SkyLOCK™ Encryption Module
SkyLOCK™
Security Policy

Document Version *1.3*

Encryption Solutions, Inc.

March 1, 2007

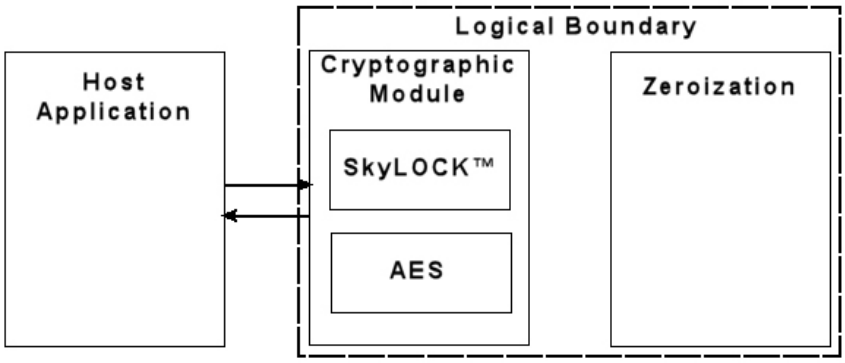
Copyright Encryption Solutions, Inc. May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

1. Module Overview

The SkyLOCK™ Encryption Module (Software Version 1.0) is a software only module that is installed on a multi-chip standalone device, such as a General Purpose Computer (See Section 7). The primary purpose for this module is to provide automated encrypted data storage. The device provides data input, data output, control input, and status output interfaces via the API (Application Program Interface) of the module. The cryptographic boundary is defined as the '.dll' dynamic linked library within which the SkyLOCK™ Encryption module resides and the SkyLOCK Zeroization application. The diagram below is a logical representation of the module as well as defining the cryptographic boundary.

Figure 1 – Image of the Cryptographic Module



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

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

3. Mode of Operation

The module only supports an Approved mode of operation and as such only operates in an Approved mode. The Approved mode can be determined by verifying the software version of the module through the Show Status service. The cryptographic module supports the following Approved algorithms:

- AES for data encryption using keys with a minimum length of 128-bits (Cert. #413)
- HMAC SHA-1 for data integrity (Cert. #187 for HMAC)
- SHA-1 (Cert. #482 for SHA-1)

The cryptographic module provides the following non-Approved algorithms:

- SkyLOCK™ Data Protection Scheme, which is not used to provide FIPS 140-2 cryptographic strength or security.

4. Ports and Interfaces

The cryptographic module provides the following logical interfaces through the API: data input, data output, status output, control input. The physical ports of the module are only those applicable to a GPC.

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module shall support two distinct operator roles (User and Cryptographic-Officer). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. The User and/or Cryptographic Officer must enter a username, password, and PIN to log in. The password is an alphanumeric string of minimum 16-characters randomly chosen from a set of 128-printable and unprintable characters.

Password guidelines are provided below:

Case Sensitive

Minimum 16 Characters

Minimum one upper case

Minimum one lower case

Minimum one numeric

Minimum one special character include “space”

Cannot contain the same character more than four times

The PIN is an eight-character string chosen from the set of 16-hex values.

PIN guidelines are provided below:

Eight digits exactly, where a digit is a hex value.

Contain at least four different digits

Cannot have more than three numbers in sequence (ascending or descending)

Cannot contain the same digit more than four times, with the exception of zeroes which may only appear twice.

Password and PIN aging requirement is an assignable option for local administration during network installation process.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Identity-based operator authentication	Username, Password, & PIN
User	Identity-based operator authentication	Username, Password, & PIN

Table 3 – Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Password & PIN	The probability that a random attempt will succeed or a false acceptance will occur is $1/(128^{16} * 16^{8})$ which is less than 1/1,000,000. A one second delay is enforced between authentication attempts; therefore, the module can only support 60 authentication attempts in a given minute. As a result, the probability of successfully authenticating to the module within one minute is $60/(128^{16} * 16^{8})$ which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	• Encrypt Data: AES-encrypts a data payload. • SkyLOCK Process Data: Uses SkyLOCK processing on a data payload. (Note: When not used in conjunction with the Encrypt Data service, this service is operating in a bypass mode and data is transmitted in obfuscated plaintext.) • Decrypt Data: Decrypt a data payload. • Change Passphrase/PIN: Change the authentication data used by the User. • Show Status: Indicates the current state of the module. Module failure state will deny service access.
Cryptographic-Officer:	• Create User: Add a User and their identification credentials. • Encrypt Data: AES-encrypts a data payload. • SkyLOCK Process Data: Uses SkyLOCK processing on a data payload. (Note: When not used in conjunction with the Encrypt Data service, this service is operating in a bypass mode and data is transmitted in obfuscated plaintext.) • Decrypt Data: Decrypt a data payload. • Change Passphrase/PIN: Change the authentication data used by the CO or Users. • Show Status: Indicates the current state of the module. Module failure state will deny service access.

Unauthenticated Services:

Any operator may invoke self-tests by re-loading the module.

Zeroize: This service is provided by the SkyLOCK Zeroization application and actively destroys all plaintext critical security parameters, including the dll.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

1. *AES Key – Used for securing data storage.*
2. *Passphrase and PIN – Used to authenticate the User and Cryptographic Officer.*
3. *Software Integrity Key – Used to verify the integrity of the software using HMAC SHA-1. This key is established by ESI and is not available to the end-user for entry or output.*
4. *CSP Integrity Key – Used to verify the integrity of the passphrase and PIN. This key is established by ESI and is not available to the end-user for entry or output.*

Definition of Security Relevant Data Items (SRDIs)

The following are SRDIs contained in the module and specified by ESI:

1. *SkyLOCK™ Protection Items – Used by the SkyLOCK™ module for data obfuscation.*

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Enter: CSP is imported into the module.
- Use: CSP is utilized by the module.
- Destroy: Destruction of the CSP value by means of active overwriting.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
X		Create User	Enter initial passphrases and PINs, Use CSP Integrity Key
X	X	Encrypt Data	Enter, Use AES Key
X	X	SkyLOCK Process Data	N/A.
X	X	Show Status	N/A.
X	X	Decrypt Data	Enter, Use AES Key

X	X	Change Passphrase/PIN	Enter, Use Passphrase & PIN, Use CSP Integrity Key
X	X	Self-Tests	Use Software Integrity Key
X	X	Zeroize	Destroy all CSPs

7. Operational Environment

The module is installed on Microsoft Windows XP Professional, which conforms to Common Criteria EAL4 in accordance with the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999. Operational testing was performed on the following platforms:

- Windows XP Professional SP2 running on an HP Pavilion dv8210us computer
- Windows XP Professional SP2 running on an HP Pavilion zt1175 computer
- Windows XP Professional SP2 running on a Dell Optiplex GX270 computer configured to be consistent with the Common Criteria evaluation configuration.

In order to maintain the FIPS 140-2 validated configuration, the module must be installed on a platform consistent with the Windows XP Professional Common Criteria evaluation. (See: http://www.niap-ccevs.org/cc-scheme/st/ST_VID4025.cfm.)

The cryptographic module is protected by a HMAC SHA-1 hash.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When the operator has not assumed a valid role through authentication, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall encrypt data using the AES algorithm.
5. The cryptographic module shall perform the following tests:

   Power up Self-Tests:

   1. Cryptographic algorithm tests:

a. AES Known Answer Test

b. HMAC SHA-1 KAT (tested as part of the Software Integrity Test)

c. SHA-1 KAT (tested as part of the Software Integrity Test)

2. Software Integrity Test (HMAC SHA-1)

3. Critical Functions Test: N/A

Conditional Self-Tests:

1. Exclusive Bypass Test

6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

Physical Security Mechanisms

The module is a software only module and does not implement physical security mechanisms.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks beyond the scope FIPS 140-2 requirements.

11. Definitions and Acronyms

AES:	Advanced Encryption Standard
API	Application Program Interface
CSP	Critical Security Parameters
EAL:	Evaluation Assurance Level
ESI:	Encryption Solutions, Inc.
FIPS	Federal Information Processing Standard
GPC:	General Purpose Computer
HMAC:	Hashed Message Authentication Code

PIN:	Personal Identification Number
SHA:	Secure Hash Algorithm