- Demilitarized Zone (DMZ)

#### 3.3.4.1. Content Filtering

Using this filter, any IP address or hostname can be filtered.

Username admin Role Crypto Officer

**Firewall -> Content Filtering**

**Add IP Address or Hostname**

IP Address or Hostname:

IP Address or Hostname List

1. www.google.com

---

2. www.cnn.com

---

### 3.3.4.2. IP Filtering

This feature restricts clients to those with specific IP address to connect to the Gateway.

Username admin Role Crypto Officer

**Firewall -> IP Filtering**

**Add IP Address**

IP Address

Private IP Address List

1. 216.239.37.101

---

2. 64.236.16.116

---

### 3.3.4.3. Virtual Server

The port range and a choice of protocols (TCP, UDP, or BOTH) along with the IP address can be entered. These parameters allow access through the firewall to the port range at the IP address specified.

Username admin Role: Crypto Officer

Port Range: [ ] ~ [ ] Protocol: BOTH IP Address: [ ] . [ ] . [ ] . [ ] Add

Port ranges	Protocol	IPs	
23~23	TCP	192.168.15.10	Del
80~80	TCP	192.168.15.11	Del

### 3.3.4.4. Demilitarized Zone (DMZ)

The DMZ allows the entire machine (all ports) to be accessed through the firewall at the IP address specified.

Username admin Role: Crypto Officer

Demilitarized Zone (DMZ)  Enable  Disable

DMZ IP Address: [192] . [168] . [15] . [12]

Apply

### 3.3.5. User Management

#### 3.3.5.1. List All Users

A list of the Crypto Officer and Administrator(s) by user ID is included.

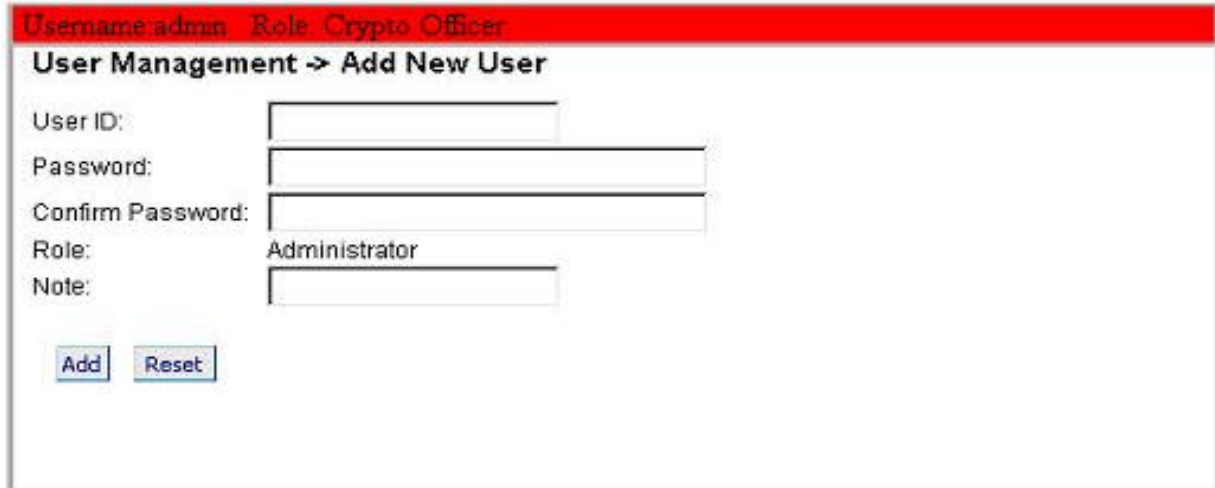
Username admin Role: Crypto Officer

User Management -> List All Users

User ID	Role	Note	
admin	Crypto Officer	my change	Edit Delete

### 3.3.5.2. Add New User

Only Crypto Officer is able to add a new user (Administrator) to the Gateway.



Username: admin Role: Crypto Officer

**User Management -> Add New User**

User ID:

Password:

Confirm Password:

Role: Administrator

Note:

### 3.3.6. System Administration

#### 3.3.6.1. Firmware Upgrade

Only the Crypto Officer can select a file to upload for firmware upgrade.



Username: admin Role: Crypto Officer

**System Administration -> Firmware Upgrade**

Click 'Browse' and select a file:

#### 3.3.6.2. Self-Tests

Both Crypto Officer and Administrators can initiate the self-test suite.

The test takes few seconds to complete. A beep will be heard at the end of the test and the result will be displayed. The self-test suite covers AES, 3DES, SHA-1, HMAC SHA-1, PRNG, Diffie Hellman for Dynamic Key Exchange, RSA decryption and SHA1 algorithm for firmware integrity test.

Username: admin Role: Crypto Officer

**System Administration - Self Test**

Click 'Start Test' button to start the self test.

### 3.3.6.3. Factory Default

Only the Crypto Officer can restore the Gateway to the factory default settings. For the 3e-522FIPS Gateway a Reset switch is provided on the back chassis that achieves the same goal. When this switch is depressed for 10 seconds or longer it resets the module back to factory default settings.

Username: admin Role: Crypto Officer

**System Administration - Factory Default**

Click 'Restore' button to reset factory default.

### 3.3.6.4. Reboot

Both Crypto Officer and Administrators can reboot the Gateway.

Username: admin Role: Crypto Officer

**System Administration → Reboot**

Click 'Reboot' button to reboot Gateway device.

## 4. Security Relevant Data Items

This section specifies the 3e-DMG’s Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-DMG.

### 4.1. Cryptographic Algorithms

The 3e-DMG supports the following FIPS Approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysizes)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- SHA-1
- HMAC-SHA1

The 3e-DMG also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman key agreement (1024-bit modulus)
- RSA decrypt (PKCS#1) for key un-wrapping.

### 4.2. Cryptographic Keys and SRDIs

The 3e-DMG contains the following security relevant data items:

Security Relevant Data Items	SRDI Description
AES or 3DES Static Key	Data encryption/decryption using an AES static key (128, 192, or 256-bits) or 3DES static key (192-bits)
AES or 3DES Dynamic Broadcast Key	Data encryption/decryption using an internally generated AES key (128, 192, or 256-bits) or 3DES (192-bits)
AES or 3DES Dynamic Unicast Key	Data encryption/decryption using an dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)
AES Internal Key	Used to encrypt configuration file
AES Post-Authentication Key	AES Key used to decrypt the 3DES/AES Dynamic Unicast Key
HMAC SHA-1 Key	Key used to verify firmware integrity and authenticity during firmware upgrade
HMAC SHA-1 Shared Secret	Secret used to authenticate the Security Server
TLS Session Key	TDES key used to encrypt/decrypt configuration sessions (via HTTPS)
RSA Private Key	Used to decrypt pre-master key in TLS negotiation
TDES Key	Used to encrypt private key file
Crypto-officer password	CO Password
Administrator password	Administrator Password



### 4.3. Access Control Policy

The 3e-DMG maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read ( R ), write ( W ), execute ( E ). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e-DMG SRDI Roles and Services Access Policy	Security Relevant Data Item	AES or TDES Static Key	AES or TDES Dynamic Broadcast	AES or TDES Dynamic Unicast	AES Internal Key	AES Post-authentication Key	HMAC SHA-1 Key	HMAC SHA-1 Shared Secret	TLS Session Key	RSA Private Key	TDES Key	CO Password	Administrator Password
	Role/Service												
Crypto-officer Role													
System Configuration					E				E	E	E		
Wireless Configuration		W			E			W	E	E	E		
Service Settings					E				E	E			
Firewall					E				E	E			
User Management									E	E		W	W
Monitoring/Reporting					E				E	E			
System Administration					E		E		E	E			
Administrator Role													
System Configuration					E				E	E			
Wireless Configuration					E				E	E			
Service Settings					E				E	E			
Firewall					E				E	E			
User Management									E	E			W
Monitoring/Reporting					E				E	E			
System Administration					E				E	E			
User Role													



Sending data		E	E	E										
Authentication Server Role														
Provides authentication				W		W		E						