ecoNet smart grid gateways: ecoNet SL and ecoNet MSA FIPS 140-2 Security Policy

Level 2 Validation
Document Version 0.5

Hardware Versions: ENSL2, ENSL5 and ENMSA2
Firmware Version: 3.2.1-FIPS

Nexgrid, LLC
4444 Germanna Hwy
Suite 330
Locust Grove, VA 22508

Revision History

Version	*Modification Date*	*Modified By*	*Description of Changes*
0.1	2011-02-22	Thomas McLure	Initial Draft
0.2	2011-06-21	Thomas McLure	Updated based on feedback
0.3	2011-08-25	Thomas McLure	More updates based on feedback, added images
0.4	2011-09-01	Thomas McLure	Added MSA images, multiple updates
0.5	2011-12-01	Thomas McLure	Updated based on feedback

Table of Contents

Table of Figures

Table of Tables

1. Overview

This document is the non-proprietary FIPS 140-2 Security Policy for the ecoNet smart grid gateways: ecoNet SL and ecoNet MSA modules by Nexgrid, LLC. This Security Policy document may be duplicated unmodified and in its entirety.

The Nexgrid ecoNet smart grid gateways: ecoNet SL and ecoNet MSA (herein collectively called the modules) are wireless access points that support the IEEE 802.11n Wi-Fi standards for wireless LAN communications and the IEEE 802.3 standard for Ethernet communications. The modules are multiple-chip standalone cryptographic modules, compliant with all requirements of FIPS 140-2 Level 2.

The modules provide a robust communications network over Wi-Fi and Ethernet to connect end electric meters and devices to a central Energy Data Server. Secure management is implemented using SSL secured TLS and SSH connections.

The ecoNet module comes in three versions: ENSL2, ENSL5 and ENMSA2. The differences in the units are as follows:

- ENSL2 – This model is designed to plug into the standard photocell adapter on top of a streetlight for power. This model uses the 2 GHz Wi-Fi spectrum.
- ENSL5 – This model is designed to plug into the standard photocell adapter on top of a streetlight for power. This model uses the 5 GHz Wi-Fi spectrum.
- ENMSA2 – This model is designed to attach to a standard meter socket adapter and obtain power from the meter socket. This model uses the 2GHz Wi-Fi spectrum.

Table 1: FIPS 140-2 Security Level

Security Component	FIPS 140-2 Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.1 Definitions and Acronyms

This Security Policy document uses the following definitions and acronyms.

Table 2: Definitions and Acronyms

Term/Acronym	Description
CSP	Critical Security Parameter
EDS	Energy Data Server. This is a Nexgrid Server that acts as a TLS Server and communicates with one or more ecoNet modules acting as TLS clients.
SSH	Secure Shell network protocol
TLS	Transport Layer Security protocol
RNG	Random Number Generator
TEL	Tamper-Evident Label

2. Diagram of Cryptographic Module

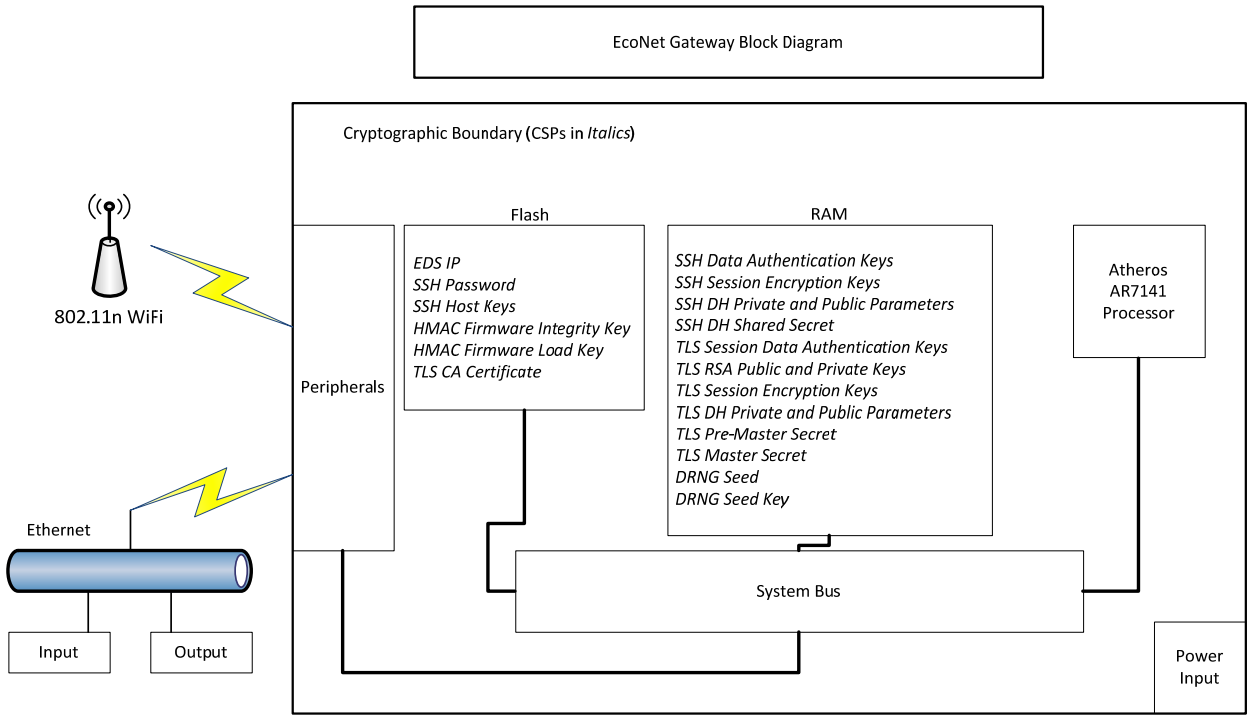

Figure 1: Module's Block Diagram

2.1 EcoNet SL Cryptographic Boundary (ENSL2 and ENSL5)

Figure 2: ENSL2 and ENSL5 Front

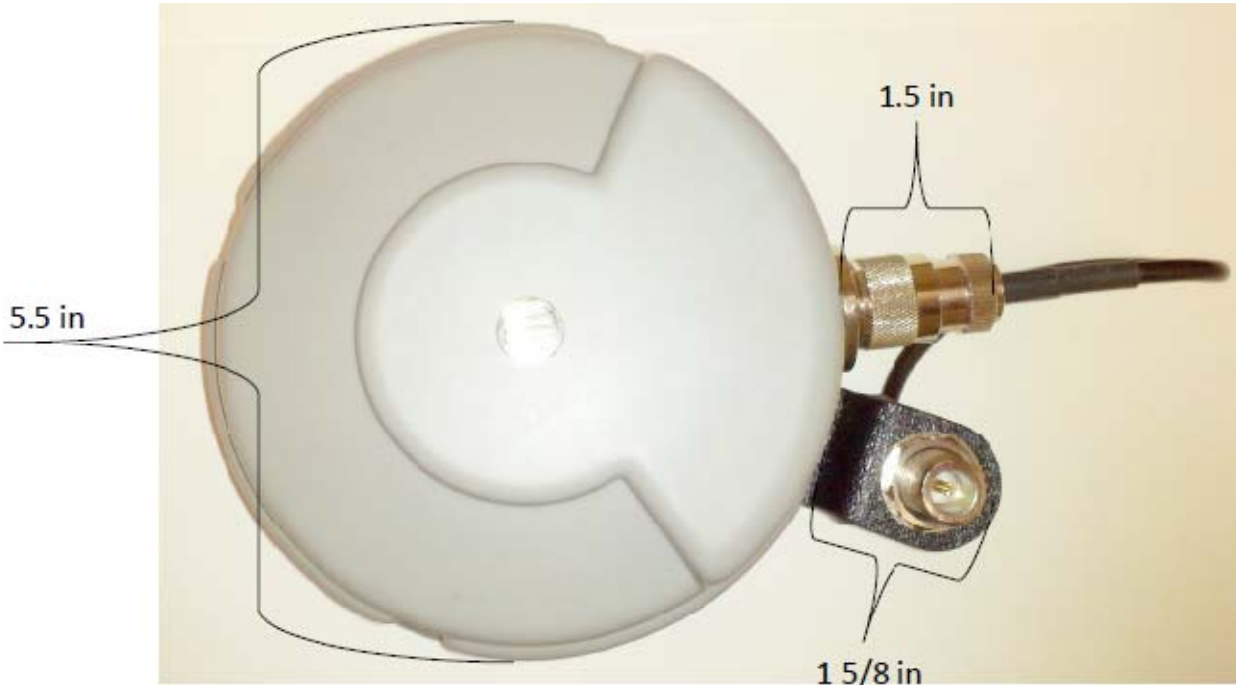

Figure 3: ENSL2 and ENSL5 Top

2.2 EcoNet MSA Cryptographic Boundary (ENMSA2)

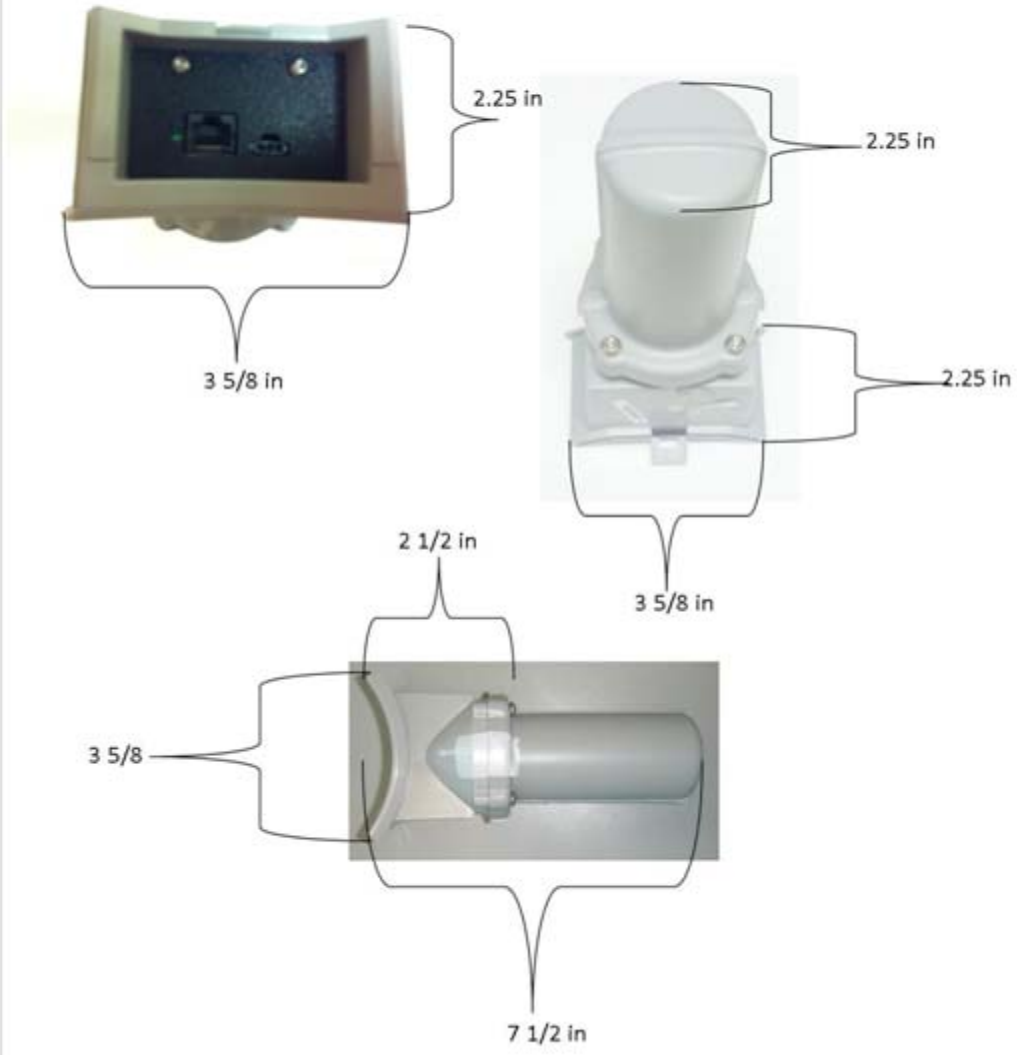

Figure 4: ENMSA2 Physical Dimensions

3. Modes of Operation

The cryptographic module supports the following FIPS approved or allowed algorithms.

Table 3: FIPS-Approved Algorithms

Algorithm	*Certificate*	*Usage*	*Keys/CSPs*
AES	#1665	encrypt/decrypt	AES keys 128, 192, 256 bits
Triple-DES	#1083	encrypt/decrypt	Triple-DES keys 112, 168 bits
DSA	#520	sign and verify	DSA keys 1024 bits
RNG (ANSI X9.31 Appendix A.2.4 using AES)	#887	random number generation	RNG seed value is 128 bits; seed key values are 128 bits, 192 bits, and 256 bits
RSA (X9.31, PKCS #1.5, PSS)	#820	sign and verify	RSA keys 1024, 1536, 2048, 3072, 4096 bits
SHA-1	#1459	hashing	N/A
SHA-224	#1459	hashing	N/A
SHA-256	#1459	hashing	N/A
SHA-384	#1459	hashing	N/A
SHA-512	#1459	hashing	N/A
HMAC-SHA-1	#979	message integrity	HMAC key
HMAC-SHA-224	#979	message integrity	HMAC key
HMAC-SHA-256	#979	message integrity	HMAC key
HMAC-SHA-384	#979	message integrity	HMAC key
HMAC-SHA-512	#979	message integrity	HMAC key

The Module supports the following non-approved but allowed algorithms:

Table 4: FIPS-Allowed Algorithms

Algorithm	*Usage*	*Keys/CSPs*
Diffie-Hellman	key establishment	Diffie-Hellman keys (shared secret provides between 80 and 224 bits of encryption strength)
RSA encrypt/decrypt	key wrapping	RSA (key wrapping; key establishment methodology provides 80 to 256 bits of encryption strength)

3.1 Non-FIPS Mode of Operation

The cryptographic module ships from the vendor in FIPS-Approved mode and does not provide a non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module supports the following physical ports and corresponding logical interfaces:

- **Ethernet:** Data Input, Data Output, Control Input, Status Output
- **Wireless:** Data Input, Data Output, Control Input, Status Output
- **Power Port:** Power Interface
- **LED:** Status Output

5. Roles and Services

The roles of the module include a Crypto-officer and User Role. In addition, the ecoNet provides a set of unauthenticated services to any operator with network and/or physical access to the module.

5.1 Roles and Required Authentication Data

Table 5: Roles and Authentication

Role	*Type of Authentication*	*Authentication Data*
Crypto-Officer	Identity-based operator authentication	Via SSH-2: Username and Password. Password can be a minimum of 10 characters and a maximum of 128 characters.
User	Role-based authentication	Via TLS HTTPS to EDS IP: EDS Server certificate must verify against stored ecoNet certificate authority
Unauthenticated	None	n/a

5.2 Strengths of Authentication Mechanisms

Table 6: Strength of Authentication

Authentication Mechanism	*Strength of Mechanism*
Username and Password	The module enforces 10-character passwords (at minimum) chosen from the 96+ human readable ASCII characters for ssh access. The password can be a maximum of 128 characters. In addition, the password must contain at least one from each of the following four groups (upper-case letters, lower-case letters, numbers, and special characters). Considering the simplest case, even without the password restrictions enforced by the module, the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million. The module enforces a timed access mechanism as follows: There is a 15-second delay between the initiation of an SSH connection and a response from the module. After that delay, a total of 5 connection attempts are permitted before the connection is broken. This leads to a maximum of 20 possible attempts in a one-minute period. The probability of a success with multiple consecutive attempts in a one-minute period is $20/(96^{10})$, which is less than 1/100,000. The actual probability of success is even lower than this because of the additional character restrictions enforced by the module.
EDS TLS Certificate	The module only supports RSA (4096 bit) certificate connections to EDS, which have a minimum equivalent computational resistance to attack of 2^{150}. Thus the probability of a successful random attempt is $1/(2^{150})$, which is less than 1/1,000,000. The ecoNet initiates the connection to the EDS server, and the connection cannot be set to more

	than once per minute. Thus, the probability of success with multiple consecutive attempts in a one-minute period is the same as a single attempt, or $1/(2^{150})$, which is less than 1/100,000.

6. Critical Security Parameters (CSPs)

Table 7: Critical Security Parameters

CSP	*Type*	*Description*
EDS IP	ASCII String	Used by the ecoNet to contact the Energy Data Server
SSH Password	ASCII String	Used by the Crypto-Officer role to access the module
SSH Private/ Public keys	RSA , DSA	Used to secure the ssh channel
HMAC Firmware Integrity Key	HMAC SHA-1	Used during firmware integrity verification
HMAC Firmware Load Key	HMAC SHA-1	Used for new firmware verification
SSH Session Data Auth. Keys	HMAC SHA	Establish & Maintain SSH Session
SSH Session Encryption Keys	AES , Triple-DES	Establish & Maintain SSH Session
SSH DH Private/Public Parameters	DH 80-224	Establish & Maintain SSH Session
SSH DH Shared Secret	DH shared secret	Establish & Maintain SSH Session
TLS CA certificate	RSA (4096)	Used to verify the EDS certificate
TLS Session Data Auth. Keys	HMAC SHA	Establish & Maintain HTTPS Session
TLS Private/Public keys	RSA, DSA	Establish & Maintain HTTPS Session
TLS Session Encryption Keys	AES , Triple-DES	Establish & Maintain HTTPS Session
TLS DH Private/Public Parameters	DH 80-224	Establish & Maintain HTTPS Session
TLS Pre-Master Secret	TLS secret	Establish & Maintain HTTPS Session
TLS Master Secret	TLS secret	Establish & Maintain HTTPS Session
RNG Seed	128-bit value	Establish & Maintain HTTPS Session
RNG Seed Key	128, 192 or 256-bit value	Establish & Maintain HTTPS Session

7. Services and CSP Access

Table 8: Access Control Policy

Service	Role	*CSPs and Access*
SSH ecoNet Access	Crypto-Officer	SSH password – read SSH Session Data Authentication Keys – read, write SSH Session Encryption Keys – read, write SSH DH Private and Public Parameters – read, write SSH DH Shared Secret – read, write RNG Seed – read, write RNG Seed Key – read SSH Private/ Public keys – read, write
Run power-up self-tests	Crypto-Officer	HMAC Firmware Integrity Key –read
Regenerate ecoNet host ssh keys	Crypto-Officer	SSH Private/ Public keys – write, zeroize
Upgrade ecoNet Firmware	User	HMAC Firmware Load Key –write, zeroize SSH Private/ Public keys – write, zeroize
Reboot ecoNet	Crypto-Officer	Zeroize all ephemeral keys (ram)
Configure ssh password	Crypto-Officer, User	SSH password – write, zeroize
Configure EDS IP	Crypto-Officer, User	EDS IP – write, zeroize
Configure system settings	Crypto-Officer, User	None
TLS HTTPS Connection to EDS	User	EDS Server IP – read TLS Session Data Authentication Keys – read, write TLS Public and Private Keys – read, write TLS Session Encryption Keys – read, write TLS DH Private and Public Parameters – read, write TLS Pre-Master Secret – read, write TLS Master Secret –read, write RNG Seed – read, write RNG Seed Key – read
Send and receive wireless data	Unauthenticated	None
Power-cycle ecoNet and run power-up self-tests	Unauthenticated	Zeroize all ephemeral keys (RAM)
View power status (via power led)	Unauthenticated	None
View FIPS status (via http page)	Unauthenticated	None
View FIPS status (via cli interface)	Crypto-Officer	None

8. Physical Security

The ecoNet series models are multi-chip standalone cryptographic modules. The entire contents of each module (including all hardware, firmware, and data) are enclosed in an opaque plastic case. The cases are sealed using tamper-evident labels in order to prevent the covers from being removed without signs of tampering. All integrated circuits (ICs) in the modules are coated with commercial standard passivation.

8.1 Tamper Label Placements

EcoNets arrive from the factory with Tamper Evident Labels already applied by Nexgrid in the following locations.
The ENSL2 and ENSL5 require a total of 2 TELs whereas the ENMSA2 utilizes a total of 4 TELs, which are shown below.

8.2 EcoNet SL (ENSL2, ENSL5) Tamper Evident Label Placement

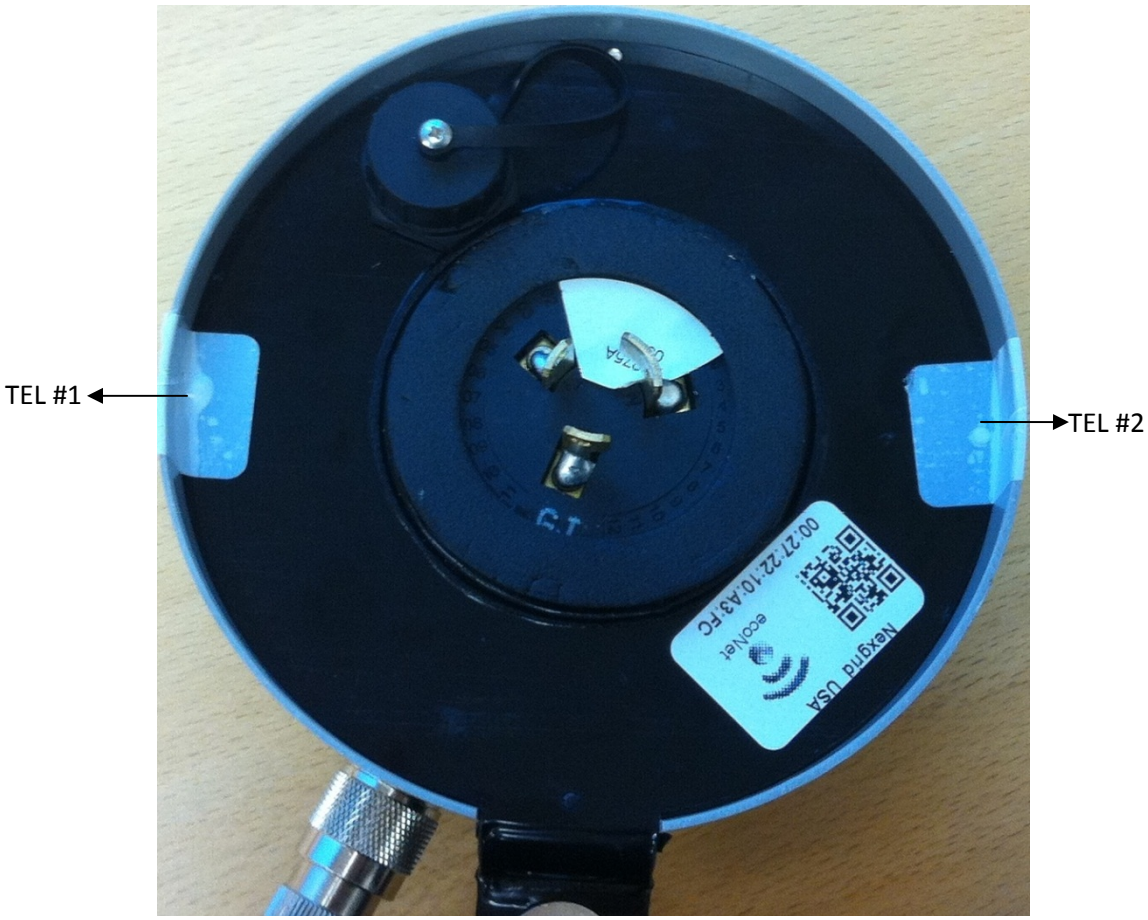

Figure 5: ENSL2 and ENSL5 Label Placement

8.3 EcoNet MSA Tamper Evident Label Placement

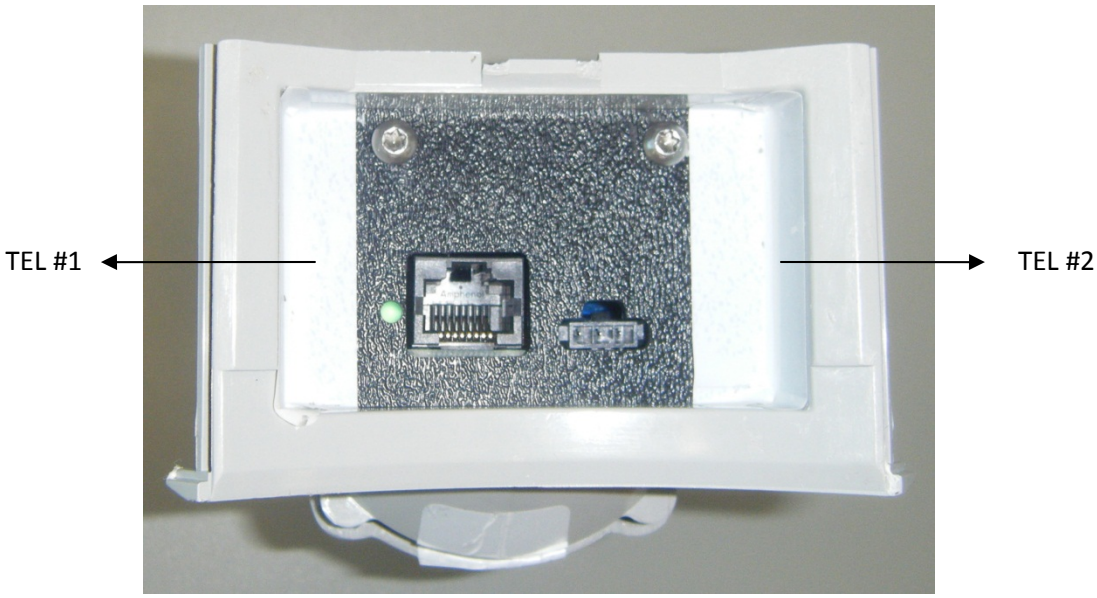

Figure 6: ENMSA Front Label Placement

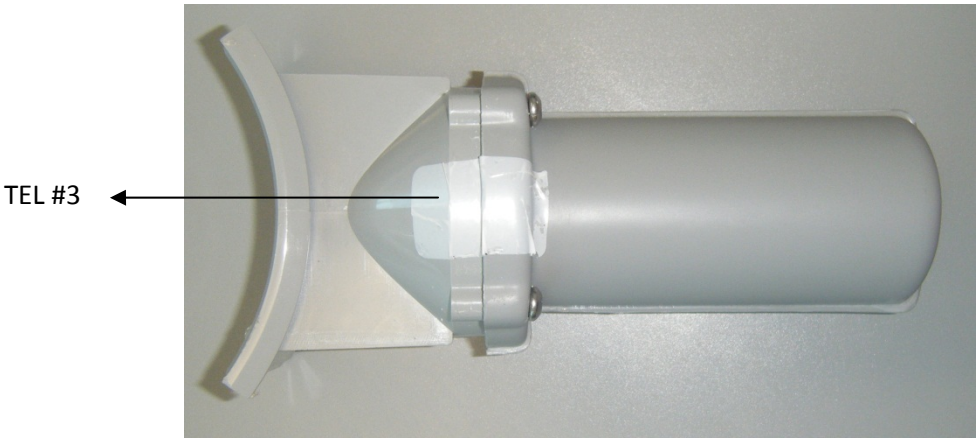

Figure 7: ENMSA2 Top Label Placement

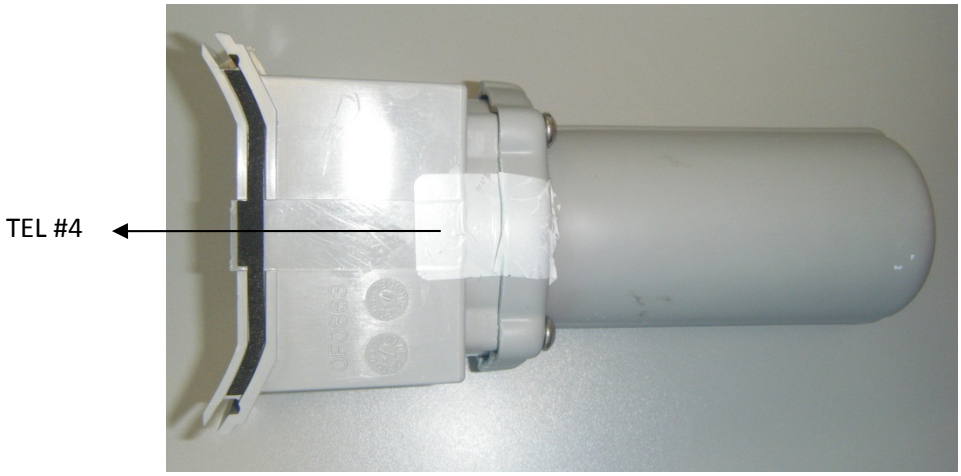

Figure 8: ENMSA2 Bottom Label Placement

9. Secure Operation and Security Rules

In order to operate the ecoNet Smart Grid Gateway securely, the operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules required.

9.1 FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements at all times.

- The ecoNet uses only FIPS-approved cryptographic algorithms.
- The ecoNet employs the FIPS-approved random number generator whenever generating keys.
- The ecoNet provides role-based authentication of operators by verifying username and password for SSH access and by verifying EDS certificate for TLS access.
- The ecoNet provides the Crypto-officer the capability to zeroize the plaintext critical security parameters contained within module.

9.2 Physical Security Rules

The Crypto-Officer must periodically inspect the physical case and tamper evident labels of the ecoNet to ensure that no attacker has attempted to tamper with the module. Signs of tampering include

- Deformation, scratches, or scrape marks in the hard plastic case of the ecoNet
- Wrinkled, faded, torn, or missing TELs, or TELs that are detached from the ecoNet case exposing the word “OPEN” in seal residue where the TEL used to be affixed to the case

9.3 Secure Operation Initialization Rules

The ecoNet arrives from the factory already configured for approved FIPS operation. No further configuration is required.

10. Mitigation of Other Attacks

Nexgrid does not wish to claim that the module mitigates any other attacks.