FIPS 140-2 Non-Proprietary Security Policy for LiteScape SPAR

Contents

1. Introduction

This non-proprietary Cryptographic Module Security Policy describes how the LiteScape SPAR (Secure Profile Authentication Reader)
meets the security requirements of Federal Information Processing Standards (FIPS) 140-2, and how it operates in a secure FIPS 140-2 mode. The policy was prepared as part of the Level 2 FIPS 140-2 validation of the LiteScape SPAR.

This document provides an overview of the LiteScape SPAR and explains the secure configuration and operation of the cryptographic module. It also explains the general features and functionality of the LiteScape SPAR and addresses the required configuration for the FIPS mode of operation.

The FIPS 140-2 publication, "Security Requirements for Cryptographic Modules" details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available at the following National Institute of Standards and Technology (NIST) website:

http://csrc.nist.gov/groups/STM/index.html

This document refers to the Cryptographic as the LiteScape SPAR or the SPAR or the device.

This document and other FIPS 140-2 validation submissions were prepared by CyberData Corp. on behalf of LiteScape Technologies. With the exception of this non-proprietary Cryptographic Module Security Policy, the entire FIPS 140-2 submission package is proprietary to CyberData Corp. and/or LiteScape Technologies. For access to these documents – under nondisclosure agreement – please contact CyberData Corp and LiteScape Technologies.

2. The LiteScape SPAR

The LiteScape SPAR is a network device (FCC ID: WBA-010835-010914) that allows for identification of users via identification cards and biometrics. It is designed to communicate via TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) with a centralized server (SPM) and a VoIP telephone. The SPM can send commands to the SPAR and receives responses and asynchronous input data from the SPAR. The SPAR acts as a proxy between the phone and the SPM.

Features include:

- Magnetic card reader
- RFID reader
- Fingerprint reader
- 10/100 Ethernet connection with one hub port
- 256-bit AES encryption
- Powered via Power over Ethernet (PoE) or 48VDC adapter
- Field upgradeable firmware

3. The LiteScape SPAR as a Cryptographic Module

The plastic case that fully encloses the SPAR serves as the cryptographic boundary for the multi-chip standalone cryptographic module. All functions and features described in this document are performed by hardware and software within the case. The SPAR uses the following cryptographic algorithms:

Section of Firmware	Algorithm	Certificate Number
Bootloader	HMAC SHA-1	HMAC: #**457**, SHA: #**822**
Netflash executable	HMAC SHA-1	HMAC: #**455**, SHA: #**820**
SPAR executable	AES 256-bit	**#822**
	HMAC SHA-1	HMAC: #**456**, SHA:# **821**

3.1 Composition of Exectuables

All filenames, with the exception of netflash -- which is contained as part of the ROMFS image --, are not actually used by the SPAR since everything is booted and loaded, based on physical addresses within the flash memory.

The image filenames are:

spar_uboot_52b5.bin – bootloader; 52b5 is the version

image102f-835.bin – Linux kernel; 1.0.2f is the version

romdisk107-835.img – ROMFS/Filesystem; 1.0.7is the version

netflash – netflash executable (contained in ROMFS)

spar – spar executable (contained in ROMFS)

From a cryptographic module standpoint, the bootloader verifies the integrity of the non-volatile configuration, the kernel, the filesystem, and itself. If all is well, it copies the kernel to ram and boots the kernel.

The kernel mounts the filesystem image and provides typical system functions (access to drivers/hardware, TCP and UDP stacks, etc). There are no cryptographic functions in the kernel.

The filesystem contains all of the executable files for the SPAR.

spar (the "SPAR exectuable") is the SPAR application which runs in multiple threads. As a cryptographic module, the application verifies the integrity of the non-volatile configuration and encrypts/decrypts all communications with the SPM.

netflash (the "Netflash executable") handles firmware upgrades (both kernel and filesystem). It is launched by the SPAR executable. As a cryptographic module, netflash verifies the non-volatile configuration and verifies the integrity of the new firmware image(s) being loaded.

4. SPAR Interfaces

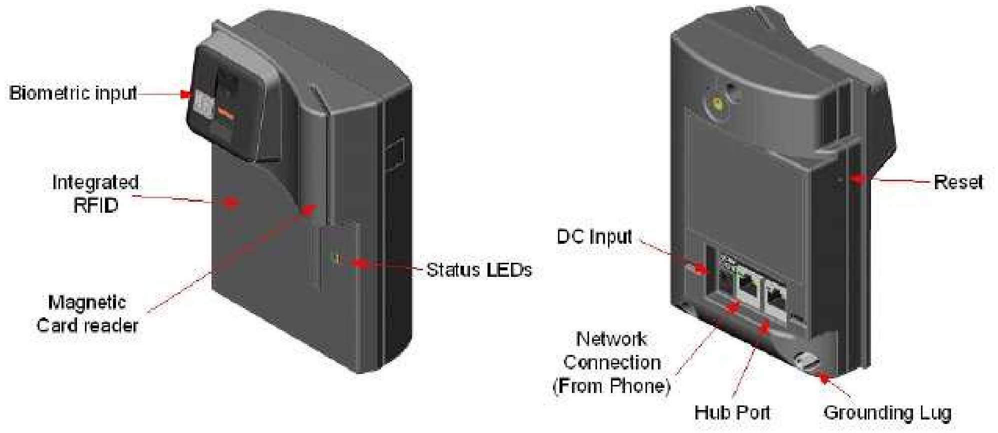

Illustration 1: SPAR Interfaces

The SPAR features two 10/100 RJ45 connectors on the rear of the device for data transfers. The front of the SPAR contains two status LEDs, a magnetic card reader, a fingerprint reader, and an area for RFID tags to be read. The actual RFID reader is not visible from the outside of the SPAR.

Table 1 details the status LEDs as they relate to the SPAR's operational state.

RED LED	GREEN LED	MODE
OFF	OFF	No power
OFF	ON	Booting
ON 0.25 seconds, OFF 0.25 seconds	OFF 0.25 seconds, ON 0.25 seconds	HMAC SHA-1 integrity test failure
ON 1 second, OFF 1 second	OFF 1 second, ON 1 second	AES self-test failure
ON 2 seconds, OFF 2 seconds	ON 2 seconds, OFF 2 seconds	HMAC SHA-1 self-test failure
ON	ON	Operational
BLINKING 10 times per second	ON	Magnetic Card or RFID read
BLINKING 10 times per second	BLINKING 10 times per second	AES key is zeroized
OFF	BLINKING 5 times per second	Settings reverted to factory defaults; safe to release reset switch

Table 1: SPAR LED Codes

If the SPAR fails any power-up self test (AES key zeroized, HMAC SHA-1 integrity test failure, HMAC SHA-1 self-test failure, AES self-test failure), it enters its “Power-up self-test failed” error state and must be returned to the manufacturer for repair. The SPAR will cease operation upon entering its failure state and will be unreachable and inoperative. It will blink an error code on its two front LEDs.

5. SPAR Roles (Identification and Authentication)

The SPAR supports three roles: Unauthenticated, User, and Crypto Officer. They are each described below.

5.1 Unauthenticated

The unauthenticated role is defined as any operator who has unauthenticated access to the module. Thus, as described in the services section below, the operator accesses the module over the RFID, fingerprint, or magnetic strip interface. When performing the phone proxy service (the service wherein the module forwards packets from the SPM to the phone or vice versa), the operator may also access the module over the Ethernet interface. Although the operator has no knowledge of or access to any of the module’s keys or CSPs, some of the user’s actions may prompt the module to send out encrypted messages, thus the user is considered to have “execute” access to the module’s AES key.

5.2 User

The User is defined as the operator who accesses the module over its Ethernet port with the correct User user name and password. The User performs services by sending encrypted service request packets which include the user name and password to the module over its Ethernet connection. When the module receives a packet, it will decrypt it, and then, if the user name and password provided are correct, and the service requested is a User service, the module will perform that service. For the module to be in FIPS approved mode, the User must change its password from the default value to something at least 6 characters in length.

5.3 Crypto Officer

The Cryptographic Officer is defined as the operator who accesses the module over its Ethernet port with the correct Crypto Officer user name and password. The Crypto Officer performs services by sending encrypted service request packets which include the user name and password to the module over its Ethernet connection. When the module receives a packet, it will decrypt it, and then, if the Crypto Officer user name and password provided are correct, and the service requested is a Crypto Officer service, the module will perform that service.

The Crypto Officer is responsible for security-related settings of the module. In particular, the Crypto Officer is responsible for initially resetting the module's AES key from its default value, and for any re-keying the module done in the future. In order for the module to remain in FIPS approved mode, the Crypto Officer must only set the module's AES key from a non-networked PC. The Crypto Officer must also change its password from the default value to something at least 6 characters in length.

6. SPAR Services (Access Control Policy)

The SPAR provides several services which are enumerated in the table below and then described in detail. All SPAR network communications use proprietary data formats. For details of these formats, please see the SPAR Software Specification in the FIPS submission package.

Service	**Role**	**Key/CSP Access: Read (R), Write (W), or Execute (X)**
Magnetic Card	Unauthenticated	AES Key: X
RFID	Unauthenticated	AES Key: X
Proxy	Unauthenticated	AES Key: X
Fingerprint (register & verify)	Unauthenticated	AES Key: X
Visual Status Output[1]	Unauthenticated	none
Reset via reset switch	Unauthenticated	HMAC Key: X
Reboot via power cycle	Unauthenticated	none
Heartbeat Request[1]	Unauthenticated	AES Key: X
Reboot (via API command)	User	AES Key: X, User Password: X
Firmware Download	User	AES Key: X, User Password: X, HMAC Key: X
Read User Configuration Items[1]	User	AES Key: X, User Password: X
Set User Configuration Items	User	AES Key: X, User Password: W, X, HMAC Key: X
Read Crypto Officer Configuration Items[1]	Crypto Officer	AES Key: X, C.O. Password: X
Store Crypto Officer Configuration Items	Crypto Officer	AES Key: X, C.O. Password: W, X, HMAC Key: X
Zeroize Keys/CSPs	Crypto Officer	AES Key:X, C.O. Password: X

1. At least part of this service constitutes Status Output.

6.1 Unauthenticated Services

6.1.1 Magnetic Card Reader

Input: Magnetic Card data

Output: Encrypted Magnetic card data passed to SPM

The SPAR features a 3-track ISO XXXX magnetic card reader. When a user swipes a magnetic card, the SPAR reads the data from the card. The SPAR does a CRC check to verify the data and counts the number of errors – if any. The SPAR assembles a packet with the above information, encrypts it, and sends it to the SPM via Ethernet.

6.1.2 RFID Reader

Input: RFID chip data
Output: Encrypted RFID chip data passed to SPM

The SPAR features an ISO XXXX RFID reader. When a user presents an RFID card, the SPAR reads the data from the card. The SPAR does a CRC check to verify the data and counts the number of errors – if any. The SPAR assembles a packet with the above information, encrypts it, and sends it to the SPM via Ethernet. The RFID reader can be enabled/disabled by the User.

6.1.3 Proxy

Input: Plaintext from Phone
Output: Ciphertext to SPM

or
Input: Ciphertext from SPM
Output: Plaintext from Phone

The SPAR acts as a proxy between the SPM and a VoIP phone. It will decrypt TCP data received from the SPM and pass it along to the phone. When TCP data is received from the phone, it will be encrypted and sent to the SPM.

6.1.4 Fingerprint Reader

Input: Fingerprint data
Output: Encrypted fingerprint data passed to SPM

The SPAR features a swipe-style fingerprint reader. During normal operation, the fingerprint reader is in “locked mode” and will not function. Upon receiving a command from the SPM, the SPAR will enable the fingerprint reader for either user registration or user verification. Typical scenarios are listed below:

User registration:

- SPM sends user registration command to SPAR
- SPAR puts fingerprint reader in registration mode
- SPM sends phone – via SPAR proxy – instructions for user to read
- User swipes finger three times
- Fingerprint reader notifies SPAR of registration success/failure

- SPAR notifies SPM of registration success/failure
- Fingerprint reader sends fingerprint template to SPAR
- SPAR encrypts fingerprint template and sends it to SPM
- SPAR deletes fingerprint from fingerprint reader's memory
- SPAR returns fingerprint reader to “locked mode”

User verification:

- SPM sends user verification command to SPAR
- SPM sends desired fingerprint template to SPAR
- SPAR sends template to fingerprint reader
- SPAR puts fingerprint reader in verification mode
- SPM sends phone – via SPAR proxy – instructions for user to read
- User swipes finger
- Fingerprint reader attempts to match user's fingerprint to template
- Fingerprint reader notifies SPAR of verification success/failure
- SPAR notifies SPM of verification success/failure
- SPAR deletes fingerprint and template from fingerprint reader's memory
- SPAR returns fingerprint reader to “locked mode”

6.1.5 Visual Status Output

Input: N/A
Output: LED status indications
This service constitutes user’s ability to obtain status information about the module via visual indicators. The indicators are: the red and green LEDs on the front of the module, the red, amber, and green LEDs in the biometric module, and the red and yellow LEDs on the ethernet ports that indicate connectivity.

6.1.6 Reset via Reset Switch

Input: Depress physical reset switch
Output: none.

This service consists of depressing the physical reset switch located on the side of the module. Doing this resets the module’s settings (including its AES key and passwords) to default values and reboots the module. As this service involves a change to the module’s non-volatile memory, the hmac signature over that memory is recalculated when the values are changed. Note that exercising this service will take the module out of FIPS approved mode.

6.1.7 Reboot via power cycle

Input: Unplug power source
Input: n/a

This service consists of rebooting the module by removing its power source (unplugging it) and then reattaching. Rebooting the module results in the module’s self tests being performed.

6.1.8 Heartbeat request

Input: encrypted XML message from SPM (exact format described in software specification)
Output: encrypted XML message to SPM (exact format described in software specification)

SPM sends message to SPAR, SPAR acknowledges if operational.

6.2 User Services

6.2.1 Reboot

Input: encrypted XML reboot request from SPM
Output: encrypted XML reboot response sent to SPM

During operation, the User can request that the SPAR reboot itself by sending the appropriate command to the diagnostic/configuration port. Rebooting the module results in the module's power-up self tests being performed.

6.2.2 Firmware Download

Input: encrypted XML firmware download request from SPM
Output: encrypted XML firmware download response to SPM

The SPAR's firmware is upgraded, remotely via TFTP, by the **User**. The SPAR's firmware is split into two images: the kernel and the ROM filesystem (or application). Both images must be uploaded separately. Before the images are burned to flash, the SPAR verifies the HMAC SHA-1 signature of each image. If the HMAC SHA-1 verification fails, the SPAR will not write the new firmware image(s) to flash.

6.2.3 Read User Configuration Items

Input: encrypted XML request from SPM
Output: configuration items as described below

The User can issue a "Configuration Read Request" in response, the SPAR will issue the following information:

- Serial number

- MAC address
- Firmware versions
- RFID reader enabled/disabled
- IP address
- Subnet mask
- Default gateway
- DHCP enabled/disabled
- DSCP (Differentiated Services Code Point; used for Quality of Service guarantees)value
- List of TCP and UDP ports assigned to various services
- List of IP addresses of known SPMs
- Phone IP address
- TFTP server IP address (used for firmware download)

6.2.4 Set User Configuration Items

Input: XML request containing configuration items

Output: XML configuration store response

The User can issue a Configuration Store Request. The SPAR will acknowledge new values, store them to flash, and reboot. If one of the changed values is stored in non-volatile memory (i.e. the User name or password), after the value has been changed, the SPAR will recalculate the HMAC signature on non-volatile memory. Note that the SPAR will never transmit the user name or password. The following settings can be changed by the User:

- RFID reader enabled/disabled
- IP address
- Subnet mask
- Default gateway
- DHCP enabled/disabled
- DSCP value
- User Name
- User password
- List of TCP and UDP ports assigned to various services
- List of IP addresses of known SPMs
- Phone IP address

- TFTP server IP address

6.3 Crypto Officer Services

6.3.1 Read Crypto Officer Configuration Items

Input: XML request containing configuration items

Output: XML configuration store response

The Crypto Officer can issue a “Configuration Read Request.” The SPAR will reply with the module’s AES mode (always 256-bit).

6.3.2 Store Crypto Officer Configuration Items

Input: XML request containing configuration items

Output: XML configuration store response

The Crypto officer may issue a “Configuration Store Request.” The SPAR will acknowledge that it accepts the new values, store them to flash, and reboot. After any of the values has been changed, the SPAR will recalculate the HMAC signature of non-volatile memory. Note that the SPAR will never transmit the Cryptographic Officer user name or password nor the AES key. Also note that any changes made by the Cryptographic Officer must be made on a closed network in order for the SPAR to continue running in FIPS approved mode. The following settings can be changed by the Cryptographic Officer:

- AES key
- Cryptographic Officer user name
- Cryptographic Officer password

6.3.3 Zeroize Keys/CSPs

Input: XML zeroize request
Output: XML zeroize response

The Cryptographic Officer can send a “zeroization” command to the SPAR via its diagnostic/configuration port. This command causes the SPAR to zeroize its stored AES key, HMAC SHA-1 key, user name and password, and Cryptographic Officer user name and password. The SPAR then stores the new zeroized values in flash and reboots itself. Note that the SPAR will be inoperative after this procedure since it will no longer be able to verify the HMAC SHA-1 signatures on its flash partitions.

7. Physical Security

The SPAR features two tamper evident labels on either side of the case. These tamper evident labels are applied by the manufacturer prior to shipment. In order to be run in FIPS approved mode, a daily inspection of the labels is required.

Illustration 2: Tamper Evident Label Intact

8. Secure Configuration

In order be be used in FIPS approved mode, the SPAR must be configured in a secure manner. That is, when a SPAR is received, it cannot be placed on a live network while its default AES key is still active. The cryptographic officer must place the SPAR on an isolated network (i.e. the SPAR would be connected to the cryptographic officer's computer via a cross-over Ethernet cable or via a hub with no other nodes attached). Once the SPAR is on the isolated network, the cryptographic officer can change the AES key from its default. It is recommended that the User also configure the SPAR's network settings on an isolated network, but it is not required for FIPS approved mode.

If it is required to change the SPAR's AES key after it has been installed, the cryptographic officer must return the SPAR to an isolated network to change the AES key. Failure to do so will result in a security compromise and the SPAR will no longer be running in FIPS approved mode.

AES keys should be non-repeating and non-sequential. Encryption keys should be randomly generated via a FIPS140 approved method. SPAR should never be installed with the default encryption key enabled.

user names and passwords must also be changed from their default values. They can be a maximum of

25 characters and are case sensitive. Valid characters include A-Z, a-z, 0-9, and the following “special characters”: ‘~!@#$%^&*()-_=+[]{}|:;,<>?

For security purposes, user names and passwords should be a minimum of 6 characters. Having a minimum length of 6 characters gives a 496,981,290,961 distinct combinations for each user name and each password. A random attempt to guess any user name or password has only a 1 in 496,981,290,961 chance of succeeding which exceeds the FIPS 140-2 requirement of 1 in 1,000,000. Testing has shown that it takes approximately 0.019 seconds to send the shortest possible command to the SPAR and receive a rejection message[1]. This results in the potential of 3,157.89 attempts at guessing in one minute. In one minute, an automated program would have a 1 in 157,377,644.9 which exceeds the FIPS 140-2 requirement of 1 in 100,000.

9. Cryptographic Key Management

The SPAR uses a variety of Critical Security Parameters during operation. Table 2 lists the various cryptographic keys used by the SPAR.

Key/CSP Name	Generation/ Algorithm	Description	Storage	Zeroization	Entered	Output
AES Key	Pre-shared secret	256-bit key used to encrypt and decrypt all communications with SPM	RAM (plain text) and non-volatile flash (plain text)	Set entire field to all zeros, store to flash and reboot	yes, by crypto officer	no
HMAC SHA-1 Key	Secret	128-bit key used to verify integrity of firmware images and non-volatile configuration	RAM (plain text) and non-volatile flash (plain text)	Set entire field to all zeros, store to flash and reboot	no	no
Passwords (crypto officer and User)	Secret	Strings between 6 and 25 characters in length used to authenticate User and Cryptographic Officer	RAM (plain text) and non-volatile flash (plain text)	Set entire fields to all zeros, replace with factory defaults, store to flash and reboot	yes	no

Table 2: Cryptographic Keys Used by the SPAR

[1] Test results detailed in proprietary package available under NDA

10. Self-Tests

The SPAR performs an array of self-tests at various points during its operation. Table 3 details these self-tests. Note that the tests labelled “power-up” happen automatically at power-up without any input from or action by the operator, and thus can be initiated on demand by power-cycling the device. Furthermore, in the tests labelled “known answer,” the noted cryptographic algorithm is provided with known values and the result of the calculation is compared with the expected answer. If the expected and calculated values do not match, the test fails, and the module enters its “Power-up Self test failed” error state. In this state, the SPAR will cease operation and will be unreachable and inoperative. Its two front LEDs will alternate blinking.

Application	Test(s) performed
Bootloader	Power-up Firmware Integrity test: HMAC SHA-1 signature verification of bootloader
	Power-up Firmware Integrity Test: HMAC SHA-1 signature verification of kernel
	Power-up Firmware Integrity Test: HMAC SHA-1 signature verification of filesystem
	Power-up Firmware Integrity Test: HMAC SHA-1 signature verification of non-volatile configuration
SPAR Application	Power-up AES decryption known answer test
	Power-up AES encryption known answer test
	Power-up HMAC SHA-1 known answer test (with underlying SHA-1 known answer test)
Firmware Upgrade (Netflash) Application	Power-Up HMAC SHA-1 known answer test (with underlying SHA-1 known answer test) Firmware Load Test (HMAC SHA-1 signature verification of filesystem and kernel)

Table 3: Self-Tests

11. Mitigation of Other Attacks

The SPAR does not claim to mitigate any attacks in a FIPS approved mode of operation other than the protection explicitly provided by the SPAR and stated in this document.