# Security Gateway SG1000 Cryptographic Module
# Security Policy
Document Version 1.2

*Meru Networks*

Revision Date: June 24, 2009

**TABLE OF CONTENTS**

# Module Overview

Meru Networks Security Gateway Cryptographic Module is a high performance purpose built security solution for Wireless LAN deployments. The Security Gateway Cryptographic Module provides a FIPS 140-2 Level 3 security solution conforming to the IEEE 802.11i security standards. The Security Gateway Cryptographic Module is installed in a slot in the Meru Networks Security Gateway SG1000 appliance.

The Meru Networks Security Gateway Cryptographic Module is a key component of the Meru Wireless LAN System and along with Meru Access Points and Meru Wireless LAN Controllers delivers unsurpassed performance for secure Wi-Fi traffic. Representing a shift to the fourth generation WLAN architecture using coordinated, intelligent Access Points at the edge, the Meru System Director OS delivers the only Wi-Fi certified infrastructure that handles toll-quality wireless VoIP and high-capacity data on a single infrastructure with no compromises.

The Meru Networks Security Gateway Cryptographic module is a hardware/firmware, multi-chip embedded cryptographic module. The Security Gateway Cryptographic module implements the authentication and encryption/decryption functionality conforming to the IEEE 802.11i standards to provide data security for the Wireless LAN. The Security Gateway Cryptographic module can be administered over a serial console and remotely over a secure network connection to the Cryptographic module. The Security Gateway Cryptographic module is encapsulated in a epoxy enclosure. The epoxy enclosure is the physical boundary of the Security Gateway Cryptographic module.

The Security Gateway Cryptographic module is built with the Security Gateway Cryptographic Card Rev_A and runs the Security Gateway v1.0-27 firmware.

# Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

**Table 1 – Module Security Level Specification**

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 3 |
| Module Ports and Interfaces | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 3 |
| Physical Security | 3 |
| Operational Environment | N/A |
| Cryptographic Key Management | 3 |
| EMI/EMC | 3 |

| | |
|---|---|
| Self-Tests | 3 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

# Modes of Operation

***Approved mode of operation***

The cryptographic module supports the following FIPS Approved algorithms:

- RSA with 1024/2048/4096 bit keys for digital signature verification.
- RSA with 1024 bit keys for digital signature generation
- Triple-DES (three key) for encrypt/decrypt
- SHA-1 for hashing
- HMAC-SHA1 for generating MACs
- AES 128 (CCMP) for encrypt/decrypt
- AES 128 (CBC mode) for encrypt/decrypt
- AES 256 (CBC mode) for encrypt/decrypt
- AES 128 (ECB mode) for AES Key Wrap

The Security Gateway Cryptographic module also supports the commercially available EAP-TLS and SSHv2 (using Diffie-Hellman) protocol for key establishment to provide a secure channel. The module's Diffie-Hellman implementation also conforms to the requirements set forth in FIPS SP800-56A.

The Security Gateway Cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31 Appendix A.2.4 for key generation. The module also relies on a hardware NDRNG for seeding material for the DRNG.

The Security Gateway Cryptographic module supports the following non FIPS Approved algorithms:

- MD5 in EAP-TLS as required by the TLS specification

The Security Gateway Cryptographic module operates in FIPS mode. The user can confirm the cryptographic module's mode via execution of the "show security-gateway" service through the command line interface (CLI).

# Physical Description

### *Dimensions*

The Meru Networks Security Gateway Cryptographic module has the following physical dimensions:

- Epoxy enclosure containing the cryptographic module

- Size:
  - Width: 6.69”
  - Length: 4.51”
  - Height: 1.90”
- Maximum Weight: 7.14 lb

## Cryptographic Module Boundaries

For FIPS 140-2 Level 3 validation, the Meru Networks Security Gateway Cryptographic module has been validated as a multi-chip embedded cryptographic module. The epoxy enclosure physically encompasses the complete set of hardware and software components and represents the cryptographic boundary of the gateway. The cryptographic boundary is defined as the epoxy enclosure containing the hardware and software components.

## Interfaces

The module supports the following physical interfaces:

| Physical Port | Pins Used | Logical Interface |
|---|---|---|
| Gigabit Ethernet (4) | RJ45<br>Transmit/Receive bidirectional pairs: Pins (1,2), (3,6), (4,5), (7,8) | Control Input, Status Output<br>Data Input, Data Output |
| Serial | DB9 | Control Input, Status Output |

All control input and status output over the Gigabit Ethernet ports is encrypted with Triple-DES or AES-128/256 within the SSHv2 session. An SSHv2 encrypted session over the Gigabit Ethernet is used to input all the CSPs into the cryptographic module. The Gigabit Ethernet ports only transmit/receive encrypted data from the wireless client users.

The Serial interface control input and status output is in the clear but is not used to input or output any CSPs.

The PCI interface on the cryptographic module is disabled.

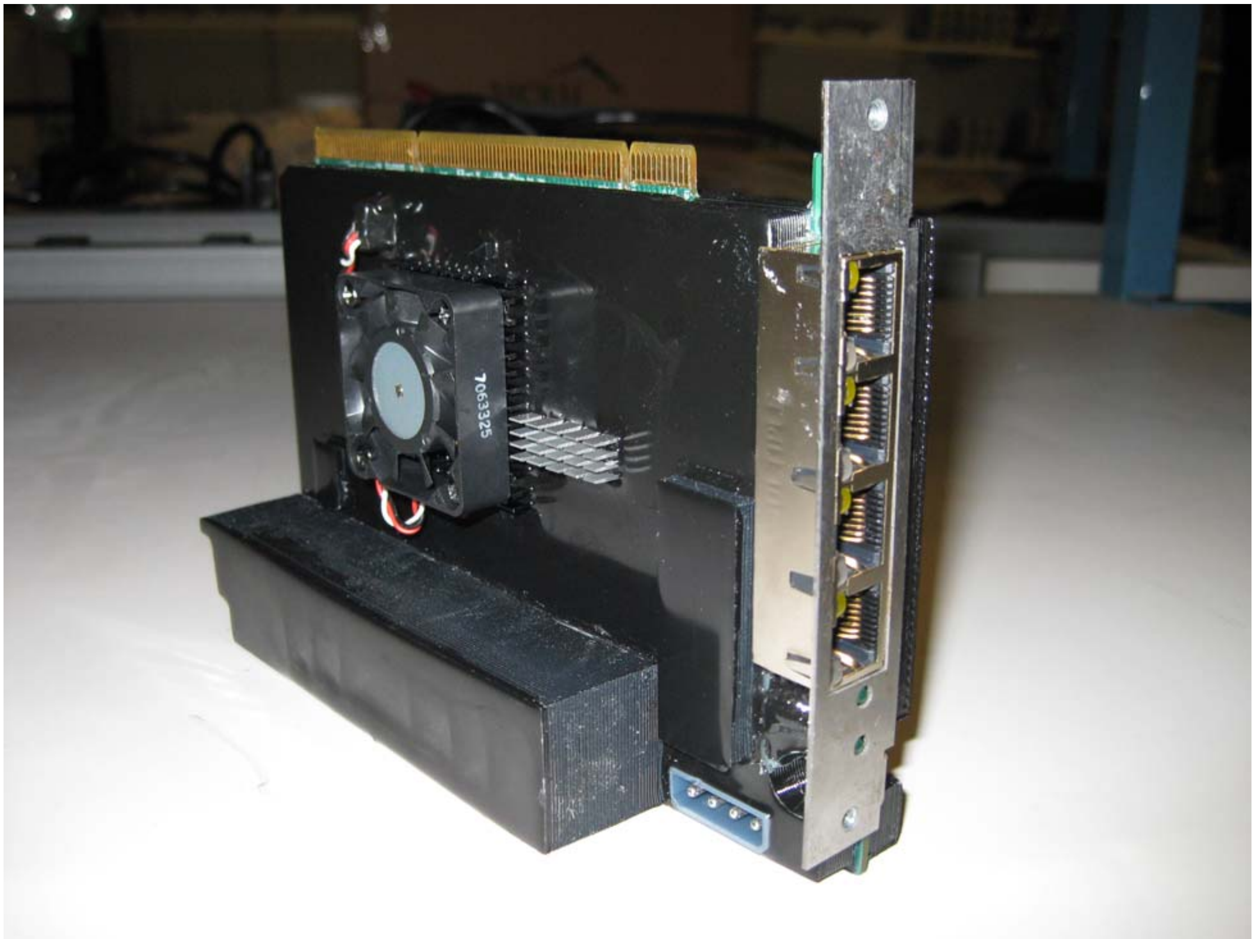
## Power Interface

The module is DC powered with a 4-pin ATX Molex Connector with pin assignment of pin 1, 12V DC, pin 2 and pin 3, Ground, pin 4, 5V.

## Physical Security

The module’s cryptographic boundary is defined to be the outer perimeter of the epoxy enclosure containing the hardware and software components. The module is opaque and completely conceals the internal components of the cryptographic module. The epoxy enclosure of the module prevents physical access to any of the internal components without having to destroy the module.

**Figure 1 – Image of Security Gateway SG1000Cryptographic Module**



## Identification and Authentication Policy

### *Assumption of roles*

The cryptographic module shall support three distinct operator roles CSO Administrator, Non-CSO Administrator and Client User. The cryptographic module shall enforce the separation of roles through different established CLI sessions or Client User Sessions. CLI sessions are setup over an SSHv2 tunnel and are authenticated with a username/password. Client User sessions are established via EAP-TLS negotiation and are authenticated with a Client Certificate.

**Table 2 – Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| CSO Administrator | Identity-based Authentication | Username/Password |
| Non-CSO Administrator | Identity-based Authentication | Username/Password |
| Client User | Identity-based Authentication | EAP-TLS Client Certificate (1024/2048/4096-bit RSA) |

**Table 3 – Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| Username and Password | Passwords are at least 6 characters long, with 95 characters available. Therefore, the probability that a random attempt will succeed or a false acceptance will occur is 1/735,091,890,625 which is less than 1/1,000,000.<br>To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 7350919 (122515 per second) attempts would have to be executed. The Security Gateway Cryptographic module limits the number of sessions that can be established to meet this requirement. |
| EAP-TLS Client Certificate (1024/2048/4096-bit RSA) | 1024-bit RSA keys are roughly equivalent to 80-bit symmetric keys. The probability that a random attempt will succeed or a false acceptance will occur is ½^80 which is less than 1/1,000,000.<br>To exceed 1 in 100,000 probability of a successful random attempt in a 1-minute period, more than 2^63 attempts would have to be executed which is beyond the capacity of the Security Gateway Cryptographic module. |

# Access Control Policy

The Security Gateway Cryptographic module supports identity-based authentication. There are three main roles in the cryptographic module that operators may assume: a CSO Administrator role, Non-CSO Administrator role and a Client User role. The CSO Administrator maps to the Crypto Officer role and can configure all the parameters including the CSPs on the cryptographic module. The Non-CSO Administrator has access only to commands that don’t operate on the CSPs on the cryptographic module. The Client Users map to the User role accessing the user data encryption/decryption service of the cryptographic module.

### *CSO Administrator Role*

The CSO administrator establishes a CLI session to configure and monitor the Security Gateway Cryptographic module. The CSO administrator is authenticated via username/password combination through a valid SSHv2 tunnel to setup the CLI session. The CSO administrator has access to all the configuration parameters including the CSPs. The CSO administrator can establish the CLI session over the serial console authenticating via username/password. However the CSO administrator doesn’t have access to commands that operate on the CSPs over the serial console CLI session. The following table is a list of services available to the CSO administrator over an SSHv2 tunnel. In addition to these the CSO administrator can access all the services listed for the Non-CSO administrator role in the next section. The CSO administrator has access only to the Non-CSO administrator role services over the serial console CLI session.

| Service | Description | Input | Output | CSP Access |
|---|---|---|---|---|
| Setup | Initializes the network configuration, date information, Master key and SSHv2 Host key pair | Command, IP address, date | Status of command | Master key, SSHv2 Host Private Key, SSHv2 Host Public Key |
| Import Server Certificate and Private Key | Allows the administrator to update the Server’s Private Key and Server’s Certificate. The key pair is input over the SSHv2 tunnel or through SCP. | Command, PEM or PKCS12 file containing the server certificate and private key. | Status of command | Server Private Key, Server Public Key |
| Import Signing Certificate | Allows the administrator to update the Signing certificate used to validate client certificates. | Command, PEM file containing the Signing certificate. | Status of command | Server Signing Certificate |
| Provisioning Administrator Accounts | Allows the administrator to manage CSO, Non-CSO administrator accounts | Command, username, password | Status of command | Administrator password |

| | | | | |
|---|---|---|---|---|
| Radius User Commands | Allows the administrator to configure Client User Allow/Deny list | Command, Client User Common Name | Status of command | None |
| Delete | Allows the administrator to delete certificates, administrators and remove client users from allow/deny list | Command | Status of command | Server Private Key, Server Public Key, Server Signing Certificate, Administrator password |
| Show certificates | Allows the administrator to view the configured certificates | Command | Certificate details | Server Public Key, Server Signing Certificate |
| Zeroize | Zeroizes the Master Key, deletes the Server Certificate/Private Key, Server Signing Certificate, SSHv2 Host Key pair and reboots to clear all volatile SDRAM. | Command | Status of command, Reboot progress | Master Key, Server Private Key, Server Public Key, Server Signing Certificate, SSHv2 Host Private Key, SSHv2 Host Public Key |
| Reload Default Settings | Clears all the configured information including the CSPs and restores the cryptographic module to the factory state | Command | Status of command, Reboot progress | Master Key, Server Private Key, Server Public Key, Server Signing Certificate, SSHv2 Host Private Key, SSHv2 Host Public Key |
| Initiate Self Tests | Allows the administrator to invoke self-tests through the CLI | Command | Status of each of the self tests | None |
| Upgrade Firmware/Software | Allows the administrator to load authenticated images into the module | Command, upgrade image file path | Status of command | SW/Firmware Validation Key |

### *Non-CSO Administrator Role*

The Non-CSO administrator establishes a CLI session to configure and monitor the Security Gateway Cryptographic module. The Non-CSO administrator is authenticated via username/password combination through a valid SSHv2 tunnel to setup the CLI session. The Non-CSO administrator doesn't have access to any of the services that operate on the CSPs. The following table is a list of services available to the Non-CSO administrator.

| Service | Description | Input | Output | CSP Access |
|---|---|---|---|---|
| Show commands | Allows the administrator to view the configured parameters and operational status | Command | Configured parameter values, associated station information, associated AP information | None |
| Show security-gateway | Allows the administrator to view the current status and other information | Command | Current State, Software version, IP information | None |
| Statistics commands | Allows the administrator to view statistics | Command | Interface statistics, Authentication statistics | None |
| Diagnostics | Allows the administrator to generate a diagnostics file on the cryptographic module | Command | Status of command | None |
| Save | Allows the administrator to save the configuration or diagnostics to a remote file | Command, file path to save the information to | Status of command, Configuration file, Diagnostics file | None |
| Network Configuration Commands | Allows the administrator to modify IP addresses, netmask, default gateway etc. | Command, IP address, netmask, default gateway | Status of command | None |
| System Configuration Commands | Allows the administrator to configure date, key expiration values, snmp configuration | Command, date, key expiration value, snmp parameters | Status of command | None |
| Show Log | Allows the administrator to view the logs | Command | System logs | None |

### *Client User Role*

This role represents the Client users from the wireless stations that connect to the cryptographic module for network connectivity. Client users are authenticated via the 802.11i Authentication mechanism. The Client user is authenticated by a successful EAP-TLS negotiation with a valid Client Certificate. A cryptographic key the Pairwise Master Key (PMK) is generated for an authenticated Client User. The cryptographic module establishes a cryptographic session for each association from an authenticated Client User via the 802.11i 4-way handshake. The 802.11i 4-way handshake uses the PMK to generate the cryptographic session keys TK and GTK. The cryptographic module processes Client user data only if a session with a valid TK/GTK has been setup, otherwise the client user data is discarded. TK is used to encrypt/decrypt unicast data to/from the wireless stations and GTK is used to encrypt multicast data to the wireless stations.

| Service | Description | Input | Output | CSP Access |
|---|---|---|---|---|
| Authentication and Client Key generation | The client user is authenticated and a PMK is generated | EAP-TLS handshake | EAP-TLS handshake | Server Private Key, Server Signing Certificate, PMK |
| Session Key Generation | The cryptographic keys for the Client User session are generated | 802.11 4-way handshake | 802.11i 4-way handshake | PMK, PTK, TK, GTK |
| Encrypt Data | Data destined to the client user wireless station is encrypted and forwarded | Plaintext data | Ciphertext data | TK, GTK |
| Decrypt Data | Data received from the client user wireless station is decrypted and forwarded | Ciphertext data | Plaintext data | TK, GTK |

The Security Gateway Cryptographic module resets the authentication state across reboots and administrators/Client users are required to re-authenticate to access the cryptographic services.

### *Unauthenticated Services*

The cryptographic module has a visible LED that indicates whether the module is powered on or not.

### *Definition of Critical Security Parameters (CSPs)*

The following are CSPs and Keys contained in the module:

- Master Key: This is a 3-Key TDES 168-bit key that is used to encrypt the Server Private Key and SSHv2 DH Host Private Key. The Master Key is generated by the module using the DRNG function during the module’s initialization phase. The Master Key is stored in EEPROM in plaintext.

- Server Private Key: This is an RSA 1024/2048/4096-bit key pair that is entered into the module by the CSO Administrator through SCP or through the CLI (SSHv2). The Server Private Key is stored encrypted by the Master Key and is used in the EAP-TLS negotiation to generate the PMK, per IEEE802.11i.
- EAP-TLS master secret: This is a 48 byte shared master secret derived from the EAP-TLS negotiation using a pre master secret, client and server random numbers. The master secret is an interim key used to derive the PMK.
- EAP-TLS HMAC Key: The HMAC key is generated using a PRF function during the EAP-TLS negotiation and is used as an integrity check for the EAP-TLS handshake.
- PMK: This 32 byte key is generated as a result of an EAP-TLS negotiation and is used to generate the TK used to encrypt/decrypt 802.11 data traffic.
- PTK: This 48 byte key block is generated by the 802.11i four way handshake using the PMK.
- GTK: This is a randomly generated number used to encrypt 802.11 data multicast to the stations.
- TK: This key is extracted from the PTK which is generated as part of the 802.11i four way handshake. This key is used to encrypt/decrypt unicast 802.11 data traffic.
- KEK: This key is extracted from the PTK which is generated as part of the 802.11i four way handshake. This key is used to encrypt the GTK sent to the client users.
- CSO Administrator Password: Passwords should be a minimum of 6 characters in length and should contain a character from at least four (for length less than 8), three (for length less than 10), two (for length less than 12) of the following groups: upper case letters, lower case letters, numbers and special characters. Empty passwords are not permitted.
- Non-CSO Administrator Password: Passwords should be a minimum of 6 characters in length and should contain a character from at least four (for length less than 8), three (for length less than 10), two (for length less than 12) of the following groups: upper case letters, lower case letters, numbers and special characters. Empty passwords are not permitted.
- SSHv2 Symmetric Key: AES 128-bit, AES 256-bit or TDES 168-bit keys used to encrypt/decrypt traffic within SSHv2.
- SSHv2 DH Host Private Key: RSA 1024-bit key pair used to authenticate the SSH server to the clients. The SSHv2 RSA key pair is generated by the module during the initialization phase. The SSHv2 DH Host Private Key is stored encrypted by the Master key.

### *Definition of Public Keys:*

The following are the public keys contained in the module:

- Software Firmware Validation Key: This is the public part of the cryptographic module's

RSA Public/Private key pair used to verify RSA signatures on new firmware.

- SSHv2 DH Host Public Key: RSA 1024-bit Public Key that is used to authenticate the SSH server to the clients.
- Server Public Key (EAP-TLS): RSA 1024/2048/4096-bit Public Key that is sent to the client to perform the EAP-TLS negotiation and generate the PMK.
- Server  Signing Certificate: RSA 1024/2048/4096-bit Public Key that is used to validate Client User Client certificates.

## Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device operates in a limited operational environment.

## Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide three distinct operator roles.  These are the Client User role, CSO Administrator role, and the non-CSO Administrator role.
2. The cryptographic module provides operator authentication through verification of 1024/2048/4096-bit RSA certificates (through EAP-TLS) and username/password combinations.
3. When the module has not been placed in a valid role, the operator shall not have access to any security functions, including cryptographic services.
4. The cryptographic module shall encrypt message traffic using the TDES or AES algorithm.
5. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      i. Cryptographic Algorithm Tests:

         a. AES-CBC 128-bit/256-bit Known Answer Test
         b. AES-ECB 128-bit Known Answer Test
         c. AES-CCMP Known Answer Test
         d. HMAC-SHA1 Known Answer Test
         e. DRNG (ANSI X9.31) Known Answer Test
         f. RSA SigVer15 Known Answer Test
         g. RSA Pair-wise Consistency Test
         h. RSA SigGen15 Known Answer Test

i. TDES Known Answer Test

j. SHA-1 Known Answer Test

k. DH Conditional Test

ii. Software Integrity Test (Checksum verification)

iii. Critical Functions Tests

a. None.

B. <u>Conditional Self-Tests:</u>

i.Continuous Random Number Generator (DRNG) Test – performed on DRNG ANSI X9.31 Appendix A.2.4.

ii.Continuous Random Number Generator (NDRNG) Test – performed on Hardware NDRNG Cavium.

iii. Software/Firmware Load Test – performed on new images with RSA signature verification.

iv. DH conditional self test as per SP800-56A.

6. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
7. Prior to each use, the internal DRNG and NDRNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
8. The key generation functions are logically separate from the network and console output functions.
9. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
10. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. The status of the tests run is displayed while performing the self tests.
12. A SHA-1 hash of the CSO administrator and Non-CSO administrator username and passwords are stored in the configuration database. The unprotected passwords are never stored on the module.
13. Administrator access for the first time is allowed with a default username and password. The default password can be changed on the initial setup.
14. The module shall support concurrent operators.

## Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks that are outside the scope of FIPS 140-2 requirements.