SX-500
FIPS 140-2 Level 1 Security Policy

Revision A
Date: 2009.08.13

REVISION HISTORY

Rev. No.	Date	Revision by	Comments
A	2009.08.13	Lee Aydelotte	Initial Version

Table of Contents

1 OVERVIEW

The SX-500 is a multi-chip standalone cryptographic module designed by Silex Technology America, Inc. (STA) to provide an encrypted wireless LAN connection for an attached client device. The client device may attach to the SX-500 via a serial port or wired Ethernet port. Secure LAN communication is provided by FIPS 140-2 compliant WPA2 (AES-CCMP) encryption with manual key distribution (WPA-PSK) or IEEE 802.11i key exchange with a RADIUS server using EAP protocols such as EAP-TLS or PEAP.

The SX-500 contains the following Approved Cryptographic Algorithms:

- AES – ECB, CBC and CCM modes
- RSA
- SHA-1
- HMAC SHA-1
- SP800-90 DRBG

This document describes the SX-500 hardware assembly, STA part number 132-00188-120 rev. B or rev. C with version 2.02 main firmware and version 3.1 boot loader.

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

1.1 Operational Environment

The module is a stand alone device 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 HMAC-SHA1. As such the cryptographic module only supports loading and running of trusted code.

The SX-500 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	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

2 CRYPTOGRAPHIC BOUNDARY

The Cryptographic Module in the SX-500 is composed of the SX-500 hardware module and associated firmware. The cryptographic boundary of the SX-500 hardware module, STA part number 132-00188-120 rev. B or rev. C, is the physical enclosure of the assembly as shown.

Figure 1 - SX-500 Cryptographic Module

The Cryptographic Module is a multiple-chip standalone module. Inside the enclosure is a print 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 indicated by the dashed line. The dashed line maps to the module enclosure. The external interfaces are through the jacks and connectors shown at the edge of the diagram, and the pushbutton switch and status LEDs. Firmware is stored in the flash memory of the system, and loaded into random access memory for execution.

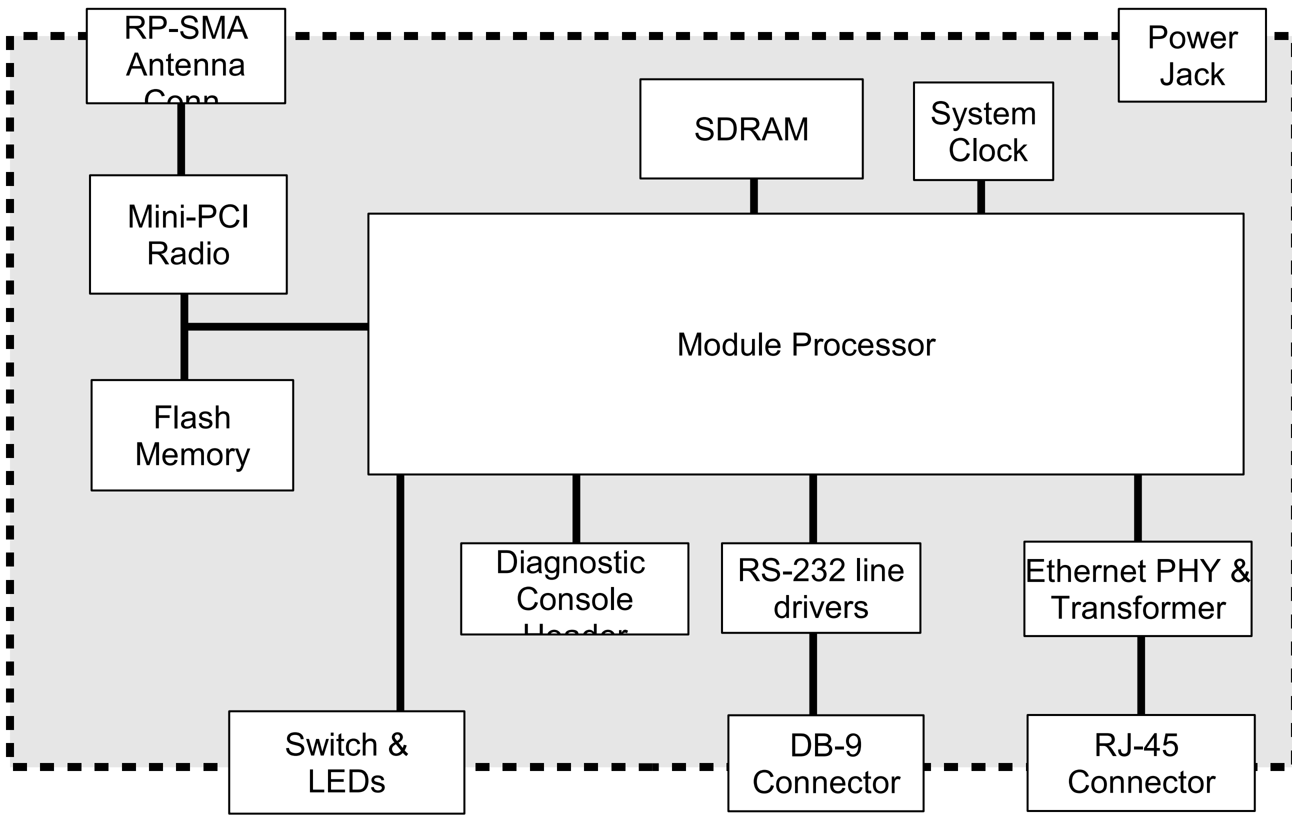

Figure 2 - SX-500 Cryptographic Module Block Diagram

2.1 Security Functions

The table below indicates the cryptographic algorithms provided by the module.

Algorithm	Approved	Algorithm Certificate Number
AES (ECB, CBC)	Y	#1138, #1139
AES (CCM)	Y	#1140
RSA (sign/verify)	Y	#540
SHA-1	Y	#1058, #1059
HMAC SHA-1	Y	#647, #648
SP800-90 DRBG	Y	#19
Non-approved algorithms		
MD5	N	n/a
RC4	N	n/a
HMAC-MD5	N	n/a
MD4	N	n/a
DES	N	n/a
Hardware RNG	N	n/a

In the FIPS approved mode, the module supports AES for encryption/decryption, RSA for authentication and key transport, HMAC SHA-1 and SHA-1 for message authentication, and SP800-90 DRBG for key generation. The module supports the following non-Approved functions as allowable for use in the FIPS mode of operation:

- non-deterministic hardware RNG (used for seeding the Approved SP800-90 DRBG in FIPS mode)
- EAP-TLS (for key establishment in FIPS mode as per FIPS 140-2 IG 7.1)
- PEAP (for key establishment in FIPS mode as per FIPS 140-2 IG 7.1)
- 802.11i KDF (for key establishment in FIPS mode as per FIPS 140-2 IG 7.2)

3 PHYSICAL PORTS AND LOGICAL INTERFACES

3.1 Physical Ports

Please refer to figure 3 for a diagram of the available physical ports. These are as follows:

Port Name	Description
Power	Jack for attachment of external power supply
Ethernet	RJ-45 connector for attachment of Ethernet cable
Serial	DB-9 connector for attachment of serial interface cable
Wireless	RP-SMA connector for attachment of an external antenna
Button	Momentary push button
LED	Green, Yellow and Orange LEDs

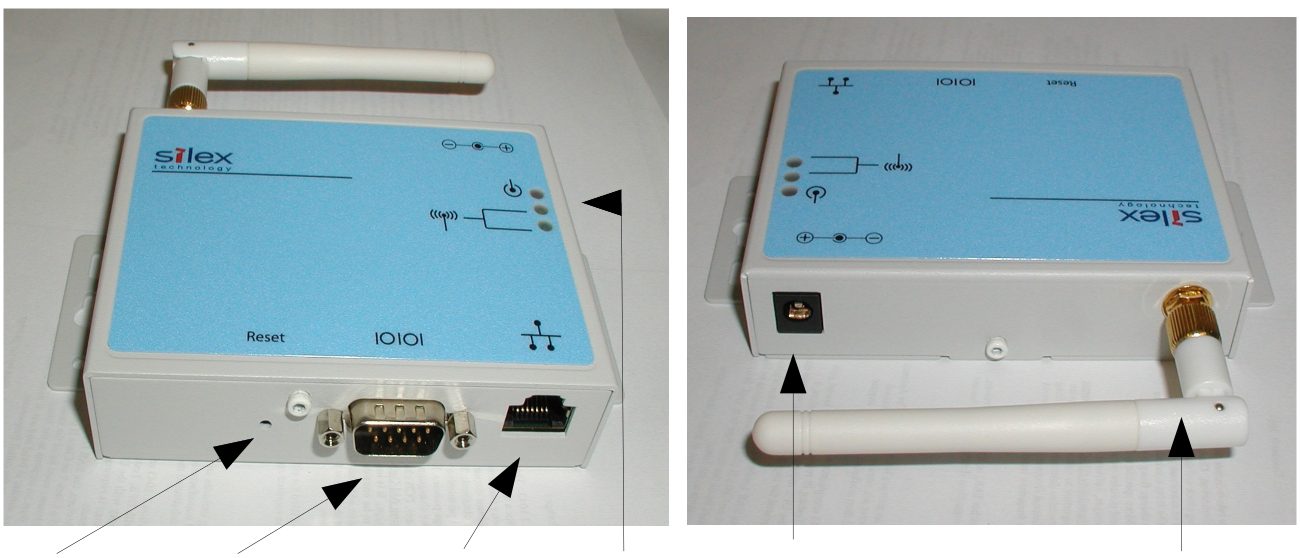

Figure 3 - SX-500 Cryptographic Module Ports

3.2 Logical Ports

The SX-500 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-500 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. Serial port control/status mode is only available if the unit is explicitly configured to allow it. The following table describes the logical interfaces of the unit when operating in a FIPS 140-2 approved mode.

FIPS-140-2 Interface	Physical Interface	Logical Interface
Data Input	Serial	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	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 console task received via Telnet
		Plaintext Control data for web config task received via HTTP
	Wireless	Control data for console task received via Telnet
		Control data for web config task received via HTTP
	Button	Invoke configuration/status function
Status Output	Ethernet	Plaintext Status response from console task via Telnet
		Plaintext Status response from web config via HTTP
	Wireless	Status response from console task via Telnet
		Status response from web config via HTTP
	Serial	Plaintext Status from button push
	LEDs	Indicate link and unit error status
Power Interface	Power input	
	Serial	

When the module enters an error state, all Data Input and Data Output interfaces are disabled. If an error state is encountered, the LED interface will indicate the error by blinking for several seconds, and then the unit will reset. The unit will not send or receive any data until the reset is complete.

The SX-500 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 during key generation or zeroization.

4 SECURITY RULES

4.1 Required Configuration

For the SX-500 to operate in FIPS 140-2 approved mode, the wireless security configuration must be set as follows:

Item	Required Setting
Wireless Encryption Mode	WPA2 (AES-CCMP)
Wireless Authentication	PSK or TLS or PEAP

The SX-500 allows other security settings for interoperability in non FIPS 140-2 environments. However, use of the SX-500 with any wireless security settings other than those indicated above is not FIPS 140-2 compliant.

The Cryptographic Officer must be aware that 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 claimed for this module is for the wireless link between the unit and an associated Access Point.

The Crypographic officer must zeroize the module when transitioning the device configuration from a FIPS-140-2 approved mode to a non-approved mode.

There are two types of bypass states possible with the module (non-approved modes). The first is to use any wireless encryption/authentication combination not specified above as being FIPS 140-2 compliant and then reset the unit. The second is to configure the unit to not be in Ethernet to Wireless mode, plug in a wired Ethernet cable, and then reset the unit.

In addition to the wireless security settings above, the following settings must be made for operation in FIPS 140-2 mode:

Item	Required Setting
HTTPS	Disabled (factory default)
S-Telnet	Disabled (factory default)
TCP data service SSL	Disabled (factory default)
Serial port console mode string	NULL (disabled – factory default)
Serial port filter	TRAP (factory default)

4.2 Cryptographic Key Management

The module supports AES for encryption and decryption, RSA for authentication and key transport, and HMAC-SHA-1 for message authentication. Each of these algorithms requires key material for secure operation.

4.2.1 Key Generation

The only key generation performed by the module is the optional generation of an RSA private key and corresponding public key and self signed certificate. This key is used for TLS session establishment. Key generation is performed using the SP800-90 FIPS approved deterministic random number generator.

Nonce values used in authentication protocols are generated using the SP800-90 FIPS approved random number generator.

4.2.2 Key Establishment

If EAP authentication methods (EAP-TLS or PEAP) are used, the TLS session keys are established at the end of the TLS handshake, as is the TLS Master Session Key (MSK) or PEAP Master Session Key. The wireless link keys are established using the 802.11i key establishment protocol, with either the TLS MSK, PEAP MSK, or WPA2-PSK being used as the 802.11i pairwise master key.

The module supports RSA key sizes of 1024 and 2048 bits. As allowed by NIST SP800-57, the RSA encryption within the TLS session establishment provides 80 bits or 112 bits of encryption strength. The remaining elements of the key establishment process provide at least 112 bits of security, as long as the WPA2-PSK value (if used) has at least 112 bits of security.

4.2.3 Key Entry/Output

If PSK authentication is used, the shared key value is entered into the module by the cryptographic officer. 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 PSK is never output from the module once entered.

The module RSA private key and corresponding public key and certificate may be entered into the module in plaintext form by the Cryptographic Officer on an isolated network (manual transport/electronic entry). 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. Session Keys are never output from the module.

4.2.4 Key Storage

The module stores the following values in either non-volatile flash memory or volatile random access memory when in use.

NAME	Description	Algorithm	Generation
Module RSA Private Key	Used to authenticate the module as supplicant during the TLS handshake.	1024-2048 bit RSA	Outside the module or by the module with input from the approved DRBG
TLS Pre-Master Secret (PMK)	Random nonce value used during TLS session establishment	384 bit Shared secret	Generated from approved DRBG.
TLS master secret	Shared secret from which new session keys can be created. Created using asymmetric cryptography	512 bit Shared secret	Negotiated during the TLS handshake.
TLS Session Encryption Key	Key used to encrypt TLS session data.	AES-128 bit	Negotiated during the TLS handshake.
TLS Integrity Key	HMAC key used for integrity protection.	HMAC-SHA-1 160 bits	Negotiated during the TLS handshake.
EAP-TLS Master Session Key	This session key is independently established by both the server and supplicant (SX-500) at the end of the EAP-TLS handshake. This key is used as the 802.11i PMK to establish 802.11i session keys.	512 bit Shared secret	Established from TLS master secret during the EAP-TLS handshake.
DRBG Seed	The seed for the approved DRBG	SP800-90 (Hash)	Generated from processor internal hardware random number generator.
PEAP Tunnel Key (PTK)	Used to establish session keys	AES-128 bit	Negotiated during the TLS handshake.
PEAP Master Session Key	This session key is independently establishd by both the server and the supplicant (SX-500) at the end of the PEAP handshake.	512 bit Shared secret	Establishd during the PEAP handshake.
WPA2-PSK	WPA2 Pre-shared key. Used for shared key authentication and session key generation when RADIUS EAP authentication is not available.	256 bit shared secret.	Generated externally. Entered by the Cryptographic officer.
802.11i Pairwise master key	Secret value used for 802.11 key establishment algorithm.	256 bit shared secret.	First half of Master session key from TLS or PEAP authentication handshake, or equal to the WPA2-PSK in PSK mode.
Wireless session keys	Keys for encrypting and decrypting unicast and broadcast traffic on the wireless network link.	AES (CCMP) 128 bit	Established by derivation from the 802.11i PMK...
Internal DRBG state	Internal state information and temporary variables for approved DRBG function.	SP800-90 (Hash)	Established during system startup and updated as required during operation.

NAME	Description	Algorithm	Generation
Cryptographic Officer password	Value entered by the Cryptographic Officer to enable configuration operations.	8-128 bit shared secret	Generated externally. Entered by the Cryptographic Officer.
Temporary TLS-PRF variables	Internal state of the TLS-PRF function.	TLS-PRF	Established when TLS-PRF function invoked.

Figure 4 - SX-500 Cryptographic Keys and CSPs

NAME	Description	Algorithm	Generation
Module RSA Public Key	Used during the TLS handshake for authentication (signing).	1024-2048 bit RSA	Outside the module or by the module with input from the approved DRBG
Certificate signing key	RSA certificate signing key. used in certificate signing chain to validate the RADIUS server RSA public key	1024-2048 bit RSA	Outside the module.
RADIUS server public key	RADIUS server RSA public key. Used during TLS session establishment. Used to encrypt the TLS pre-master key.	1024-2048 bit RSA	Outside the module.

Figure 5 - SX-500 Public Keys

4.2.5 Key Zeroization

All key values both in volatile and non-volatile memory may be explicitly zeroized by the CRYPO officer by submitting the ZEROKEYS command to the module console configuration task. When it is determined that a transient value (e.g., TLS session key) is no longer required, it is zeroized by the module before the associated memory is released.

4.3 Self Tests

4.3.1 Power on Self Tests

The power on self test 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. A 32-bit checksum is computed on the stored firmware image, and compared to the expected value. The firmware integrity test passes if and only if the computed checksum matches the value previously stored with the firmware image. If the integrity test fails the firmware will not be allowed to execute.

The configuration memory 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. 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:

AES – CBC & CCM
RSA
DRBG
SHA-1
HMAC-SHA-1

MD5
TLS-PRF

4.3.2 Conditional Self Tests

The module performs the following conditional self tests:

Algorithm	Procedure
Approved DRBG	Continuous test
Non-approved hardware RNG	Continuous test
Wireless link encryption bypass test	First packet encryption verification
Firmware load	Firmware keyed hash verified after download and before flash firmware image is modified.
Encryption algorithms	Known answer tests from the previous section when directed by the Cryptographic Officer
RSA key generation	Pairwise consistency test after key generated.

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 to the Ethernet or 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 Data port.

The Cryptographic Officer role configures the module for operation, including the Wireless authentication and encryption parameters, as well as non-cryptographic configuration such as the target AP SSID. Other tasks performed by the Cryptographic Officer include key entry (RSA and PSK), key zeroization, initiate the algorithm known answer tests on demand and check the status of the cryptographic module.

The Cryptographic Officer role requires a password when accessed from one of the physical network ports. As a level 1 device, no minimum length password is required for approved operation, but it is recommended that the password be at least 8 characters.

There is at most one encrypted wireless link active at any one time. Multiple concurrent operators are not supported by the module.

6 ACCESS CONTROL POLICY

The following table indicates the services available to each role within the module.

Role	Service	Keys and CSPs	Access
Cryptographic Officer	Module Configuration, including key entry and operating mode (including bypass) and firmware upgrade via HTTP, Telnet, and TFTP each of which is a plaintext service.	RSA Public and Private keys, WPA Pre-shared key, Cryptographic Officer password.	Write
	Show status	No CSPs are displayed in status information	Read
	Zeroize	RSA Public and Private keys, WPA Pre-shared key, TLS-Pre Master Secret, TLS Master secret, TLS session encryption key, TLS integrity key, EAP-TLS MSK, PEAP Tunnel Key, PEAP Master Session Key, WPA PSK, 802.11i pairwise master key, Wireless Session Keys, Cryptographic officer password, DRBG internal state, PRF internal state	Zeroize
	Self Test	No CSPs are used for self tests, known key values are used	None
	Firmware update	Firmware Integrity key	Use
User	EAP-TLS	RSA private key	Use
		TLS pre-master secret, TLS Master secret, TLS integrity key, TLS session key, TLS Master session key, 802.11i pairwise master key, wireless session keys	Compute(as part of authentication) and use.
	EAP-PEAP	RSA private key	Use
		TLS pre-master secret, TLS Master secret, PEAP tunnel key, TLS integrity key, PEAP Master Session Key, 802.11i pairwise master key,	Compute and use

Role	Service	Keys and CSPs	Access
		wireless session keys	
	WPA-PSK	PSK, 802.11i pairwise master key, wireless session keys	Use
	AES-CCMP link encryption	Wireless Session Keys	Compute and use
	Show status	No CSPs are displayed in status information	Read

7 PHYSICAL SECURITY

The SX-500 is validated as a FIPS 140-2 level 1 module and therefore there is no physical security requirement. The SX-500 provides a production grade physical enclosure, but no additional physical security mechanism.

8 MITIGATION OF OTHER ATTACKS

The module is not designed to mitigate any other attacks.

9 ELECTROMAGNETIC COMPATIBILITY

The module conforms to FCC Regulations Part 15, Class B. The module radio is certified for intentional emissions with FCC ID N6C-SX10WG.