SX-590-1402
FIPS 140-2 Level 1 User Guidance Manual

Revision A
Date: 2020.10.27

REVISION HISTORY

Rev. No.	Date	Revision by	Comments
A	2020.10.27	Lee Aydelotte	Initial Release

Table of Contents

1 OVERVIEW

This document is the User Guidance manual 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 (WPA-PSK).

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

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

2 DEVICE OPERATION

2.1 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 signing of 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

2.2 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.

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.

2.3 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.

CAVP 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 Random Bit Generation	Link-Compatible App-Compatible
C2011, C2017	KDF	SP 800-108	HMAC-SHA-1 HMAC-SHA-256		Key Derivation	Link-Compatible App-Compatible
C2012	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

[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.

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

Copyright 2020 silex technology Inc. All rights reserved

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
ECDSA (non-compliant)	Key Generation for Key Agreement in Non-Compatible mode
RSA (non-compliant)	CA Public Key Chain Validation of peer in Non-Compatible mode
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 unit.

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
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

FIPS-140-2 Interface	Physical Interface	Logical Interface
	Serial System Console Port	status messages
	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
	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

FIPS-140-2 Interface	Physical Interface	Logical Interface
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 key information is output through the Data Output interfaces or Status interfaces at any time.

3.3 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)*
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 8 - Mode and Wireless Status

4 INSTALLATION AND USE

Before the SX-590-1402 may be used in the target environment, it must be properly configured by a Cryptographic Officer with the necessary security parameters and network identification values. Please refer to the Cryptographic User Guidance Manual for details of this procedure.

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

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.

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 9: 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 Installation

To install the device, it must be connected to a target client device and power applied. A cable should be attached between the target device and either the wired Ethernet port, or the Serial Data Port as appropriate. The antenna should be attached to the u.fl antenna connector for best performance (this is done at the factory for the SD-330AC-1402). The antenna should be positioned so that there are a minimum number of obstacles (walls, filing cabinets, etc.) between the antenna and the target Access Point. Power must be supplied to the unit. For the SX-590-1402, refer to the end product containing the module for installation details. On the SD-330AC-1402, this is done either via the power jack, using the power adapter provided with the unit, or equivalent) or by providing +5V power on pin 9 of the serial port DB-9 connector. Power should not be supplied from both sources at the same time.

4.3 Use

Once properly configured by the Cryptographic Officer, use of the SX-590-1402 is quite simple. Simple enable the power supply to the unit (by plugging it in or throwing the appropriate power switch). After a short initialization period, the SX-590-1402 will be operational and ready to secure wireless LAN communication to the attached device. If the Cryptographic Officer has configured the device for App-Compatible mode, secure network connection via a TLS/TCP connection to a Serial Data Port service will also be available. The state of the module can be observed by monitoring the status signals as shown in Table 8.

To terminate use of the device, remove power from it.

4.4 Self Tests

4.5 Self Tests

4.5.1 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 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
AES CMAC	Sign and verify CBC mode, 128, 192, 256 key lengths
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

4.5.2 Conditional Self Tests

The module performs the following conditional self tests:

Algorithm	Procedure
DRBG Health Test	Tested as required by [SP80090A] Section 11
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-SHA256 firmware file signature verified after download and before flash firmware image is modified.

4.5.3 Self Test Failure

If one of the unit self tests detects an error, the unit enters an error state. This is indicated on the LED status lines as defined in Table 8. The user must reset the device by removing and the reapplying power. If the error recurs repeatedly, please notify the appropriate people in your organization for diagnosis, repair or replacement.

5 MAINTENANCE

There is no user maintenance involved in the use of the SX-590-1402. If a defect is observed in the operation of the device, it should be referred to security management personnel for replacement or repair.

6 ELECTROMAGNETIC COMPATIBILITY

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