SC4000 Series Mesh Radio

Non-Proprietary FIPS 140-2 Security Policy

Version: 1.2

Date: 12 December 2018

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Silvus Technologies SC4000 Series Mesh Radio base board, hereafter denoted the Module. The Module combined with a suitable RF front end (RFFE) component is used in a family of MIMO radios used to provide a wireless mesh network. Each radio is capable of operating in a multitude of configurations that are accessed via simple web pages within the radio. Settings such as transmit power, frequency, channel bandwidth, link adaptation and range control can be accessed by simply using a web browser to log into any radio within the network.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version	Distinguishing characteristic
1	SC4200	SC42-SUB-FIPS Rev A1	3.16.0.0	2 antenna
2	SC4400	SC44-SUB-FIPS Rev A1	3.16.0.0	4 antenna

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated radios.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	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
Overall	2

1.1 Module Cryptographic Boundary

The physical form of the Module is depicted in Figures 1 through 4. The module is composed of the baseboard circuit board surrounded by an opaque aluminum shield that serves as an EMI shield, heat sink, and FIPS enclosure. The Module is a multi-chip embedded embodiment with a non-modifiable operational environment. The cryptographic boundary is the surface of the entire module.

SC4200

Figure 1 - Top View of SC4200

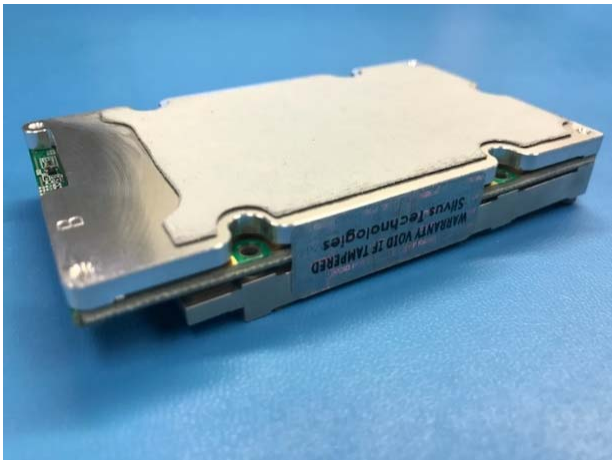

Figure 2 - Bottom View of SC4200

SC4400

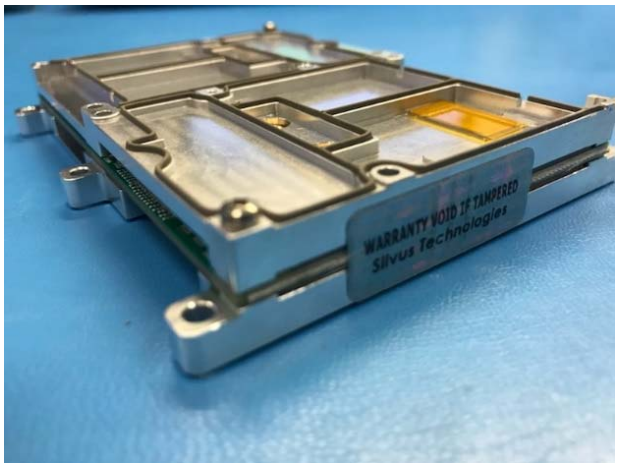

Figure 3 - Top View of SC4400

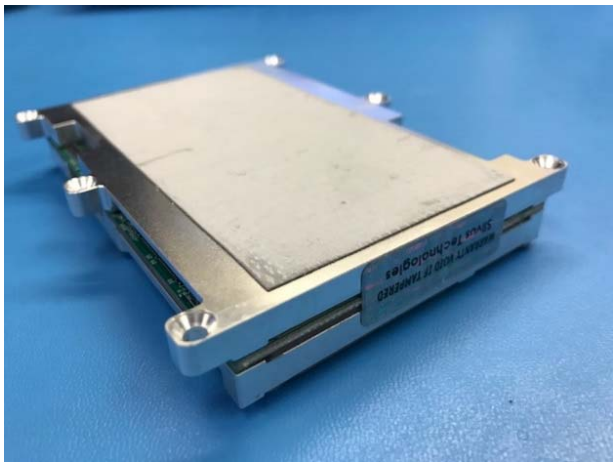

Figure 4 - Bottom View of SC4400

The module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Battery	Power from battery	Power input
Ethernet	1000-Base T	Control in, Data in, Data out, Status out
External BDA control	Bi-directional amplifier	Data output
GPIO	General Purpose I/O	Control in, Data in, Data out, Status out
LED	Multi-state status output	Status out
MICTOR*	Reset pin. (debug interface hardware present but non-functional)	Control input
Multi-position Switch	Used to power on/off and discrete volume settings, etc.	Control input
Power Supply	Power from external source	Power input
PTT	Push To Talk audio (mic, spkr, activate)	Control in, Data in, Data out
RFFE Interface	Control to and status from the RFFE	Data in, Data out
RF	RF to and from antennas (SC4200 has 2; SC4400 has 4)	Control in, Data in, Data out, Status out
RF Power	Power to RFFE	Power output
Serial	RS232 (console or user data)	Control in, Data in, Data out, Status out
USB (2)	As host (supports mass storage, Ethernet, Wi-Fi, RS232 Serial) As device (acts as Ethernet over USB)	Power input and output, Control in, Data in, Data out, Status out

* On SC4400 only. Reset pin is always functional. Debug interface not functional without separate FPGA configuration image/firmware signed and encrypted by the manufacturer.

1.2 Modes of Operation

The module supports both an Approved and non-Approved mode of operation. By default, the module ships in a non-Approved mode of operation. The user must follow the instructions in section 8 to place the module in an Approved mode. To verify that a module is in the Approved mode of operation, the operator can compare the configuration of the module to what's defined in Section 8. The non-Approved mode of operation has the same services running as the Approved mode as stated in Section 3.5 of the Security Policy. The only two differences between Approved and non-Approved modes is 1) Availability of DES block encryption of RF-link packets in ECB mode in the non-Approved mode of operation and 2) Use of HTTP instead of TLS is allowed in non-Approved mode, versus Approved mode where it is mandatory. All the rest of the services and algorithms are the same.

2 Cryptographic Functionality

The cryptographic protocols and primitives implemented and used by the module are listed in this section. The module provides TLS for secure configuration of the module using the methods identified in Table 4 when in an approved mode. The module can also provide a SSHv2 server for module configuration and administration. Table 5 lists the security methods used when configuring the module over SSH. No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

Table 4 – TLS Ciphersuites Available in the Approved Mode

Cipher Suite String	Key Exchange	Auth	Cipher	MAC
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE	ECDSA	AES_256_CBC	HMAC-SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES_256_CBC	HMAC-SHA-384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE	ECDSA	AES_256_GCM	

Table 5– SSH Security Methods Available in the Approved Mode

Key Exchange	Auth	Cipher	Integrity
ECDH-sha2-nistp521	ECDSA P-521 with SHA-512	AES CTR 256	HMAC-SHA256

The module also supports USB Wi-Fi adapters for establishing local standards-compliant wireless access but does not rely on the security of the Wi-Fi channel as all communications related to the security of the module are tunneled over SSH or TLS. The RF link to other nodes in the mesh network can be encrypted if configured to do so.

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 6 – Approved and CAVP Validated Cryptographic Functions

Cert	Algorithm	Mode	Description	Functions/Caveats
5497 & 5613	AES (Hardware) [197]	ECB [38A]	Key size: 256 bits	Encrypt
		GCM [38D][1]	Key size: 256 bits	Encrypt, Decrypt
5496	AES [197]	CBC [38A]	Key size: 256 bits	Encrypt, Decrypt
		CTR [38A]	Key size: 256 bits	Encrypt, Decrypt

[1] If power is lost then restored, a new key is established using the validated KAS scheme. The IV is generated internally deterministically using a 48 bit device unique id and a 48 bit counter.

Cert	Algorithm	Mode	Description	Functions/Caveats
		GCM [38D][2]	Key size: 256 bits	Encrypt, Decrypt
VA	CKG [IG D.12]	[133] Section 6.1 Asymmetric Signature Key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2 Asymmetric Key Establishment Key generation using unmodified DRBG output		
		[133] Section 7.1 Direct Symmetric Key generation using unmodified DRBG output		
		[133] Section 7.3 Derivation of symmetric keys from a Key Agreement shared secret.		
1948	CVL: TLS KDF [135]	V1.0/1.1, v1.2	SHA-1, SHA-256, SHA-384	Key Derivation
	CVL: SSH KDF [135]	V2	SHA-512	
2167	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation
1474	ECDSA [186]		P-256, P-521	KeyGen
			P-521	PKV
			P-256 (SHA-1, 384) P-384 (SHA-1, 384) P-521 (SHA-1, 256, 384, 512)	SigGen
			P-256 (SHA-1, 384) P-384 (SHA-1, 384) P-521 SHA(1, 256, 384, 512)	SigVer
3647	HMAC [198]	SHA-1	Key Size < Block Size	Message Authentication, KDF Primitive, Password Obfuscation
		SHA-256	Key Size < Block Size	
		SHA-384	Key Size < Block Size	
185/ VA	KAS ECC [56A]/[56Ar2][3]	Ephemeral Unified (Initiator, Responder)	Parameter set EE: P-521 SHA-512/SHA-256 HMAC	Key Agreement

[2] If power is lost then restored, a new key is established using the validated KAS scheme. The IV is generated in compliance with TLS, as described in RFCs 5116, 5288 and 5289.

[3] Testing was performed to [56A] including the concatenation KDF with SHA-512. The module uses the concatenation KDF with SHA-256 which is not part of [56A] or the CAVS testing but is allowed per [56Ar2]. The Vendor affirms compliance to [56Ar2].

Cert	Algorithm	Mode	Description	Functions/Caveats
N/A	KTS [197] & [38F]	GCM, CTR+HMAC, CBC+HMAC	AES Certs. #5497 and #5613, AES Cert. #5496 with HMAC Cert. #3647	Key Transport
4406	SHS [180]	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest Generation, Password Obfuscation
Zynq Secure Boot[4]				
2363	AES [197]	CBC [38A]	Key size: 256 bits	Decrypt
1465	HMAC [198]	SHA-256	Key size: 256 bits, λ = 256	Message Authentication
2034	SHS [180]	SHA-256		Message Digest

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES (no security claimed)	For WPA controlled 802.11
EC Diffie-Hellman	(CVL Cert. #1948, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
KDF (no security claimed)	PBKDF2 for WPA
MD5 (no security claimed)	Used in TLS per IG 1.23 example 2aD.2
NDRNG	[Annex C] Non-Deterministic RNG; minimum of 64 bits per access. The NDRNG output is used to seed the DRBG with at least 497 bits of entropy.
RSA (no security claimed)	RSA SigVer used for secure boot. Validated by chip manufacturer but not on this Operating Environment.
SHS (no security claimed)	For RSA SigVer used for secure boot. Validated by chip manufacturer but not on this Operating Environment.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

Table 8 – Non-Approved Algorithms (Used only in the non-Approved Mode)

Algorithm	Description and usage
DES-ECB	DES block encryption of RF data packets in ECB mode

[4] These algorithms are only used by the secure boot process of the module processor and therefore only used during self-test.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3.

Table 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Cookie-Key	256 bit HMAC-SHA-384 key for signing cookies (ephemeral)
DRBG-EI	DRBG entropy input to the AES-CTR mode DRBG.
DRBG-State	Internal state variables V and Key stored in RAM as an OpenSSL context
Passwords	5-character minimum user authentication passwords
RF-DH-Priv	P-521 ECDHE private key for establishing the TEK/TDK
RF-Auth-Key	256 bit HMAC-SHA-256 key for authenticating the RF-DH ephemeral public key
RF-TDK	AES-GCM 256 bit Traffic Decryption Key
RF-TEK	AES-GCM 256 bit Traffic Encryption Key
SSH-DH-Priv	SSHv2 ECDHE P-521 Private Key
SSH-Host-Priv	SSHv2 Host Static ECDSA P-521 Private Key
SSH-SENC	SSHv2 Session Encryption AES-CTR-256 Key
SSH-SMAC	SSHv2 256 bit HMAC-SHA-256 Session Authentication Key
TLS-DH-Priv	TLS ECDHE P-256, P-384 or P-521 Private Key
TLS-Host-Priv	TLS Host Static ECDSA P-256, P-384 or P-521 Private Key
TLS-MS	TLS Master Secret
TLS-PMS	TLS Pre-Master Secret
TLS-SENC	TLS Session Encryption AES CBC/GCM 256 bit key
TLS-SMAC	TLS Session Authentication HMAC-SHA-1 (160 bit) or HMAC-SHA-384 (384 bit) Key

2.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
RF-DH-Pub	RF ECDHE P-521 public key
SSH-Host-Pub	SSH host static ECDSA P-521 public key
SSH-Client-Pub	SSH client static ECDSA P-521 public key used for authentication
SSH-DH-Pub	SSH ECDHE P-521 client and server public keys
TLS-Host-Pub	TLS host ECDSA P-256, P-384 and P-521 public key used for authentication.
TLS-DH-Pub	TLS ECDHE P-256, P-384 and P-521 client and server public keys

Key	Description / Usage
FW-Update-Pub	ECDSA P-521 public key used to verify firmware updates and license files.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports role based authentication with four distinct operator roles, Cryptographic Officer (CO), Advanced User, Basic User and Mesh Node. The cryptographic module enforces the separation of roles using a standard session based architecture. Re-authentication is enforced when changing roles and is cleared upon power reset. The module supports concurrent operators but maintains the separation of roles for each.

Table 11 lists the operator roles along with a description of their use and the nature of the authentication Data. The Module does not support a maintenance role. The CO is the only role that has access to authentication data after being authenticated.

Table 11 – Roles Description

Role ID	Role Description	Interfaces
Crypto Officer (CO)	Role to install and configure the cryptographic parameters of the module.	HTTPS/TLS-API, SSH, Shell-API
Advanced User (AU)	Role to configure advanced but non-security relevant settings.	HTTPS/TLS-API, Shell-API
Basic User (BU)	Role to configure basic settings.	HTTPS/TLS-API, Shell-API
Mesh Node (MN)	Peer node in the wireless mesh network	RF Link

3.2 Interfaces that Authenticate

HTTPS/TLS-API

A web interface and JSON "API" is available on the HTTPS web port. Users authenticate using a minimum five (5) character password. Upon successful authentication a TLS session authentication cookie associated with the role is returned which is created using HMAC-SHA-384 with the module "Cookie Key". The cookie must accompany each subsequent access. The web interface will accept maximum 20 login attempts per second due to CPU limitation. The API service on the module will handle at most 10 API request per second due to CPU limitation.

SSH

An SSH command shell interface is available on the module. SSH client key authentication is required using an ECDSA P-521 Public key. The key must be loaded onto the module after authentication as the CO using the Configure Security settings service. The P-521 bit key gives equivalent cryptographic strength as a 256-bit symmetric key and all session communication is encrypted with the same strength. The client

public key could be viewed as authentication of the CO role. However, the Shell-API requires separate authentication for each call as described below.

Shell-API

The module provides the ability to call the "API" via a shell interface available on a debug console as well as the SSH connection. Each "API" call must include a role and a minimum five (5) character password.

RF Link

The nodes in the mesh network communicate with each other via an RF encrypted interface. Authentication is via the 256 bit HMAC-SHA-256 RF-Auth-Key.

3.3 Authentication Strength

Table 12 – Authentication Description

Authentication Method	Justification
TLS Session cookie	The 256 bit Cookie-Key (HMAC-SHA 384-bit) used to create and authenticate the cookie is derived directly from the DRBG. Randomly guessing this key would succeed once in 2^256 which is less than one in 1,000,000. TLS access is performance limited to 20 requests per second. Given 20 attempts per second, the probability of success in a one (1) minute period is 1200/2^256 which is less than one in 100,000.
Password	The passwords must be at least five (5) characters long each, and the password character set is the alphanumeric characters (a-z,A-Z,0-9) which is 62 characters. This makes the probability, 1 in 62^5, which is less than one (1) in 1,000,000 that a random attempt will succeed or a false acceptance will occur for each attempt. Login attempts are performance limited to 20 per second. Given this the probability of success in a one (1) minute period is 1200/62^5 which is less than one (1) in 100,000.
SSH client key	The ECDSA P-521 key pair gives equivalent cryptographic strength as a symmetric key of size of 256 bits. This implies that the probability of a random attempt of guessing the key is one (1) in 2^256, which is less than one (1) in 1,000,000. The ssh server on the module has been configured to handle maximum one (1) concurrent authentication attempt. Each attempt takes at least one (1) second due to CPU limitation. Given one (1) attempt per second, the probability of success in a one (1) minute period is 60/2^256 which is less than one (1) in 100,000.
RF link key	The 256 bit RF-Auth-Key (HMAC-SHA-256) used in link key establishment is derived directly from the DRBG. Randomly guessing this key would succeed once in 2^256 which is less than one (1) in 1,000,000. The RF Link can process at most 20 authentication requests per second due to CPU limitation. Given 20 attempts per second, the probability of success in a one (1) minute period is (60 * 20)/2^256 which is less than one (1) in 100,000.

3.4 Services

All services implemented by the Module are listed in the tables below.

Table 13 – Authenticated Services

Service	Description	CO	AU	BU	MN
Configure advanced settings	Advanced non-security relevant configuration	X	X		
Configure basic settings	Basic non-security relevant configuration	X	X	X	
Configure security settings	Security relevant configuration, including uploading license and settings files, bypass and factory reset.	X			
Diagnostics	Initiation of diagnostics like ping, iperf, etc.	X	X	X	
Reset	Reset by API command “radio_reset” or by Navigating to Web interface -> Security -> Upgrade -> Reboot.	X			
RF wireless link	Establish and transmit data with another module.				X
SSH Session	Establish an SSH Session	X			
Status	Retrieve module status through HTTPS and API	X	X	X	
Update firmware	Upload new firmware image	X			
Zeroize	Zeroization through the web interface. Destroy all CSPs. The user needs to attach a USB dongle with a “reset license” – a Silvus supplied module-locked file that can be authenticated using FW-Update-Pub. When the module detects this file, it will initiate zeroization.	X			

Table 14 – Unauthenticated Services

Service	Description
Input and output data	Input/output of PTT Audio, GPIO, serial and wired network traffic.
Reset (perform self-test)	Reset by the reset line or power cycle.
Status	Retrieve module status through LEDs, unauthenticated Web
TLS session	Establish an unauthenticated TLS Session

Table 15 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

G = Generate: The service generates the CSP.
O = Output: The service outputs the CSP.
E = Execute: The service uses the CSP in an algorithm.
I = Input: The service inputs the CSP.
Z = Zeroize: The service zeroizes the CSP.

Table 15 – CSP Access Rights within Services

Service	CSPs																
	Cookie-Key	DRBG-EI	DRBG-State	Passwords	RF-DH-Priv	RF-Auth-Key	RF-TDK	RF-TEK	SSH-DH-Priv	SSH-Host-Priv	SSH-SENC	SSH-SMAC	TLS-DH-Priv	TLS-Host-Priv	TLS-PMS	TLS-SENC	TLS-SMAC
Authenticated																	
Configure advanced settings	E			E													
Configure basic settings	E			E													
Configure security settings	E			E O I		G I O				G I O				G I O			
Diagnostics	E			E													
Reset	G Z	G E Z	G Z		Z		Z	Z	Z		Z	Z	Z		Z	Z	Z
RF wireless link			G E		E G	E	E G	E G									
SSH session			G E						G E	E	G E	G E					
Status																	
Update firmware																	
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Unauthenticated																	
Input and output data																	
Reset	G Z	G E Z	G Z		Z		Z	Z	Z		Z	Z	Z		Z	Z	Z
Status																	
TLS session			G E										G E	E	G E	G E	G E

Table 16 – Public Key Access Rights within Services

Service	Public Keys						
	RF-DH-Pub	SSH-Host-Pub	SSH-Client-Pub	SSH-DH-Pub	TLS-Host-Pub	TLS-DH-Pub	FW-Update-Pub
Authenticated							
Configure advanced settings							
Configure basic settings							
Configure security settings		G I O	I O		G I O		
Diagnostics							
Reset	Z			Z		Z	
RF wireless link	G I O E						
SSH session		E	E	G I O E			
Status							
Update firmware							I E
Zeroize	Z	Z	Z	Z	Z	Z	
Unauthenticated							
Input and output data							
Reset	Z			Z		Z	
Status							
TLS session					E	G I O E	

3.5 Non-Approved Services

The non-Approved mode of operation has the same services running as the Approved mode. In addition, the non-Approved mode offers DES block encryption of RF-link packets in ECB mode. The module also allows the use of HTTP instead of HTTPS via TLS.

4 Self-tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs self-tests described in Table 17 below without any operator action required. All data output via the data output interface is inhibited when an error state exists and during self-tests. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters a fatal error state. The web page will switch to using HTTP only vs. HTTP/TLS and will only display a single page showing more information about the error state, e.g., which KAT failed. The user may then reboot the module to resume operation. If all KATs complete successfully, the module will enter a functional state. The user may navigate to Web -> Security -> Encryption page and read back the text alongside the "FIPs Mode" dropdown. It should read "Success".

Table 17 – Power Up Self-tests

Test Target (Cert. #)	Description
Firmware Integrity AES (2363), HMAC (1465), SHS (2034)	Firmware is decrypted and MAC verified. There is also a redundant 32 bit CRC of some components.
AES (5497 & 5613)	Encrypt and Decrypt KAT using 256 bit ECB
	Encrypt and Decrypt KAT using 256 bit GCM
AES (5496)	Encrypt and Decrypt KAT using 256 bit CBC
	Encrypt and Decrypt KAT using 256 bit CTR
	Encrypt and Decrypt KAT using 256 bit GCM
CVL (1948)	TLS and SSH KDF KATs
DRBG (2167)	CTR_DRBG KAT
ECDSA (1474)	Signature Generation and Verification KAT using P-521 and SHA-256
HMAC (3647)	KAT using SHA-1, SHA-256, and SHA-384
KAS (185)	Primitive "Z" Computation KAT using P-521
SHS (4406)	SHA-1, SHA-256, SHA-384, SHA-512 KAT

Table 18 – Conditional Self-tests

Test Target	Description
Bypass Test	Exclusive Bypass Test performed when encryption is enabled using the Configure security settings service.
DRBG Health Checks	Performed conditionally per SP 800-90 Section 11.3. Required per IG 9.8.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
Firmware load	Signature verification (P-521 and SHA-256) of a manifest file containing SHA-1 hashes of all components which are verified.

Test Target	Description
NDRNG	NDRNG Continuous Test (RCT) performed when a random value is requested from the NDRNG.
SP 800-56A Assurances	Performed conditionally per Section 5.5.2, 5.6.2, and/or 5.6.3. Required per IG 9.6.

The module does not have any Critical Functions tests other than those described above.

5 Physical Security Policy

The cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Two (2) tamper-evident seals applied during manufacturing

An operator in the CO role is responsible for the following:

- Inspecting the tamper-evident seals based on the schedule described in Table 19 below for any signs of tamper.
- If the module shows signs of tampering, the CO should zeroize the module and contact the manufacturer.

Table 19 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test
Tamper-Evident Seals	Inspect tamper-evident seals every 12 months.

Tamper-Evident Seal Locations- SC4200

Figure 5 – SC4200 Right Side

Figure 6 – SC4200 Left Side

Tamper-Evident Seal Locations- SC4400

Figure 7 – SC4400 Right Side

Figure 8 – SC4400 Left Side

6 Operational Environment

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

No mitigation of other attacks is implemented by the module.

8 Security Rules and Guidance

To operate in an Approved mode of operation the operator must perform the following steps. The module ships in a non-Approved mode of operation.

1. Open the web interface and navigate to Security->Encryption tab.
2. Change FIPS mode to enable.
3. A popup window will appear, confirming this choice. Upon saying “OK”:
    a. All CSPs will be zeroized or reset to default values. The web login password for the “Basic”, “Advanced” and “Crypto Officer (admin)” roles will be updated to be “HelloWorld”.
    b. The SSH-Host-Priv, SSH-Host-Pub and TLS-Host-Priv, TLS-Host-Pub will be reset to default factory keys.
    c. The 256-bit RF-Auth-Key will be zeroized to a factory default 0x1234567812345678123456781234567812345678123456781234567812345678.
    d. The radio will be subsequently rebooted into the Approved mode of operation. The initialization will not be considered complete until the user logs in as the CO and performs the following operations:

i. Updates the web login passwords to something different from “HelloWorld” on the Admin page.
ii. Creates/Uploads a new SSH-Host-Priv, SSH-Host-Pub key pair and a TLS-Host-Priv, TLS-Host-Pub key pair on Security->Key Management page.
iii. Creates/Uploads a new RF-Auth-Key on Security->Encryption page. All modules wishing to communicate to each other over the same mesh network will need to be configured with the same RF-Auth-Key. Hence the recommended procedure is to generate the RF-Auth-Key on the first module, and then upload it on all the remaining modules.
iv. At this point, the module is fully operational in Approved mode.

The module can be returned to a non-approved mode by unselecting “FIPS mode” in the Security->Encryption tab of the web interface which will zeroize/reset all CSPs requiring reconfiguration.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 20 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Abbreviation	Full Specification Name
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Table 21 – Acronyms and Definitions

Acronym	Definition
MIMO	A radio technology that uses multiple antennas to exploit multipath propagation to increase capacity.