KoolSpan SecurEdge Lock
Hardware Part Number LRF05123
Firmware Version 3.1.1
Security Policy

FIPS 140-2 Level 2 Validation

July 2007
Version 1.02

1 Introduction 3
1.1 Document History 4
1.2 Acronyms and Abbreviations 4
2 KoolSpan SecurEdge Lock 5
2.1 Functional Overview 5
2.2 Module Description 7
2.2.1 Logical Block Diagram 8
2.2.2 Hardware Block Diagram 8
2.3 Module Ports and Interfaces 10
3 Security Functions 11
4 FIPS Approved Mode of Operation 12
5 Identification and Authentication 12
6 Cryptographic Keys and CSPs 14
7 Roles and Services 15
8 Access Control 16
9 Physical Security 17
10 Self Tests 19
11 Mitigation of Attacks 20
12 References 20

1 Introduction

This document is the Security Policy for KoolSpan SecurEdge Lock cryptographic module. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the KoolSpan SecurEdge Lock cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard, and information on the CMV program, can be found at http://csrc.nist.gov/cryptval. More information describing the Lock application can be found at http://www.KoolSpan.com.

In this document, the KoolSpan SecurEdge Lock device is also referred to as “the module” or “the Lock”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “KoolSpan’ - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The KoolSpan SecurEdge Lock cryptographic module meets the overall requirements applicable to Level 2 security for FIPS 140-2 as shown in Table 1.

Table 1. Cryptographic Module Security Requirements.

Security Requirements Section	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2

1.1 Document History

Document Version History

Version	Date	Comments	Name
0.01	1/10/06	Initial Draft	Ward Rosenberry
0.02	2/1/06	2nd Draft	Ward Rosenberry
0.02	2/15/06	Submission Draft	Ward Rosenberry
0.03	3/9/06	Corrections	Ward Rosenberry
0.04	5/1/06	Corrections 2	Ward Rosenberry
1.00	10/30/06	Final Submission	Ward Rosenberry

1.2 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
SHA-1	Secure Hash Algorithm

2 KoolSpan SecurEdge Lock

2.1 Functional Overview

The KoolSpan SecurEdge solution provides an integrated authentication and remote access solution using smart cards, not servers. The KoolSpan solution consists of a device on a LAN called a "lock" and an external (outside the LAN) device called a "key". The key is a USB token containing an Axalto Cryptoflex EGate 32 USB smart card device that plugs into a remote computer (like a laptop). The key securely stores authentication data and cryptographic keys used to establish a secure session (tunnel) between the laptop and the lock device on the LAN. At the completion of user authentication, the lock and the remote laptop share an AES key that decrypts incoming data and encrypts outgoing data.

One lock can support many (1024) keys. A management server on the LAN creates a secure connection to the lock using a similar key device. The management server uses that secure connection to update end user authentication data stored on the lock. The management server plays another important role; It initializes the lock and all its related keys so they share certain cryptographic keys used to establish the secure tunnel and to pre-authenticate end users.

Features:

- The module generates a per-packet 256-bit AES key for data encryption and decryption for increased security.
- The lock and key establish an ISO Layer 2 (Data Link layer) connection that allows end users to map network drives and perform other operations as though the user was logged in directly to the LAN.
- Locks may be hierarchical or in series for layered protection of resources.

Figure 1 illustrates one cryptographic module configuration that connects wireless users to an internal wired LAN. Communications between the wireless user and the KoolSpan SecurEdge Lock are encrypted. The lock decrypts the incoming wireless data and sends it to the wired LAN. Clear text data coming from the LAN is encrypted and sent to the wireless user.

Figure 1. Functional View of the Cryptographic Module.

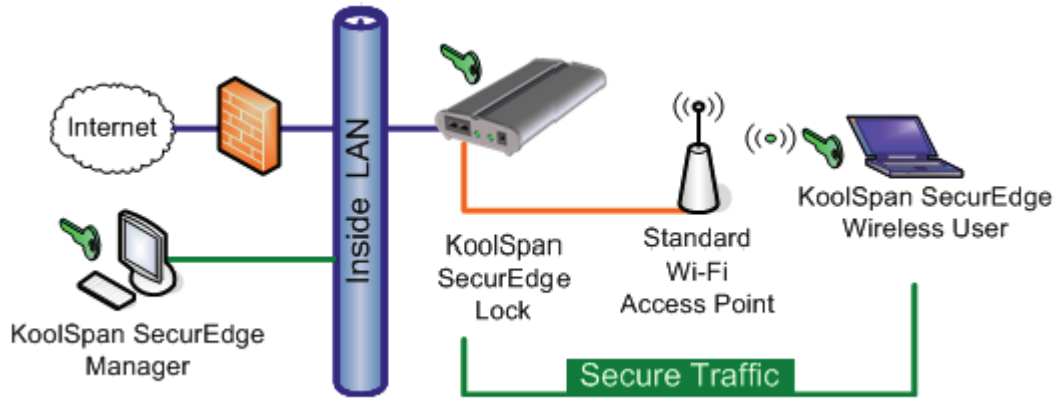
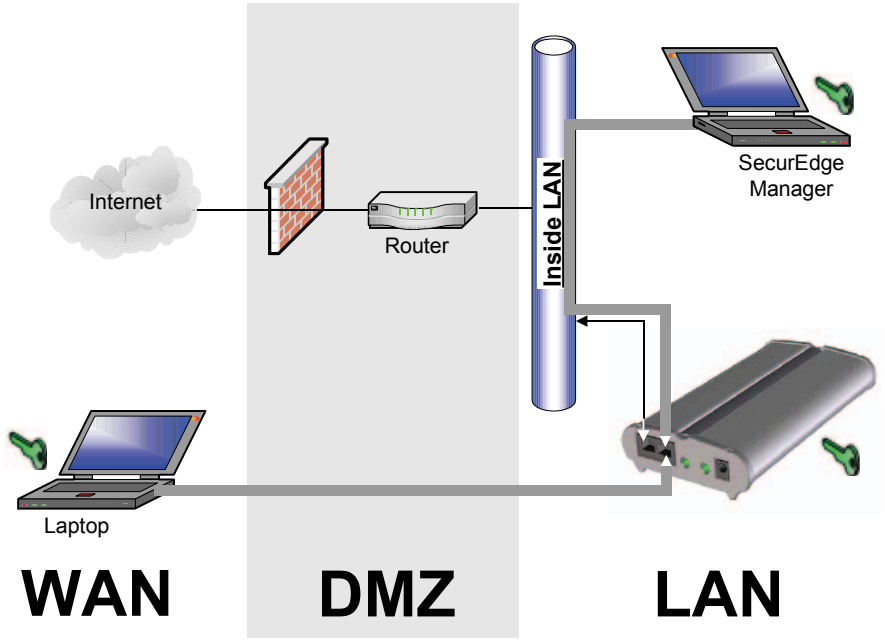


Figure 2 shows a configuration providing a secure tunnel for remote computers.

Figure 2. Remote Access Configuration.



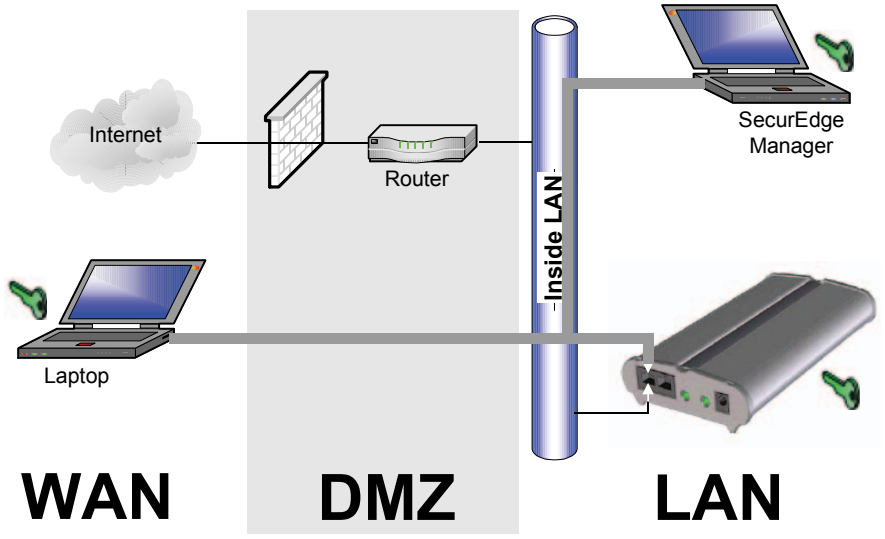
Legend:

Encrypted traffic

Decrypted traffic

Figure 3 shows an alternate configuration providing a secure tunnel for remote computers. The external port is left open for connection to a wireless LAN to allow both wireless users and remote users to access the internal LAN resources.

Figure 3. Remote Access Alternate Configuration.



Legend:

Encrypted traffic

Decrypted traffic

2.2 Module Description

The KoolSpan SecurEdge Lock cryptographic module is a multi-chip standalone cryptographic module consisting of production-grade components contained within an opaque hard production-grade enclosure (the outside case is aluminum and the end covers are steel). The removable cover is protected by tamper evident security tape in accordance with FIPS 140-2 Level 2.

The module comprises the following Lock hardware and firmware

- Hardware part number: LRF05123
- Firmware version 3.1.1

The module has a limited operational environment. The module firmware runs on a CPU implemented using an Altera FPGA. The module operating system (μC/OSII) is a limited operating system that does not provide any general purpose functions. The module provides authentication, cryptographic key management, and firmware integrity services assuring operators of a valid firmware state within the module and privacy services for the secure storage of cryptographic keys, and CSPs. The module does not have a bypass or maintenance mode.

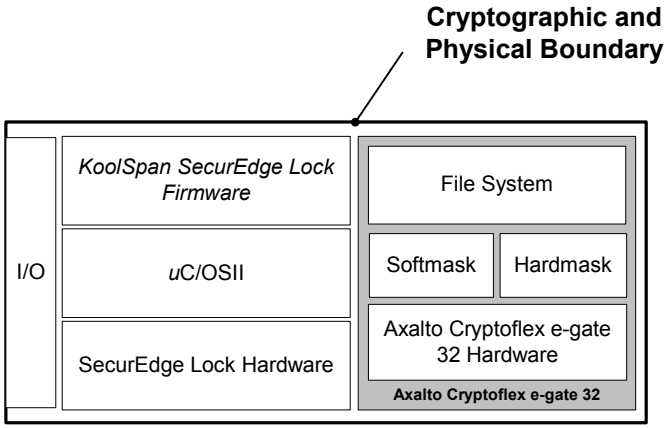
Figure 6 in section 2.3 shows the lock cryptographic module, highlighting module status LEDs and the module connectors.

The lock meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, for Class A devices.

2.2.1 Logical Block Diagram

Figure 4 shows a logical block diagram of the cryptographic module that illustrates the cryptographic and physical boundaries of the module and shows the module interfaces.

Figure 4. High Level Logical Block Diagram Showing Cryptographic and Physical Boundaries.



Logical blocks have the following functions:

SecurEdge Lock Hardware – Supports the Altera FPGA, Axalto smart card, RAM , Flash RAM, and I/O circuitry.

KoolSpan SecurEdge Lock Firmware. – Performs authentication of end users using cryptographic keys and authentication data stored within the Axalto smart card. Also performs per-packet AES data encryption and decryption for users and crypto officers.

uC/OSII – The operating system for the Altera FPGA. This provides support services for the KoolSpan SecurEdge Lock Firmware.

I/O – interfaces for data in\out, control in, status out, and power in.

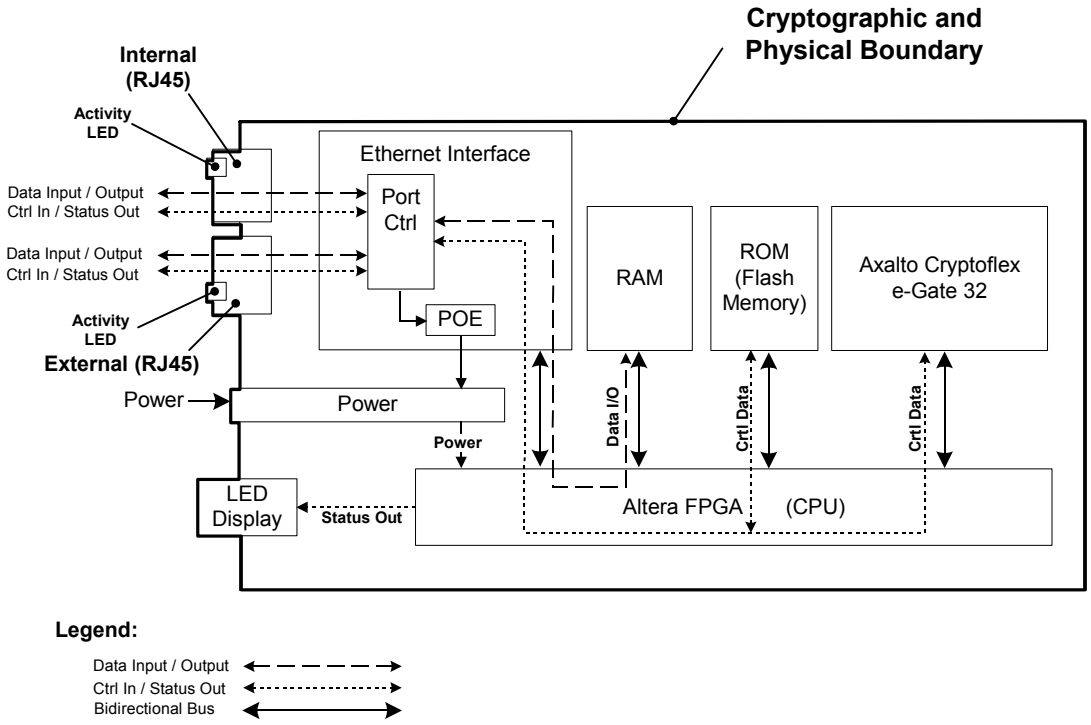
Axalto e-Gate 32 Hardware – This embedded FIPS approved cryptographic module (Certificate No. 242), securely stores module cryptographic keys and the card Holder Verification number (the Crypto Officer PIN). Also performs Triple-DES encryption and decryption, random number generation (for cryptographic keys and key material).

File System – A container system for storing cryptographic keys and CSPs.

2.2.2 Hardware Block Diagram

Figure 5 is a hardware block diagram showing the cryptographic and physical boundaries of the module and the module hardware subsystems. The figure shows the flow of data through the module as well as the module physical ports and interfaces.

Figure 5. High Level Hardware Block Diagram Showing Cryptographic and Physical Boundaries.



Hardware components have the following functions:

Internal – A bidirectional RJ45 Ethernet port that communicates with external devices using 802.3 and TCP/IP protocols.

Activity LEDs – Each RJ45 Ethernet port has an activity LED that flashes whenever data of any type enters or exits the port.

External – A bidirectional RJ45 Ethernet port that communicates with external devices using 802.3 and TCP/IP protocols. This connector may be unused when all communication uses the INTERNAL RJ45 connector.

Power – Provides power input from an A.C. Adapter of 6 VDC at 800 ma.

LED Display – Link and Power LEDs that provide various status outputs to the crypto officer.

Ethernet Interface – Supports 802.3 and TCP/IP protocols. Contains a port controller that routes data to the correct physical port (INTERNAL or EXTERNAL) based on instructions from the FPGA.

Altera FPGA – A fully programmable gate array that is the CPU for the module. The FPGA performs all per-packet AES encryption for end users, interacts with the Axalto EGate 32 smart card for authentication operations and for loading end-user authentication data into the smart card.

RAM – System scratchpad memory (128K x 16) subsystem for module operations. Cryptographic keys loaded into this memory subsystem are zeroized after use.

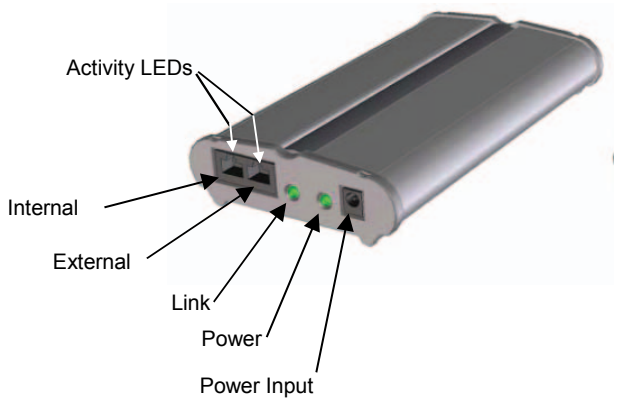
ROM (Flash ROM) – (128K x 16) memory device that contains the module firmware (KoolSpan SecurEdge Lock Firmware and *u*C/OSII limited operating system).

Axalto Cryptoflex e-Gate 32 smart card – A FIPS-validated (Certificate No. 242) Axalto Cryptoflex e-Gate 32 smart card that securely stores module cryptographic keys and CSPs. The smart card also generates key material and random numbers and deciphers enciphered client authentication data passed into the smart card.

2.3 Module Ports and Interfaces

The cryptographic module has seven physical interfaces/indicators and four logical FIPS 140-2 interfaces. The physical ports and logical interfaces are shown in Figure 6.

Figure 6. KoolSpan SecurEdge Lock Physical View.



The physical ports have the functions described in Table 2.

Where distinct logical interfaces share the same physical port (INTERNAL port, EXTERNAL port), communication protocols (TCP/IP and 802.3) logically separate and isolate these interfaces from one another. The system processor (FPGA) manages data as it passes through the module. The module relies on programmatic functionality and the system processor to ensure that logically distinct categories of data do not occupy the data path at the same time. The system relies in part on the smart card communication protocol (application protocol data units) to logically disconnect the input and output data paths from the circuitry and processes that perform key generation and key zeroization that are performed on the internal smart card device.

Table 2. Physical Ports and Logical FIPS 140-2 Interfaces.

Physical Interface/Indicator	*FIPS 140-2 Logical Interface*
Internal	Data input, data output, control input, and status output.
External	Data input, data output, control input, and status output.
Activity LEDs (2)	Status Output. Indicates port activity for the INTERNAL and EXTERNAL ports.
Link LED	Status Output
Power LED	Status Output
Power Input	This is not a FIPS 140-2 logical interface. Power input enters the module via the power connector.

The FIPS 140-2 logical interfaces correspond to physical ports as described in Table 3.

Table 3. FIPS 140-2 Logical Interfaces.

Logical Interface	*Description*
Data input	Data input consists of ciphertext data entering the cryptographic module from end users or crypto officers via the Ethernet interface for the purpose of authentication, session establishment, or decryption. Data input consists of plaintext data entering the cryptographic module from internal LAN resources via the Ethernet interface for the purpose of encryption.
Data output	Data output consists of ciphertext data exiting the cryptographic module to end users or crypto officers via the Ethernet interface. Data output consists of plaintext data exiting the cryptographic module to internal LAN resources via the Ethernet interface.
Control input	Control input from crypto officers enters the module using the Ethernet interface. Control input commands consist of module commands such as uploading keys and getting or setting operational parameters.
Status output	The status output consists of module status returned from status requests by crypto officers and other module outputs indicating module conditions. Examples of status data include module version information, module identifier, network address, and results of the power on self test. Status output exits the module via the Ethernet interfaces, and via the LEDs on the module physical perimeter that indicate the module operational state.

3 Security Functions

The Lock cryptographic module implements the security functions described in Table 4. The column Axalto Certificate lists cryptographic functions in the embedded Axalto Cryptoflex e-Gate 32 module.

Table 4. Module Security Functions.

Approved Security Function	*KoolSpan Certificate*	*Axalto Certificate*
Symmetric Key Encryption		
AES (FIPS PUB 197) CBC(e/d; 256)	388	
Triple-DES (FIPS 46-3) TECB(e/d; KO 2,3) TCBC (e/d; KO 2,3)		97
Hashing		
SHA-1 (FIPS PUB 180-2) (BYTE-only)	464	
Random Number Generation		
RNG (ANSI X9.17 PRNG)		(vendor affirmed)

An approved RNG implemented on the smart card is used to generate cryptographic keys.

The module smart card provides Triple-DES symmetric key encryption / decryption used for network identification and key transport. Symmetric key transport methodology provides 80 bits of encryption strength.

The module provides AES symmetric key encryption / decryption for crypto officer and user data encryption and decryption.

The module provides SHA-1 data hashing for data integrity purposes.

4 FIPS Approved Mode of Operation

The module's approved mode of operation is restricted to performing only FIPS-approved cryptographic algorithms and security functions. The module enters FIPS approved mode on power up as soon as it successfully completes the power-on self test. In the FIPS approved mode, crypto officers may configure the module for operation and they may load authentication data for users. Users authenticate to the module, after which, the module encrypts and decrypts user data for user data transfer from and to the internal (secure) LAN.

The module does not have a non-approved mode.

5 Identification and Authentication

The module supports a crypto officer role and a user role. The crypto officer and user may be different people or they may be the same person performing role-specific module operations. The module uses role-based authentication.

The KoolSpan *SecurEdge Bridging, Wi-Fi, & Remote Access User Guide* specifies three roles: a master crypto officer, a clone crypto officer (defined as an administrator using a clone key) and a user role. The only difference between a master and clone crypto officer is the ability of the master crypto officer to issue clone crypto officer authentication keys. Clone crypto officers cannot perform this function. With respect to the KoolSpan SecurEdge Lock, there is no distinction between these two crypto officer roles and these appear as a single crypto officer role in this Security Policy.

An operator assumes the crypto officer role by authenticating to the module with the respective crypto officer master or clone key. Crypto officers may upload authentication data to the module and they may change the module cryptographic keys or CSPs.

Multiple concurrent operators are allowed but operators cannot change roles while authenticated to the module. Separation of roles is achieved by first requiring operator authentication before granting access to services offered by a particular role. The firmware then programmatically separates roles and services during module use by providing role-specific services to operators authenticated within a specific role. The module does not display any authentication data entered into the module. Access to the authorized roles is restricted as explained in Table 6:

Table 6. Roles and Required Identification and Authentication.

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer	Role-based	A crypto officer must mutually authenticate with the lock module, demonstrating knowledge of the crypto officer authentication data to assume the crypto officer role.
User	Role-based	An user must provide the correct authentication data to the module to assume the user role.

The module does not require any physical maintenance. The strength of the operator authentication, per the above roles, is as follows in Table 7:

Table 7. Strength of Authentication.

Authentication Mechanism	*Strength of Mechanism*
NKUID	Users authenticate using the client Triple-DES 112-bit key (NKUID) to encrypt key material used to establish a secure session. The lock securely stores the same Triple-DES key indexed by key serial number. Successful decryption of the key material using the stored Triple-DES key authenticates the user. A crypto officer authenticates by demonstrating knowledge of the crypto officer authentication data (the lock Triple-DES 112-bit NKUID) that encrypts the return message in a lock-manager authentication sequence. A 112-bit key yields 4.95716^27 possible keys putting the possibility of correctly guessing the key at less than 1 in 1,000,000,000. The possibility of randomly guessing authentication data in 60 seconds is less than 1 in 100,000 as the module allows a maximum of three attempts before locking out the user or crypto officer.

The module uses the crypto officer NKUID, which must be in possession of the crypto officer. This key is inserted into the USB port of the manager station to achieve authentication. Associated with this key is a PIN, which must be known by the crypto officer, to make use of the manager station application. Authentication, therefore, is accomplished by using Triple-DES, whereas access to the manager station is accomplished using the PIN. This is the same in the case of a User except a Client NKUID is used and the application is the called the Secure Edge Client.

When the cryptographic module is powered off and subsequently powered on, the results of previous authentications (the per-packet session key) are cleared from memory. When the module is powered up again, operators must re-authenticate, using the correct key.

6 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module. Plaintext cryptographic keys and CSPs are never output from the module.

Table 8. Cryptographic Keys and CSPs.

Data Item	*Description*
External Key (EK)	This 112-bit Triple-DES key performs enciphered reads of encrypted Network User ID Keys (NKUIDs) passed into the Axalto Cryptoflex EGate 32 smart card. The EK is loaded onto the module when the module is initialized by the crypto officer, replacing the default EK shipped with the module. It is stored in plaintext form within the Axalto E-Gate 32 smart card. The key is used only on the smart card (in smart card RAM) and never leaves the smart card. The key is not zeroized by the crypto officer using the zeroize command.
Network Key (NKR)	This 112-bit Triple-DES key performs decryption of session data data being passed to the module. The NKR key is created when the module is initialized by the crypto officer. It is generated and stored in plaintext form within the Axalto E-Gate 32 smart card. The key is output from the smart card to lock RAM for use in receiving session data sent to the lock by clients or the manager. The key is deleted from lock RAM when the lock powers down. The key on the smart card is not zeroized by the crypto officer using the zeroize command.
Network Key (NKS)	This 112-bit Triple-DES key performs encryption of session data being sent from the module. The NKS key is created when the module is initialized by the crypto officer. It is generated and stored in plaintext form within the Axalto E-Gate 32 smart card. The key is output from the smart card to lock RAM for use in sending session data to clients or to the manager. The key is deleted from lock RAM when the lock powers down. The key on the smart card is not zeroized by the crypto officer using the zeroize command.
Lock Network User ID Key (NKUID)	A 112-bit Triple-DES key used to encrypt key material during lock authentication to the KoolSpan SecurEdge manager. This key is generated on the lock (in the Axalto Cryptoflex e-Gate 32 smart card) during module initialization. It is exported off of the smart card in enciphered form (encrypted by the external key) and stored in the KoolSpan SecurEdge manager hard disk for use in authentication operations. The key is stored in plaintext format in the Axalto E-Gate 32 smart card and is used only in smart card RAM during authentication to the manager. It is not zeroized on a zeroize command.

Data Item	Description
Client database (Client NKUID keys)	A table of 112-bit Triple-DES keys that identify clients in the network. These keys are generated off the module during client key issuance and are loaded onto the lock by the KoolSpan SecurEdge manager. The lock uses these keys to decrypt key material sent by clients and to encrypt key material returned to clients. The keys are individually encrypted under the External key before they are uploaded into the lock's client database. Each key is indexed by the client key serial number that is stored in plaintext along with the enciphered key. A client key is added to the table when a load authentication data operation is performed by the crypto officer. A client key is deleted from the table when a remove authentication data operation is performed by the crypto officer. The client database is zeroized whenever a zeroize command is given by the crypto officer.
AES Base Session Key (BSK)	An ephemeral 256-bit per-user AES key used in module RAM to construct a per-packet AES key. One half of the key is generated off the module using a FIPS approved RNG. This segment of the key is passed to the module enciphered under the client NKUID over an encrypted channel (using NKR). The module generates the other half of the AES key using an approved RNG (implemented on the smart card), sending it back to the user enciphered under the client NKUID via an encrypted channel (using NKS) while keeping a copy for itself. Both the module and the external system concatenate the two key halves to produce the complete AES base session key. The AES Base Session Key is stored in RAM during the session only and is used again only for deauthentication purposes. It is zeroized after use.
Per-Packet AES Key (PPK)	An ephemeral 256-bit AES key used to decrypt incoming packets (packets coming from a user on an unprotected network) and to encrypt outgoing packets (packets going to the same user on an unprotected network) This key is an obfuscation of the AES base session key using a 32-bit packet sequence number and a resulting initialization vector. The key is used once for a packet after which the next key in the sequence is calculated and so on, until the session ends when the lock receives a deauthentication message from the operator (crypto officer or end user). The AES PPK is not stored and is zeroized after use.
Deauthentication data	This ephemeral CSP is sent by the operator (crypto officer or end user) to signal the end of a session. The CSP is a 20 byte SHA-1 hash of the AES Base Session Key. It is sent within a deauthentication message to the lock.
Initialization Vector (IV)	This ephemeral CSP is used to produce per-packet keys from the base session key. The IV is produced by using the base session key to AES-encrypt the 32-bit koolspanSequence number.
RNG Seed	A hardware NDRNG on the smart card seeds the FIPS-approved DRNG that is also on the smart card.

7 Roles and Services

The module supports services that are available to operators in the crypto officer role or the user role. All of the services are described in detail in the module's user documentation. Table 9 shows the services available to the various roles.

Table 9. Roles and Services

Service	*Crypto Officer*	*User*
Initialize Lock Module	●	
Authenticate (Client – Lock)		●
Authenticate (Lock - Manager)	●	
Get/Set Settings	●	
Load authentication data	●	
Remove authentication data	●	
Block client	●	
Disable client	●	
Run self test (Reboot command or power cycle)	●	
Show status	●	
Data encryption and decryption	●	●
Deauthenticate	●	●
Reboot	●	
Zeroize	●	

8 Access Control

Table10 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic service.)
D - The item is **deleted** by the service.

Table 10. Access Control

Key or CSP	*Service*	*Access Control*
Triple-DES Symmetric Key (NKR, NKS)	Initialize Lock Module	W
	Authenticate	R,E
	Run self test	R,E
	Data encryption and decryption	E
	Zeroize	W
Triple-DES Symmetric Key (EK)	Initialize Lock Module	W
	Authenticate	R,E
	Run self test	R,E
	Zeroize	W
Triple-DES Symmetric Key (Lock NKUID)	Initialize Lock Module	W
	Authenticate	R,E
	Run self test	R,E
	Zeroize	W
AES Symmetric Key (ephemeral base session key)	Authenticate	W
	Data encryption and decryption	E
	Deauthenticate	E,D
	Reboot	D
AES Symmetric Key (ephemeral per-packet AES key)	Send packet	W, E
	Receive packet	W,E
	Deauthenticate	D
	Reboot	D
	Zeroize	W, E, D
Client Database (Client NKUIDs)	Load authentication data	W
	Authenticate (Client-Lock)	R, E
	Remove authentication data	D
	Zeroize	D
Initialization Vector	Send packet	W, E
	Receive packet	W,E
	Deauthenticate	D
	Reboot	D
	Zeroize	E, D
RNG Seed Key	Any RNG function	W,R,E,D

9 Physical Security

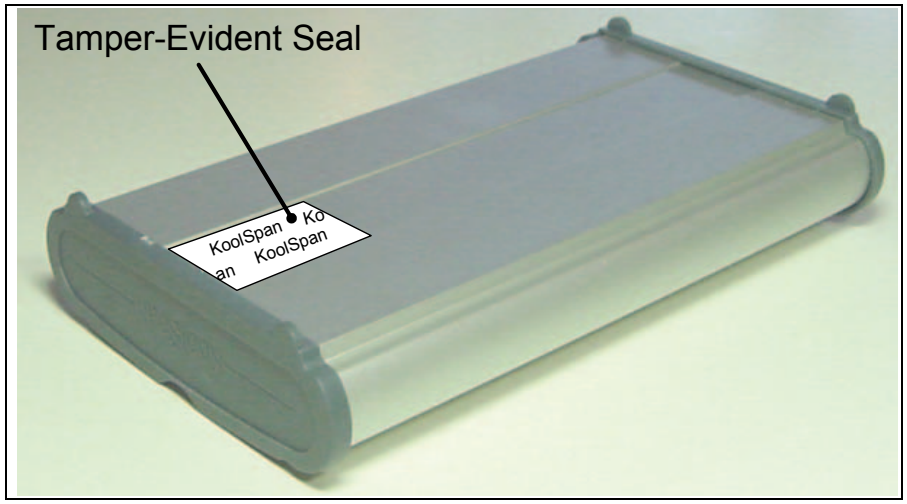
The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The cryptographic module consists of production-grade components that include standard passivation techniques (a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage). The module meets commercial-grade specifications for power, temperature, reliability, shock and vibration.

A tamper evident seal is placed over the module cover retention screw such that any attempt to remove the cover will leave evidence of tampering. The crypto officer guidance directs the crypto officer to periodically inspect the module for signs of tampering such as dents or scratches on the module enclosure or damage to the tamper evident seals. If tampering is detected, the crypto officer is instructed to perform a zeroize command and then to contact KoolSpan Technical support for further assistance.

Figure 7 shows how the tamper evident seals are placed over the module cover retention screws.

The tamper-evident seal is placed on the bottom of the unit to cover the single screw that holds the end-plate onto the circuit board. The seal does not extend onto the end-plate.

Figure 7. Tamper Evident Seal.



10 Self Tests

{Note: The embedded Axalto Smart Card is FIPS-approved (Cert. #242). As such, the FIPS-approved Smart Card performs power-on status check in compliance with FIPS}

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state, blocking all data output via the data output interface and preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions.

While the module is performing any power on self test, firmware rules permanently coded within the executable image prevent the module from entering a state where data output via the data output interface is possible. During any conditional tests, the module sets a self test flag. Processes that could output data monitor this flag, preventing data output via the data output interface and preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions if it is set. `

Anyone with physical access to the module can run the POST on demand by power cycling the module.

Table 11 summarizes the system self tests.

Table 11. Self Tests.

Self Test	*Description*
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, Triple-DES, SHA-1, and RNG) performed by the module, is tested using a “known answer” test to verify the operation of the function.
Firmware Integrity Test	The module computes a SHA-1 hash of the firmware to verify its integrity.
Conditional tests performed, as needed, during operation:	
Continuous RNG	16 bits continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG. This test is a “stuck at” test to check the RNG output data for failure to a constant value.

Any self test success or failure messages are output to LEDS. Solid green indicates success. Solid red indicates a self-test failure. Blinking yellow indicates a failure to authenticate. Additionally, the module sends messages to a syslog when this capability is enabled.

Known answer tests for encryption/decryption or hashing, function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated outmatch does not match the expected value. The test then decrypts the ciphertext string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

11 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

12 References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: http://www.nist.gov/cmvp.