SX-590-1402
FIPS 140-2 Level 1 Non-Proprietary Security Policy

Revision D
Date: 3-4-2022

REVISION HISTORY

Rev. No.	Date	Revision by	Comments
A	10.30.2020	Lee Aydelotte	Initial Version
B	9.26.2021	Jarrod Rafferty	Added changes based on NIST review: • Added Non-Proprietary to title • Changed KDF to KBKDF on Table 1 • Showed NDRNG inside imx6ull on diagram • Added info to 'Approved Mode' operation • Added detail to sec. 4.2.4 about PSK key • Removed AES CMAC references • Pluralized 'DRBG Health Test'
C	2.9.2022	Jarrod Rafferty	Added further changes based on NIST review • Clarified a reset is required to change FIPS modes • Clarified requirements on the PSK key • Listed the tests run for the Health Check
D	3.4.2022	Jarrod Rafferty	Added CVL to KDF-TLS in table

Table of Contents

1 OVERVIEW 1

1.1 Operational Environment 1
1.2 Approved Modes 2

2 CRYPTOGRAPHIC BOUNDARY 3

2.1 Security Functions 6

3 PHYSICAL PORTS AND LOGICAL INTERFACES 10

3.1 Physical Ports 10
3.2 Logical Ports 11
3.3 Link-Compatible Data Service 15
3.4 App-Compatible Data Services 16
3.5 Non-Compatible Mode (Non-Approved Mode) 17
3.6 LED Status Outputs 18

4 SECURITY RULES 20

4.1 Required Configuration 20
4.2 Cryptographic Key Management 21
4.2.1 Cryptographic Error 22
4.2.2 Key Generation 22
4.2.3 Key Establishment 22
4.2.4 Key Entry/Output 23
4.2.5 Critical Security Parameters and Public Keys 23
4.2.6 Key Zeroization 28
4.3 Self Tests 29
4.3.1 Power on Self Tests 29
4.3.2 Conditional Self Tests 30
4.3.3 Critical Function Tests 31

5 IDENTIFICATION AND AUTHENTICATION POLICY 31

6 ACCESS CONTROL POLICY 32

7 PHYSICAL SECURITY 37

8 MITIGATION OF OTHER ATTACKS 37

9 ELECTROMAGNETIC COMPATIBILITY 38

10 MODULE INSTALLATION 38

10.1 SX-590-1402 38
10.2 SD-330AC-1402 38
10.2.1 Installing the SD-330AC-1402 38
10.3 Monitoring Serial Device Server Status 40
10.4 Device Configuration 42
10.4.1 Link-Compatible Mode Configuration 42

10.4.2 App-Compatible Mode Configuration 43

Index of Tables

Table 1: Approved Cryptographic Algorithms 8
Table 2: Allowed Algorithms 8
Table 3: Non Approved Algorithms 9
Table 4: Physical Ports 10
Table 5: Link-Compatible Mode Interfaces 12
Table 6: App-Compatible Mode Interfaces 14
Table 7: Ethernet Status Outputs 18
Table 8 - Mode and Wireless Status 19
Table 9: Approved mode required Wireless port configuration 20
Table 10: App-Compatible Mode required configuration 21
Table 11: SX-590-1402 Cryptographic Keys and CSPs used in Link-Compatible and App-Compatible mode 24
Table 12: SX-590-1402 Cryptographic Keys and CSPs used in App-Compatible mode 26
Table 13: Public Keys Used in Link-Compatible and App-Compatible mode 26
Table 14: Public Keys Used in App-Compatible Mode 27
Table 15: Approved Mode services 35
Table 16: Non-approved mode services 36
Table 17: Inspection/Testing of Physical Security Mechanisms 37
Table 18: Mitigation of other attacks 37
Table 19: Ethernet Status Outputs 40
Table 20 - Mode and Wireless Status 41

1 OVERVIEW

This document is the non-proprietary security policy description for the silex technology, Inc. SX-590-1402 module and the also included SD-330AC-1402 module. The SX-590-1402 is a multi-chip standalone cryptographic module designed by silex technology. Inc. (silex) to provide an encrypted wireless LAN connection for an attached client device. In addition, application level TCP/IP encrypted socket connections using TLS 1.2[1] may be used.

The SX-590-1402 is a security module designed to be incorporated into another product, which should provide an enclosure and suitable electrical connections to the module. The SD-330AC-1402 is a multi-chip standalone product which incorporates the SX-590-1402 module along with an enclosure and connectors for some of the SX-590-1402 hardware ports Items described in this document for the SX-590-1402 apply to both the SX-590-1402 and SD-330AC-1402, unless specifically mentioned otherwise.

The client device may attach to the SX-590-1402 via a serial port or wired Ethernet port. Secure LAN communication is provided by FIPS 140-2 compliant WPA2 (AES-CCMP) encryption with shared secret key (WPA2-PSK).

This document describes the SX-590-1402 01A hardware assembly with version 2.02 firmware, and SD-330AC-1402 01A hardware assembly with version 2.02 firmware

References in this document to the SX-590-1402 apply equally to the SD-330AC-1402, unless noted otherwise.

This document may be copied in its entirety and without modification.

1.1 Operational Environment

The SX-590-1402 module is a multi-chip standalone module with operating firmware programmed in non-volatile Flash memory. Operation of the device requires connection of a power source and interface cables to the interface ports desired to be used. Operation of the device commences when power is applied and the power up self-test and initialization completes. Operation ceases when power is removed.

The module contains a limited operational environment that is enforced via the firmware load test using RSA signature verification with a SHA-256 digest. As such the cryptographic module only supports loading and running of trusted code.

[1]No parts of the TLS protocol other than the KDF have been tested by the CAVP and CMVP

The SX-590-1402 has been evaluated for FIPS 140-2 compliance at the following levels:

Security Requirements Area	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.2 Approved Modes

The SX-590-1402 has two approved modes of operation. In the Link-Compatible mode, the Wireless Port data link is encrypted. Security is only claimed for the Wireless data link between the SX-590-1402 and the Access Point to which is it connected. No security is claimed beyond the link to the Wireless Access Point. A valid 32 byte shared key is required to be entered as defined in section 4.2.4 to be in this approved mode. The Cryptographic Officer is responsible for ensuring the key's strength.

In App-Compatible mode, in addition to the Wireless Port data link encryption provided by the Link-Compatible mode, the Application TLS service is available to provide TLS transport security on an end-to-end network connection to the Serial Data port. TLS uses RSA wrapping only, more details provided in table 15.

In order to change modes, a reset of the device is always needed.

2 CRYPTOGRAPHIC BOUNDARY

The SX-590-1402 Cryptographic Module is composed of the SX-590 hardware module and associated firmware. It consists of a printed circuit assembly (PCA) with processor, memory and peripherals as shown in the block diagram below. All components shown are within the cryptographic boundary, which is the physical limit of the module. The external interfaces are through electrical connections to the interface connector, and the antenna connector. Firmware is stored in the flash memory of the system and loaded into random access memory for execution.

All firmware executed by the SX-590-1402 is within the cryptographic boundary.

Figure 1 - SX-590-1402 Cryptographic Module

The SD-330AC-1402 packages the SX-590-1402 module in an enclosure on a daughterboard with physical connectors and port interface circuitry. The included SX-590-1402 provides all cryptographic functions, and the cryptographic boundary of the SD-330AC-1402 is that of the enclosed SX-590-1402.

Figure 2 - SD-330AC-1402 Cryptographic Module

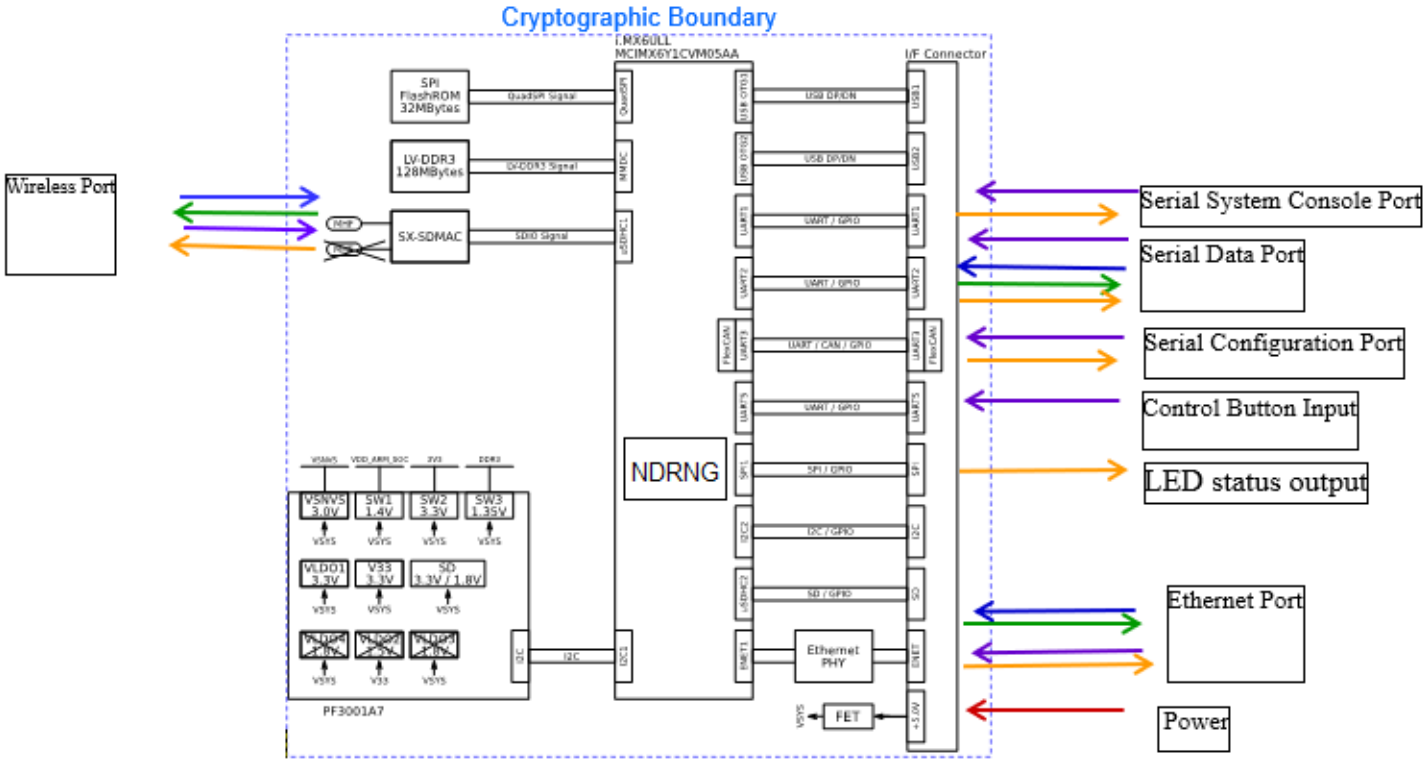


Figure 3 - SX-590-1402 Cryptographic Module Block Diagram

Port Key	
→	Data Input Port
←	Data Output Port
→	Control Port
←	Status Port
→	Power
----------	Cryptographic Boundary

2.1 Security Functions

The tables below indicates the cryptographic algorithms provided by the module. The additional algorithms listed on the certificates are tested but not used by the module.

AVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves, or Moduli	Use	Approved Modes Using the Algorithm
C1997	AES	FIPS 197 SP800-38A	ECB, CCM	128, 256[2]	Data Encryption / Decryption	Link-Compatible App-Compatible
	AES	FIPS 197 SP800-38A	CBC, GCM[3]	128, 256	Data Encryption / Decryption	App-Compatible
	RSA	FIPS 186-4	PKCS #1.5, SHA-256	4096	Digital Signature Verification	Link-Compatible App-Compatible
	CVL	SP 800-56B	RSADP	2048	Key Unwrapping	App Compatible
	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest	Link-Compatible App-Compatible
	SHS	FIPS 180-4	SHA-384		Message Digest	App-Compatible
	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256,	128 256	Message Authentication	Link-Compatible App-Compatible
	HMAC	FIPS 198-1	HMAC-SHA-384	384	Message Authentication	App-Compatible
C2191	DRBG	SP800-90A	CTR -AES	256	Deterministic	Link-Compatible

[2] The 256 key size is only used in the AES-ECB prerequisite required for AES-GCM-256; the module does not support AES-CCM-256.
[3] AES GCM IV generation is performed in accordance with Scenario 1 of IG A.5 TLS 1.2 protocol IV generation.The application closes the TLS session after 2^41 bytes have been transferred, so the IV will be incremented at most 2^41 times (at 1 byte/TLS record worst case) which is less than the 2^64 limit.

AVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves, or Moduli	Use	Approved Modes Using the Algorithm
					Random Bit Generation	App-Compatible
C2011, C2017	KBKDF	SP 800-108	HMAC-SHA-1 HMAC-SHA-256		Key Derivation	Link-Compatible App-Compatible
C2012	CVL KDF-TLS	TLS 1.2 SP800-135 rev 1			Key Derivation	App-Compatible

Table 1: Approved Cryptographic Algorithms

The module also uses the following allowed algorithms

Algorithm	Caveat	Use	Approved Modes Using the Algorithm
Hardware NDRNG		Seeds the DRBG with a minimum security strength of 112 bits	Link-Compatible App-Compatible
TLS v1.2 RSA key wrapping	allowed until 2023.12.31 per FIPS 140-2 IG D.9 RSA-based key wrapping/unwrapping algorithm that uses an RSA modulus that is 2048 bits long.	Key Wrapping	App-Compatible

Table 2: Allowed Algorithms

The module uses the following non-approved algorithms. These non-approved algorithms are only available in Non-Compatible mode, which is not an approved mode of operation.

Algorithm	Use
MD5	Wireless link establishment in Non-Compatible mode
RC4	Wireless link encryption in Non-Compatible mode
HMAC-MD5	Wireless link establishment in Non-Compatible mode
ECC DHE (non-compliant)	Key Agreement in Non-Compatible mode (see required configuration section 19)
ECDSA (non-compliant)	Key Generation for Key Agreement in Non-Compatible mode (see required configuration section 19)
RSA (non-compliant)	CA Public Key Chain Validation of peer in Non-Compatible mode (see required configuration section 19)
RSA key wrapping (non-compliant)	RSA key with non-approved key size (not 2048 bits)

Table 3: Non Approved Algorithms

3 PHYSICAL PORTS AND LOGICAL INTERFACES

3.1 Physical Ports

The following physical ports are available on the SX-590-1402

Port Name	Sub-Port name	Description
System connector		High density connector with pins assigned for the sub-ports listed below.
	Power	Power (+5V and ground) connections

	Ethernet	Ethernet 10/100 wired network interface
	Serial Data port	Serial Port for data transfer
	Serial Configuration Port	Serial port for Configuration and status
	Serial System Console Port	Serial port for status
	Control button input	Control input, active low
	LED status output	Status outputs, active low and connected to LEDs on the SD-330AC-1402
Wireless		u.FL connector for antenna attachment

Table 4: Physical Ports

3.2 Logical Ports

The SX-590-1402 has logical interfaces for transfer of data and for configuration and control of the unit. These logical interfaces may share a physical port. The application firmware in the SX-590-1402 separates and routes the data to the appropriate internal firmware task associated with the logical interface. For network ports (Ethernet, Wireless) this separation is based on the TCP or UDP protocol port number. For the serial port, data or control/status mode is controlled by specific protocol strings, only one mode is active at a time.

The following table describes the logical interfaces of the unit when operating in the FIPS 140-2 approved link mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data Input	Serial Data Port	Plaintext data for transmission to network
	Ethernet	Plaintext data for bridging to wireless network
	Wireless	Ciphertext data for Serial or Ethernet port

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data Output	Serial Data Port	Plaintext data received from wireless network
	Ethernet	Plaintext data received from wireless network
	Wireless	Ciphertext data from Serial or Ethernet port
Control Input	Ethernet	Plaintext Control data for Configuration Service received via Telnet
		Control data for Configuration Service received via HTTP
		Discovery Request via silex custom UDP port
	Wireless	Control data for Configuration Service received via Telnet
		Control data for Configuration Service received via HTTP
		Discovery Request via silex custom UDP port
	Control Button Input	Invoke configuration reset
	Serial Configuration Port	Control data for configuration service
	Serial System Console Port	Control data for configuration service
	Serial Data Port	Control sequence entry to invoke CLI status task
Status Output	Ethernet	Status response from Configuration Service via Telnet
		Status response from Configuration Service via HTTP
		Discovery request response
	Wireless	Status response from Configuration Service via Telnet
		Status response from Configuration Service via HTTP
		Discovery request response
	Serial Data Port	status from CLI status query
	Serial Configuration Port	status messages from Configuration Service
	Serial System Console Port	status messages

FIPS-140-2 Interface	Physical Interface	Logical Interface
	LED status output	Indicate operating mode, link status and unit error status
Power Interface	Power input	

Table 5: Link-Compatible Mode Interfaces

Please note that in Link-Compatible mode, all application level data is considered plaintext. Only the wireless link is considered ciphertext due to the link encryption thereon. In App-Compatible mode, application level ciphertext transport is available on a limited number of ports.

The following table describes the logical interfaces of the unit when operating in the FIPS 140-2 approved App-Compatible mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data input	Serial Data Port	Plaintext data for transmission to network application.
	Ethernet	Ciphertext data from designated TCP socket *
	Wireless	Ciphertext data from designated TCP socket * Note: Only Ethernet or Wireless interface is active for a current session, determined by the existence (or not) of an Ethernet link during the module initialization
		* Note: After 2^41 bytes have been transferred on any one encrypted serial to network connection, the connection will be closed. This forces a new connection to be established with a new session key.
Data Output	Serial Data Port	Plaintext data received from wireless application
	Ethernet	Ciphertext data received from Serial data port to designated TCP socket

FIPS-140-2 Interface	Physical Interface	Logical Interface
	Wireless	Ciphertext data received from Serial data port to designated TCP socket
Control Input	Ethernet	Control data for Configuration Service via HTTPS
		Discovery Request via silex custom UDP port
	Wireless	Control data for Configuration Service via HTTPS
		Discovery Request via silex custom UDP port
	Control Button Input	Invoke configuration reset
	Serial Configuration Port	Control data for Configuration Service
	Serial System Console Port	Control data for configuration service
	Serial Data Port	Control sequence entry to invoke CLI status task
Status Output	Ethernet	status data via HTTPS
		Discovery Request response
	Wireless	status data via HTTPS
		Discovery Request response
	Serial Data Port	status from CLI status query
	Serial Configuration Port	status messages from Configuration Service
	Serial System Console Port	status messages
	LED status output	Indicate operating mode, link status and unit error status
Power Interface	Power input	

Table 6: App-Compatible Mode Interfaces

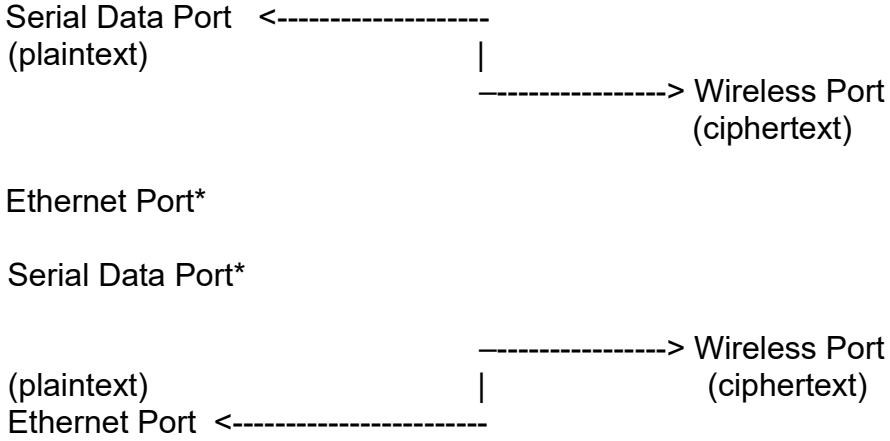
When the module enters an error state, all Data Input and Data Output interfaces are disabled. If an error state is encountered, the LED status output will indicate the error by blinking in a pattern until the unit is reset. The unit will not send or receive any data until the reset is complete.

The SX-590-1402 performs cryptographic self-tests during initialization after power up or a firmware induced reset. Until the self-tests are complete, no data input or output interfaces are active. If the self-test fails, the unit will enter an error state.

The Data Output interfaces are logically disconnected from the processes that perform key generation and zeroization. No plaintext key information is output through the Data Output interfaces or Status interfaces at any time.

3.3 Link-Compatible Data Service

The Link-Compatible mode is an approved mode of operation which only provides physical link security. The service provided is Wireless network port encryption, in one of two configurations:



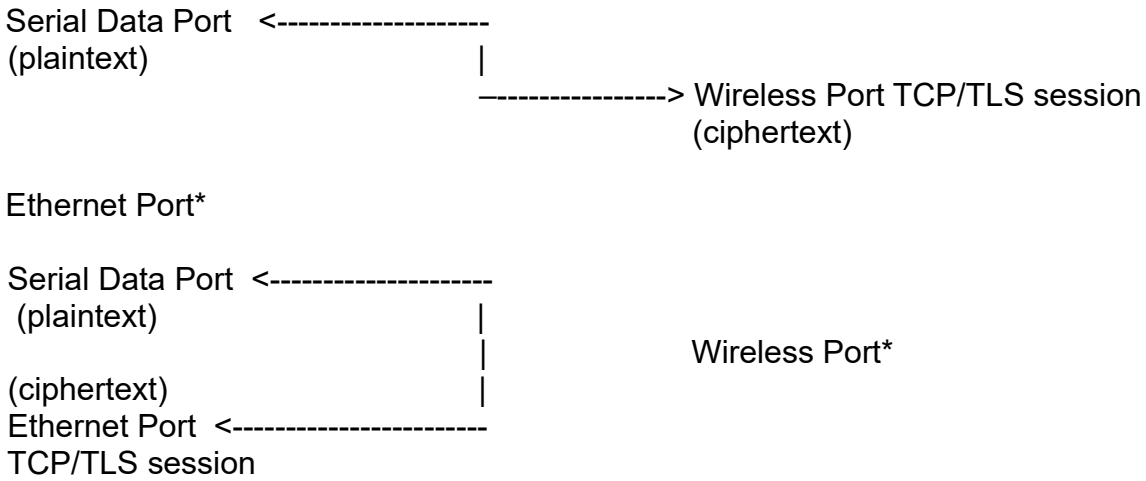
* Only one of the Ethernet Port or Serial Data port can be logically connected to the Wireless port. The other port (depending on the configuration) is logically disconnected from data transfer (input or output).

Only one of the Ethernet Port or Wireless Port is active as a network port at a time. The unit must be reset to use a different network port. Serial Data Port to Ethernet Port data connection is not permitted in Link-Compatible mode.

Link-Compatible mode is configured by the Cryptographic Officer. The unit must be reset before the mode selection takes effect.

3.4 App-Compatible Data Services

In App-Compatible mode, in addition to the Wireless Port encryption, if the Serial Data Port is used it must be connected over a TCP connection protected by a TLS session with approved encryption.



* Only one of the Ethernet Port or Wireless Port is active as a network port at a time. The unit must be reset to use a different network port.

App-Compatible mode is configured by the Cryptographic Officer. The unit must be reset before the mode selection takes effect.

3.5 Non-Compatible Mode (Non-Approved Mode)

The SX-590-1402 may operate in Non-Compatible mode, which is a FIPS 140-2 non-approved mode of operation. No security is claimed in the mode, and all data ports are considered plaintext.

To enter this mode, the Cryptographic Officer must configure the device for the Non-Compatible mode of operation, reset the compatible mode configuration to the default state to remove existing non-volatile CSPs, zeroize the unused space in the non-volatile r/w file system, and then reset the unit to begin operation in the Non-Compatible mode.

All cryptographic algorithms used in the approved modes of operation (see table Table 1) are available in the Non-Compatible mode. In addition, the non allowed MD5, RC4 and HMAC-MD5 algorithms are used to support the legacy TKIP Wireless LAN encryption method for systems which required this (strongly not recommended).

The Non-Compatible mode also allows the silex technology Inc. proprietary FLDP production test service to run. This service provides functional tests to verify the module hardware operation. No data transfer operations are performed by this service, no cryptographic operations are performed by this service, and the unit configuration and firmware are not modified by it.

3.6 LED Status Outputs

The LED status outputs indicate the operating mode and network (Ethernet and Wireless) port status as shown below.

The Ethernet port status is shown as follows:

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO1 GPIO5	RJ45 yellow RJ45 green	Yellow: OFF Yellow Green: OFF	The wired LAN cable is not connected.
		LED Yellow: OFF Green Green: ON	Wired LAN connected by 10BASE-T.
		LED Yellow: ON Green: ON	Wired LAN connected by 100BASE-TX.

Table 7: Ethernet Status Outputs

The SX-590-1402 displays status on 3 GPIO lines as shown in this section. When used in the SD-330AC-1402, the GPIO lines control the LEDs on the top of the enclosure as described.

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO8	Orange LED	Off	The unit is not powered
		On	The unit is powered and active
		Blinking*	Firmware update is in progress **(Important:** *Do not power off the module during the update process)*

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO7	Yellow LED	Off	No wireless link
		Blink	Associated with AP, IP address not acquired
		On	Associated with AP & IP address acquired
GPIO6	Green LED	Off	Non-Compatible mode
		ON	FIPS 140-2 Link-Compatible mode
		Blink	FIPS 140-2 App-Compatible mode
GPIO8 GPIO7 GPIO6	Orange LED Green LED Yellow LED	All blink alternating	Firmware detected error, unit must be reset

Table 8 - Mode and Wireless Status

4 SECURITY RULES

4.1 Required Configuration

When the SX-590-1402 operates in a FIPS 140-2 approved mode, Wireless port link encryption is required. The wireless security configuration must be set as shown in the table below. Use with these parameters set to any value not in the table is not FIPS 140-2 compliant.

Item	Required Setting
Wireless Encryption Mode	WPA2 (AES-CCMP)
Wireless Authentication	PSK
Radio mode	Infrastructure

Table 9: Approved mode required Wireless port configuration

NOTE: The default setting includes a known PSK value. The Cryptographic officer MUST configure the device with a different PSK value before operating the device. Operation of the device using the default PSK value is NOT FIPS 140-2 compliant.

The SX-590-1402 allows other security settings for interoperability in the Non-Compatible mode. However, use of the SX-590-1402 in Non-Compatible mode is not FIPS 140-2 compliant.

The Cryptographic Officer must be aware that in Link-Compatible mode all configuration program inputs are in plaintext for purposes of FIPS 140-2 compliance regardless of the transport encoding used. The only FIPS 140-2 cryptographic protection in Link-Compatible mode claimed for this module is for the wireless link between the unit and an associated Access Point.

In App-Compatible mode, the following application parameters must be set as shown in the table below:

Item	Setting
NW BRIDGE	Disable
APPTLS TLSECC	Disable
APPTLS TLSRSA	Enable
APPTLS CACERT	Not Configured

Table 10: App-Compatible Mode required configuration

In App-Compatible mode, the transport protocols are limited to those using approved encryption. If the encryption option is used for the raw TCP port protocol, or the ECable protocol, App-Compatible mode must be enabled. In addition, the Ethernet port to Wireless port bridging option must be disabled in App-Compatible mode.

In App-Compatible mode, the Cryptographic Officer must load a 2048 bit RSA key pair. No other size is allowed in the approved mode of operation.

The compatible mode and Non-Compatible mode configurations are kept separate. No operations in Non-Compatible mode affect the compatible mode configuration (and vice-versa).

ECC DH Ephemeral Key Agreement cannot be used in the approved modes.

4.2 Cryptographic Key Management

The module supports AES for encryption and decryption, RSA for authentication and key transport, and HMAC-SHA-n for message authentication. Each of these algorithms requires key material for secure operation.

4.2.1 Cryptographic Error

When the module enters an error state, all Data Input and Data Output interfaces are disabled. If an error state is encountered, the LED status output will indicate the error by blinking in a pattern until the unit is reset. The unit will not send or receive any data until the reset is complete.

4.2.2 Key Generation

When TLS RSA key wrapping is used, the pre-master secret is generated directly from the output of an approved DRBG.

4.2.3 Key Establishment

The wireless link keys are established using the 802.11i key establishment protocol, with the WPA2-PSK being used as the 802.11i pairwise master key. The 802.11i key establishment uses the SP800-108 KDF algorithms. The WPA2-PSK value must have a strength of at least 112 bits.

Session keys used for application network encryption are established during the TLS handshake establishing the connection using RSA key wrapping to establish the TLS Pre Master Secret. The TLS KDF is used to derive the TLS Master Secret and TLS session keys.

Nonce values used in key agreement and key derivation protocols are generated using an approved DRBG.

The module supports one RSA key size of 2048 bits. As allowed by NIST SP800-57, the RSA encryption within the TLS session establishment provides a minimum of 112 bits of encryption strength. The remaining elements of the key establishment process provide at least 112 bits of security.

4.2.4 Key Entry/Output

For the Wireless link, the WPA2-PSK shared key value is entered into the module by the Cryptographic Officer. This shared key value is a 32 byte key and not a passphrase. The shared key value should be provided to the Cryptographic Officer via a secure method and must be entered on an isolated network (manual transport/electronic entry). The Cryptographic Officer must have physical control of the module or the device containing the module during the key entry operation. The PSK is never output from the module once entered.

The module RSA private keys and corresponding public keys and certificates must be entered into the module in plaintext form by the Cryptographic Officer on an isolated network (manual transport/electronic entry). The Cryptographic Officer must have physical control of the module or the device containing the module during the key entry operation. Once entered, the RSA private key is never output from the module. The public key certificate is provided to the authenticating peer during TLS based authentication.

Session Keys used for wireless link encryption are established during wireless authentication with the Access Point using the SP800-108 KDFs. Session keys used for application end-to-end encryption are established during the TLS session set up on the TCP connection using the TLS KDF. Session Keys are never output from the module.

4.2.5 Critical Security Parameters and Public Keys

The first table below summarizes the cryptographic keys and CSPs used by the module in both Link-Compatible and App-Compatible mode. The second table shows those CSPs used only in App-Compatible mode.

Name	Description	Algorithm	Generation	Establishment	Entry	Output	Storage	Protection	Zeroization	Key to Entity
WPA2 Pre-shared key (PSK)	Used for shared key authentication and session key derivation on the Wireless port link	256 bit shared secret.	External	n/a	manually transported/ electronically entered	None	FLASH & RAM	The module contains no function for output of this value. Only the Cryptographic Officer may replace this value.	zeroize by following zeroize procedure in Security Policy	Entry is related to the Cryptographic Officer role via password. Use is related to the User role via retrieval from configuration memory and checksum verification.
802.11i Pairwise Master Key (PMK)	Key input value to the WPA SP800-108 KDF function.	256 bit Shared secret	n/a	Copied from PSK at session start.	n/a	None	RAM	The module contains no function for output of this value. Only the Cryptographic Officer may replace or zero this value (in PSK configuration).	Reset unit to zeroize RAM	Related to User role contained int the WPA state related to the wireless Access Point connection.
Wireless Session Keys	Keys for encrypting and decrypting unicast and broadcast traffic on the wireless network link.	AES (CCMP) 128 bit	n/a	derived from the 802.11i PMK. using SP800-108 KDF	n/a	None	RAM	The module contains no function for input or output of this value It is established dynamically as needed.	Reset unit to zeroize RAM	Related to User role contained int the wireless driver state related to the wireless Access Point connection.
DRBG_internal_state	Internal state information and temporary variables for approved DRBG function.	CTR DRBG AES-256	n/a	Established during system start up	n/a	n/a	RAM	The module contains no function for input or output of this value It is established dynamically as needed.	zeroized on unit restart	Related to User role when random data required in normal operation.
SP800-108-KDF_internal_state	Internal state of the SP800-108 KDF	SP800-108 KDF HMAC-SHA-1 HMAC-SHA-256	n/a	Established as required during Wireless port link communications	n/a	n/a	RAM	The module contains no function for input or output of this value It is established dynamically as needed	zeroized on unit restart	Related to User role during TLS session establishment

Table 11: SX-590-1402 Cryptographic Keys and CSPs used in Link-Compatible and App-Compatible mode

Name	Description	Algorithm	Generation	Establishment	Entry	Output	Storage	Protection	Zeroization	Key to Entity
App_RSA_Private_Key	Used to decrypt pre-master secret information if RSA key exchange used.	2048 bit RSA key unwrap	External	n/a	manually transported/ electronically entered	None	Flash & RAM	The module contains no function for output of the private key. Only the Cryptographic officer may input, or zeroize the module private key.	zeroize by following zeroize procedure in Security Policy	Entry is related to the Cryptographic Officer roll via password. Use is related to the User role via retrieval from configuration memory and checksum verification.
App_TLS Pre_Master_Secret	Value from initial handshake on application session set up used for subsequent key generation	Shared Secret (384 bits)	For RSA key exchange in client role, output of approved DRBG	RSA key exchange	RSA key exchange used in server role, transmitted from the client peer encrypted by the App_RSA_Public_Key	If RSA key exchange used in client role, transmitted to the server peer encrypted by the App_Peer_RSA_Public_Key	RAM	The value is generated randomly and encrypted if transmitted. This is a transient value, there is no function for input or modification of this value.	zeroized after APP TLS Master Secret is derived.	Related to User role in the TLS session establishment
App_TLS_Master_Secret	Derived value used as input to session key derivation	384 bit Shared secret	n/a	Derived from the APP TLS Pre-Master Secret with the TLS KDF	n/a	None	RAM	The module contains no function for output of this value. It is computed during the TLS handshake and not used outside the TLS authentication process.	zeroized when TLS session ends zeroized on unit restart	Related to User role in the TLS session establishment
App_TLS_Session_key_block	Derived information used to set up TLS session encryption	AES GCM (128 and 256 bit keys) AES CBC (128 and 256 bit keys)	n/a	Derived from the APP TLS master secret using the TLS KDF	n/a	None	RAM	The module contains no function for input or output of this value. It is computed during the TLS handshake and not used outside the TLS authentication process.	zeroized when TLS initial handshake completes zeroized on unit restart	Related to User role in the TLS session establishment

Name	Description	Algorithm	Generation	Establishment	Entry	Output	Storage	Protection	Zeroization	Key to Entity
App_TLS_session_keys	Keys used for encryption and decryption of data in TLS session	AES GCM (128 and 256 bit keys) AES CBC (128 and 256 bit keys)	n/a	Copied from App_TLS session_key_block at session start up	n/a	None	RAM	The module contains no function for input or output of this value. It is computed during the TLS handshake and not used outside the TLS session	zeroized when TLS session ends zeroized on unit restart	Related to User role in the TLS session establishment
App_TLS-KDF_internal_state	Internal state of the application TLS KDF .	TLS KDF (SP800-135)	n/a	Established as required during TLS session	n/a	n/a	RAM	The module contains no function for input or output of this value It is established dynamically as needed and zeroized after use	zeroized after each computation	Related to User role during TLS session establishment

Table 12: SX-590-1402 Cryptographic Keys and CSPs used in App-Compatible mode

The module uses the following public keys in both Link-Compatible and App-Compatible mode.

Name	Description	Algorithm	Generation	Establishment	Entry	Output	Storage	Protection	Key to Entity
Firmware_Verification_Key	Key used to verify firmware signature for firmware update verification	4096 bit RSA	External	Programmed into the firmware image	Programmed into the firmware image	n/a	R/O Flash	The value is never output, and is used only by the firmware to verify candidate firmware upload files.	Related to the Cryptographic Officer role when a firmware update is attempted

Table 13: Public Keys Used in Link-Compatible and App-Compatible mode

The module uses the following public keys only in App-Compatible mode.

Name	Description	Algorithm	Generation	Establishment	Entry	Output	Storage	Protection	Key to Entity
App_RSA_Public_Key	Public key corresponding to App_RSA_Private_Key Used during the application TLS session establishment	2048 bit RSA	external	n/a	Manually transported/ electronically entered	Transmitted to session peer in X509 certificate during TLS session establishment. Can also be uploaded by Cryptographic Officer in a certificate for transport to remote peer..	Flash & RAM	The key certificate is only output during the TLS authentication set up, if requested by the session peer, and when explicitly requested by the Cryptographic Officer. The Cryptographic Officer may load a new key.	Entry is related to the Cryptographic Officer role for entry. Output via digital certificate is related to the Cryptographic Officer. Use is related to the User role via retrieval from configuration memory Output is related to the user role in the TLS handshake.
App_Peer_RSA_Public_Key	Application session peer RSA public key. Used during TLS session establishment. Used to encrypt the TLS pre-master key.	2048 bit RSA	External	n/a	Transmitted from the TLS peer during TLS session establishment.	n/a	RAM	Application session peer public key is never output and cannot be modified.	Related to User role initiating the application session.

Table 14: Public Keys Used in App-Compatible Mode

4.2.6 Key Zeroization

All non-volatile items, can be cleared by resetting the unit configuration to default values. The values can be replaced with new values at any time by using the web configuration GUI or the configuration task CLI.

After resetting the configuration items to their default value, the Cryptographic officer must overwrite the r/w file store free space with a Configuration console CLI command provided for the purpose. The unit should then be reset to zeroize volatile items. The free space in RAM used for dynamic allocations is overwritten with zeros during start up.

4.3 Self-Tests

4.3.1 Power on Self Tests

The power on self-tests consists of a firmware integrity test, configuration memory integrity test, and known answer tests for the cryptographic algorithm implementations.

The firmware integrity test is performed when the module is initialized after power-up or a soft reset. The boot code verifies a checksum on the Linux kernel segment before loading and executing it. During start up, the kernel and root file systems are read, and a SHA-256 sum of each segment is computed and compared to the saved value from when the firmware was last updated. The firmware integrity test passes if and only if the computed SHA-256 sum matches the value previously stored with the firmware image. If the integrity test fails the firmware enters an error state.

When the configuration file is read an integrity test reads the configuration information from the flash storage, computes a 16 bit checksum, and compares it to the stored value in the configuration when it was written. If the values do not match the module enters a transient error state and the configuration memory is zeroized and reset to the factory default values.

The module also performs the known answer tests on the following algorithms using the tests in the OpenSSL FIPS 140-2 approved engine. All tests are performed at start up no matter what mode the module is operating in.

Algorithm	Test Attributes
HMAC	One KAT per SHA1, SHA224, SHA256, SHA384 and SHA512 Per IG 9.3, this testing covers SHA POST requirements.
AES	Separate encrypt and decrypt, ECB mode, 128 bit key length
AES CCM	Separate encrypt and decrypt, 192 key length
AES GCM	Separate encrypt and decrypt, 256 key length
RSA	Sign and verify using 2048 bit key, SHA256, PKCS#1
DRBG	CTR_DRBG: AES, 256 bit with and without derivation function

The module control firmware adds the following known answer tests

Algorithm	Test Attributes
TLS-KDF	One KAT each for SHA-256 and SHA-384 based KDF PRF algorithms
SP800-108 KDF	One KAT each for SHA-1 based counter after fixed data and SHA-256 based counter before fixed data

4.3.2 Conditional Self Tests

The module performs the following conditional self tests. These tests may be executed in any mode of operation, if the triggering condition is met.

Test	Procedure
DRBG Health Tests	Tested as required by [SP80090A] Section 11, see note 1 below
DRBG Continuous Random Number Generator Test	FIPS 1402 continuous test for stuck fault
Non-approved hardware NDRNG Continuous Random Number Generator Test	Continuous test
Firmware update file validation	RSA-4096-SHA256 firmware file signature verified after download and before flash firmware image is modified.

Failure of any Conditional Self Test results in a transition to the CRYPTO_ERROR state, and no further data transfer can occur until the module is reset.

Note 1: The DRBG Health Tests are run at power on self test, and cyclically after 2^24 bits have been generated. Also, if a bit pattern of all ‘0’ or all ‘1’ is generated, the health checks will be run. If the bit pattern is identical to the previous bit pattern generated, then the health tests will be run as well. The health tests cover the following tests: known answer testing, testing the instantiate function, testing the generate function, and testing the reseed function.

4.3.3 Critical Function Tests

The SX-590-1402 does not implement any Critical Function Tests

5 IDENTIFICATION AND AUTHENTICATION POLICY

The module supports two roles, a User and a Cryptographic Officer role. The roles are implicitly assumed when a module function is invoked. Sending data to one of the module Data Input ports implicitly selects the User role. Sending data to one of the module Control Input ports implicitly selects the Cryptographic Officer role.

The User role supplies data to the module via the Ethernet or Serial Data port for encryption and transmission on the Wireless Port, and receives data decrypted upon receipt from the Wireless port and intended for the Ethernet or Serial Data port. In addition, in the App-Compatible mode, the data supplied to the Serial Data port is transmitted via an encrypted TLS connection to a remote host via either the Ethernet or Wireless network port.

Only one user operator is allowed. Multiple concurrent operators are not allowed.

The Cryptographic Officer role configures the module for operation, including the Wireless authentication and encryption keys and parameters and application encryption keys and parameters, as well as non-cryptographic configuration such as the target AP SSID. Other tasks performed by the Cryptographic Officer include key zeroization and checking the status of the cryptographic module.

6 ACCESS CONTROL POLICY

The following table indicates the services available to each role within the module in the approved modes of operation.

Role	Mode	Service	Keys and CSPs	Access
Cryptographic Officer	Link-Compatible	Module Configuration (*)	WPA2 Pre Shared Key App_RSA_Private_Key App_RSA_Public_Key	Write
			DRBG_internal_state,	Compute and use
	App-Compatible	Module Configuration (*)	WPA2 Pre Shared Key	Write
			App_RSA_Private_Key App_RSA_Public_Key	Write and Use
			App_Peer_RSA_Public_Key	Use
			DRBG_internal_state, App_TLS_Pre_Master_Secret, App_TLS Master secret, App_TLS_Session_key_block App_TLS_session keys APP_TLS-KDF_internal_state	Compute and use
	Link-Compatible App-Compatible	Zeroize	All keys and other CSPs listed in section 4.2.5 except the Firmware_verification_key public key	Zeroize
	Link-Compatible App-Compatible	Firmware Update	Firmware_verification_key public key	Use
	Link-Compatible App-Compatible	LED Show status	No CSPs are used or displayed in status information	n/a

Role	Mode	Service	Keys and CSPs	Access
	Link-Compatible App-Compatible	Button Control	All keys and other CSPs listed in section 22 except the Firmware_verification_key public key, App_RSA_Private_Key and App_RSA_Public_Key	Zeroize
			App_RSA_Private_Key App_RSA_Public_Key	Delete[4]
	Link-Compatible App-Compatible	Discovery Status	No CSPs are used or displayed	n/a
User	Link-Compatible App-Compatible	Wireless Link Data Encryption (used in all approved modes)	WPA2 Pre Shared Key (PSK), 802.11i Pairwise Master Key	Use
			Wireless Session Keys SP800-108-KDF_internal_state DRBG_internal_state	Compute and use
	Link-Compatible	Serial Data port to Wireless Network (*)	No CSPs are used or displayed by the service.	n/a
	Link-Compatible	Wired Network to Wireless network Bridging (*)	No CSPs are used or displayed by the service.	n/a
	App-Compatible	Application TLS (*)	App_Peer_RSA_Public_Key App_RSA_Private_Key App_RSA_Public_Key	Use

[4] The files containing the App_RSA_Private_Key and App_RSA_Public_Key are deleted from the file system, but the free space is not overwritten. The Cryptographic Officer must explicitly invoke the overwrite operation if zeroization is required.

Role	Mode	Service	Keys and CSPs	Access
			App_TLS_Pre_Master_Secret, App_TLS Master secret, App_TLS_Session_key_block App_TLS_session keys DRBG_internal_state, APP_TLS-KDF_internal_state	Compute and use
	Link-Compatible App-Compatible	Self Test	No CSPs are used for self tests, known key values are used	n/a
	Link-Compatible App-Compatible	LED Show status	No CSPs are used or displayed in status information	n/a
		* These services use the Wireless Link Data Encryption service for Wireless port network I/O		

Table 15: Approved Mode services

The following table indicates the services available in the non-approved Non-Compatible mode of operation:

Role	Mode	Service
Cryptographic Officer	Non-Compatible	Module Configuration (*)
		Zeroize (*)
		LED Show status
		Button Control (*)
		Discovery Status

Role	Mode	Service
		(*) Configuration changes by these services affect only the Non-Compatible mode configuration
User	Non-Compatible	Wireless Link Data Encryption
		Serial Data port to Network (*)
		Wired Network to Wireless network Bridging (*)
		Application TLS (*)
		Self Test
		LED Show status
		silex production test (FLDP)
		(*) These services use the Wireless Link Data Encryption service for Wireless port network I/O

Table 16: Non-approved mode services

7 PHYSICAL SECURITY

The SX-590-1402 is validated as a FIPS 140-2 level 1 module and therefore there is no physical security requirement. The user of the SX-590-1402 module should provide an enclosure to limit access to the module. The SD-330AC-1402 provides a production grade physical enclosure, but no additional physical security mechanism.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
n/a	n/a	n/a

Table 17: Inspection/Testing of Physical Security Mechanisms

8 MITIGATION OF OTHER ATTACKS

The module is not designed to mitigate any other attacks.

Other Attacks	Mitigation Mechanism	Specific Limitations
n/a	n/a	n/a

Table 18: Mitigation of other attacks

9 ELECTROMAGNETIC COMPATIBILITY

The module conforms to FCC Regulations Part 15, Class B. The module SX-SDMAC radio is certified for intentional emissions with FCC ID N6C-SDMAC

10 MODULE INSTALLATION

10.1 SX-590-1402

The SX-590-1402 is intended to be embedded in a Manufacturer's product. The Manufacturer of the product containing the SX-590-1402 shall document the proper installation of the product.

10.2 SD-330AC-1402

The SD-330AC-1402 is a silex technology product incorporating the SX-590-1402. The SD-330AC shipping kit includes a power adapter for supplying power to the SD-330AC-1402 power input jack. Note that +5V power can also be provided via pin 9 of the SD-330AC-1402 DB-9 connector for the Serial Data Port. The installer will need to provide the Ethernet and/or serial cable to connect your client device to the SD-330AC-1402.

10.2.1 Installing the SD-330AC-1402

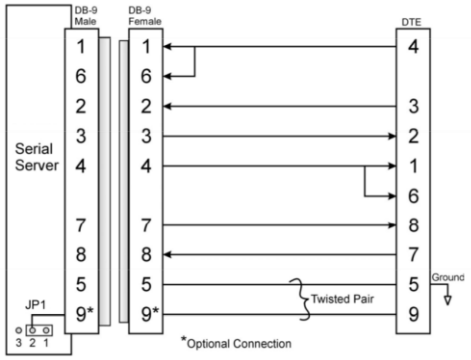
Follow the steps below to install the SD-330AC-1402. The unit default settings should be sufficient for many serial connections; however, some of the configuration settings may have to be changed for your particular installation.

1. Before attempting to install the SD-330AC-1402, make sure you have installed and set up your client device as described in the documentation that came with the device.

2. Write down the 12-digit MAC (Media Access Code) address printed on the label located on the bottom of the SD-330AC-1402 (for example: 84253F6C0165). You may need this number in order to configure the Serial Device Server.

3. Connect the SD-330AC-1402 to your client device. If you are using serial RS-232, you may use standard PC cabling (you should normally use a null modem crossover cable). The 9-pin connector pin-outs and cabling are as follows:

Pin	Description
1	DCD (Data Carrier Detect) Input
6	DSR (Data Set Ready) Input
2	RxD (Receive Data) Input
3	TxD (Transmit Data) Output
4	DTR (Data Terminal Ready) Output
7	RTS (Request To Send) Output
8	CTS (Clear To Send) Input
5	Ground
9	RI (Ring) Input or +5 VDC Power Input (Optional)



RS-232 connector pin-outs and cabling

If you are connecting to the client device via Ethernet, you will need to use an Ethernet crossover cable to connect the client device to the SD-330AC-1402. Note in this case, you will need to configure the device via a PC connected to the SD-330AC-1402 Ethernet port before you can connect the client device.

4. Plug the SD-330AC-1402 power supply adapter into a suitable AC receptacle, and then plug the power supply cable into the SD-330AC-1402. Alternatively, you can use pin 9 on the 9-pin DB-9 connector to provide power to the Serial Device Server (1 amp @ +5V is required).

When power is applied the SD-330AC-1402 will run through a sequence of power-up diagnostics for a few seconds, then the Orange status led will be lit..

- The unit powers up in the Normal mode, which provides for connection from the network to device(s) connected to the Serial Data Port of the SD-330AC-1402.
- If the orange LED blinks continuously in a regular pattern, or all the LED blink in a patter, a problem exists. If this is the case, try powering the unit OFF and then ON again.

5. Connect the SD-330AC-1402 to the configuration host device you will use for configuration (usually a PC or laptop) directly using a category 5 (CAT5) Ethernet crossover cable. Alternatively, both the host device and SD-330AC-1402 can be connected to an Ethernet hub or switch, as long as no other devices are connected to the nub or switch.. Then cycle power on the device to ensure the unit uses the Ethernet port as the active port for configuration. The wireless networking will not be enabled in this case.

6. The SD-330AC-1402's IP address must be configured before a network connection is available. If the configuration host offers DHCP (Dynamic Host Configuration Protocol), the SD-330AC-1402 will automatically search for a DHCP server upon power up and obtain an IP address. If the configuration host does not offer DHCP, after a few attempts the SD-330AC-1402 will use a default fixed IP address of 169.254.111.111. The default IP parameters may be changed during the initial configuration.

10.3 Monitoring Serial Device Server Status

The LED status outputs indicate the operating mode and network (Ethernet and Wireless) port status as shown below.

The Ethernet port status is shown as follows:

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO1 GPIO5	RJ45 yellow RJ45 green	Yellow: OFF Yellow Green: OFF	The wired LAN cable is not connected.
		LED Yellow: OFF Green Green: ON	Wired LAN connected by 10BASE-T.
		LED Yellow: ON Green: ON	Wired LAN connected by 100BASE-TX.

Table 19: Ethernet Status Outputs

The SX-590-1402 displays status on 3 GPIO lines as shown in this section. When used in the SD-330AC-1402, the GPIO lines control the LEDs on the top of the enclosure as described.

SX-590-1402 LED status signal	SD-330AC-1402 LED	Light pattern	Status
GPIO8	Orange LED	Off	The unit is not powered
		On	The unit is powered and active
		Blinking*	Firmware update is in progress **(Important:** *Do not power off the module during the update process)*
GPIO7	Yellow LED	Off	No wireless link
		Blink	Associated with AP, IP address not acquired
		On	Associated with AP & IP address acquired
GPIO6	Green LED	Off	Non-compatible mode
		ON	Link-Compatible mode
		Blink	App-Compatible mode
GPIO8 GPIO7 GPIO6	Orange LED Green LED Yellow LED	All blink alternating	Firmware detected error, unit must be reset

Table 20 - Mode and Wireless Status

10.4 Device Configuration

Once the product containing the SX-590-1402, such as the SD-330AC-1402, is installed the Cryptographic Officer must configure the device as desired for operation, pursuant to the Cryptographic Office Guidance Manual. Depending on the operational environment, the device may need to be installed twice – once in a secure location for loading of the necessary keys for subsequent operation, and then again after configuration to the target operating environment.

10.4.1 Link-Compatible Mode Configuration

To configure the device for Link-Compatible Mode operation, the Cryptographic Officer must access the Configuration CLI, either directly via the Serial Configuration Port, or via the local network via the Configuration GUI. The following commands must be executed via the Configuration CLI:

SET FIPS1402 LINK ENA
SET NW WPAPSK <64 hex character PSK value>
SAVE

Note the factory default setting includes a default PSK value. The PSK value configured must be different than the default configuration value to properly operate in the Link-Compatible mode.

After configuring the above values, the unit must be reset. Verify that the GPIO6/Green LED signal is asserted to indicate the Link-Compatible mode is active.

10.4.2 App-Compatible Mode Configuration

To configure the device for App-Compatible mode operation, in addition to the Link-Compatible configuration described in the preceding section, the Cryptographic Operator must load an RSA public and private key pair of 2048 bits into the unit through the Configuration GUI. If the Configuration GUI will be used for subsequent configuration, the HTTPS protocol should be enabled on the GUI TCP page. Either the raw TCP protocol should be configured for the desired TCP port through the I/O Services page, or the eCable client should be configured to connect to the desired remote IP address/port through the I/O port page. One of these services must be used to provide the application Serial Data Port to network connection. Only one or the other can be enabled at a time.

Once the keys and desired service have been configured, App-Compatible mode is configured with the Configuration CLI command:

SET FIPS1402 APP ENA

The unit must be reset for the App-Compatible mode to become active. Verify the GPIO6/Green LED signal is blinking to indicate the App-Compatible mode is active.