Cruzer Enterprise FIPS Edition
Security Policy

Document *Version 1.25*

SanDisk®

Revision Date: 6/17/2011

Prepared By:

Metatron Security Services Ltd.

66 Yosef St.,
Modiin, Israel 71724

TABLE OF CONTENTS

1. Module Overview

The SanDisk Corporation Cruzer Enterprise FIPS edition secure USB flash drive (HW P/N# 54-89-15381-004G, 54-89-15381-008G, 54-89-15381-016G, and 54-89-15381-032G, Revision 1; FW Version 9.5.21.01.F3) offers on-the-fly hardware encryption/decryption to protect information stored on SanDisk Corporation USB flash drives.

The module is a multi-chip embedded cryptographic module, as defined by FIPS 140-2, and consists of a PCB containing the S3 controller and FLASH memory integrated circuit. Both components are encased in an opaque, production grade integrated circuit packaging and soldered onto the PCB. All security-relevant components and the data connections between the components are covered with an opaque tamper-evident epoxy encapsulation.

The only hardware components of the module excluded from the requirements of FIPS 140-2 are non security-relevant electronic components (resistors, capacitors, oscillator, fuse, etc.) that are mounted outside the epoxy-protected area on the PCB.

The external casing for the USB flash drive is not included within the cryptographic module boundary.

Note: All files mounted within the CD drive are outside the logical boundary of the cryptographic module, as they cannot execute within the cryptographic boundary, cannot lead to a compromise of the module's security, and exist for storage only.

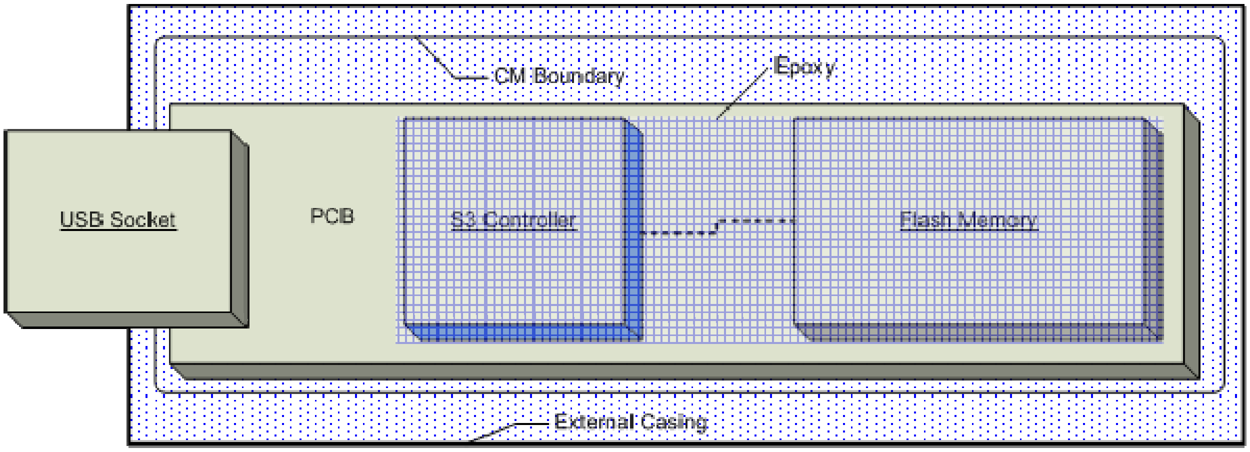

Figure 1 – SanDisk Corporation Cruzer Enterprise FIPS Edition Block Diagram

2. Security Level

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

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

Table 1 – Module Security Level Specification

3. Modes of Operation

The Cruzer Enterprise FIPS edition module supports both a FIPS Approved mode and non-Approved mode of operation.

In order to place the module into FIPS Approved mode, the operator must successfully open the private area by entering a valid password to authenticate to an authorized user Role, and set a password for the Cryptographic Officer role.

NOTE: Drives are configured in manufacturing with a private area and no user writable public area. The initial private area password must be supplied by the user on first application of power to the device after manufacturing. The private area is not functional until the initial private area password has been set. Devices are also configured in manufacturing to disallow creation of a user writable public area after manufacturing.

Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES 256 (CBC, CMAC) – (Certificate No. 1432, 1433)
    - Data Encryption/Decryption
    - Message Authentication Code
- RSA PSS 2048 (Certificate No. 702)
    - Signature Verification
- SHA-256 for hashing (Certificate No. 1295)

Furthermore the S3 microcontroller in FIPS mode offers key generation services:

- AES Key generation

For random number generation of all cryptographic keys, the S3 microcontroller employs an implemented deterministic random number generator (RNG) that is compliant with ANSI X9.31 Appendix 2.4. This RNG is FIPS Approved and has been issued Certificate #779.

Non-Approved Algorithms

- Seed and seed key for the RNG will be generated by the S3's NDRNG which is implemented in Hardware. The NDRNG is used in FIPS and non-FIPS mode of operation.
- RSA Encrypt/Decrypt of data: This algorithm shall not be used in the FIPS mode of operation.

Non-Approved mode of operation

The use of the RSA Encrypt/Decrypt algorithm will cause the module to transition into the non-FIPS Approved mode of operation.

4. Ports and Interfaces

The example cryptographic module provides the following physical ports and logical interfaces:

Physical Port	**Logical Interface Definition**	**Description**
USB port	- Data input - Data output - Status output - Control input - Power input	The purpose of the USB core is to receive and send the data and control information.
LED	- Status output	Blinks when power is applied to the module.

Table 2 – Physical Ports and Logical Interfaces

5. Identification and Authentication Policy

Assumption of roles

Role	Type of Authentication	Authentication Data	Description
Cryptographic Officer	Role-based operator authentication	Password (128 bits[1]): The module persistently stores the password hashed and AES encrypted in FLASH.	The Cryptographic Officer has access to the zeroization command. The Cryptographic Officer does not have access to the private User domains.
User	Role-based operator authentication	Password (128 bits[1]): The module persistently stores the password hashed and AES encrypted in FLASH.	The User has full Access to all services except the zeroize service.
Firmware Update Officer	Role-based operator authentication	RSA 2048 signature.	The Firmware Update Officer's sole responsibility is the external loading of new firmware updates. All firmware is signed by SanDisk.

Table 3 – Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Cryptographic Officer Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000. The module's S3 controller processes invalid Cryptographic Officer password processing in a little less than 2ms, i.e. cannot perform more than 600 password verification operations per second. Therefore, the probability that a random attempt will be successful within a one minute period is less than 36,000/2^128, which is less than 1/100,000.
User Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000. The user is locked out after 100 consecutive login failures[2], therefore the random success rate for multiple retries is 100/2^128, which is less than 1/100,000.
RSA Signature	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112 which is less than 1/1,000,000. The module's S3 controller cannot perform more than 3 RSA signature verifications per second. Therefore, the probability that a random attempt will be successful within a one minute period is 180/2^112 which is less

[1] The module always uses a password length of 16 octets, and allows any 128 bit value to be used as a password.

Note: The original authentication data for the Cryptographic Officer and User is assumed to meet the 1/1,000,000 strength requirements defined in Section 4.3.3 in FIPS 140-2

[2] The maximum number of consecutive login failures before user lock-out is a configuration setting that is set in manufacturing, normally set to 10. The maximum number of attempts configurable is 100.

	than 1/100,000.

Table 4 – Strengths of Authentication Mechanisms

6. Access Control Policy

Roles and Services

The S3 microcontroller supports three distinct Roles, a User, Cryptographic Officer, and Firmware Update Officer. The cryptographic module does not support concurrent operators. The User and Cryptographic Officer roles shall enter a username and its password to log in, whereas the Firmware Update Officer must enter a valid RSA signature. The operator to service mapping is shown below is shown Table 5 below.

Operator	Services
User Role	o Open Private Area: Allows read/write to secure area o Close Private Area: Closes Private area to disallow read/write o Change User Private Area Password o Read/Write Private Area
Cryptographic Officer Role	o Zeroize Keys: Zeroizes all FIPS keys o Change Cryptographic Officer password
Firmware Update Officer	o Externally Load FW: Load RSA signed Firmware. This firmware will only be loaded if the RSA 2048 bit signature is verified.
Unauthenticated Services (No Role)	o Self-tests: This service executes the suite of self-tests required by FIPS 140-2. o Device Reset: Reformats specific Private Area of the User currently selected when the User password can not be remembered. Once this is performed a User must reinitialize the device for their use. All data and keys associated with that particular User Role will have been zeroized. o CD Emulation: Provides access to the public area (read only) of the FLASH memory. o Get Version: This allows the operator to retrieve the module versioning information o Show status and error: Provides current module status and error state indicator

Table 5 – Services Authorized for Roles

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

Key	Description/Usage
AES default key	Module AES-256 key used to encrypt on-the-fly all data stored on the public area on the flash memory. Used in combination with user password to derive key encryption key for encrypting private area key.
User Private Area AES key	User AES-256 key to encrypt private data on private area.
Crypto Officer Password	Password to authenticate an operator to the Crypto Officer Role.
User Password	Password to authenticate an operator to the User Role.
DRNG Seed Key	NDRNG generated output used to seed the Approved ANSI X9.31 RNG
DRNG Seed	NDRNG output used as the seed into the ANSI X9.31 RNG

Table 6 – CSPs

Definition of Public Keys

The following Keys are contained within the module:

Key	Description/Usage
RSA Source Code Integrity public key	Used for digital signature source code verification and Firmware Update Officer authentication.

Table 7 – Public Keys

Definition of CSPs Modes of Access

Table 8 defines the relationship between access to CSPs and the different module services. The type access to each data object is identical for each role. The modes of access shown in the table are defined as follows:

- I - Input: the CSP is input into the module.
- E - Encrypt: The CSP item is used to encrypt plaintext data.
- D - Decrypt: The CSP is used to decrypt ciphertext data.
- A – Authenticate: CSP is used to authenticate.
- U – Used: Used in the Random Number Generator.
- Z - Zeroize: the CSP is zeroized.
- G - Generate: the CSP is generated using the FIPS approved ANSI X9.31 DRNG.
- L - the CSP is generated using NDRNG hardware

	User Role				**CO Role**		**Firmware Update Officer Role**
CSP	**Open Private Area**	**Close Private Area**	**Read/Write Protected Area**	**Change User Private Area Password**	**Change Cryptographic Officer Password**	**Zeroize Keys**	**Externally Load FW**
AES default key	*D*			*E*		*Z*	
User Private Area 1 AES key	*G**		*E, D*			*Z*	
Cryptographic Officer Password					*I,A*	*I, A, Z*	
User Password	*I, A*		*I, A*	*I, A*		*Z*	
DRNG Seed Key	*U, L*					*Z*	
DRNG Seed	*U, L*					*Z*	

Table 8 – Services to CSP Access mapping

* Generated only if it does not currently exist

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module has a limited operational environment.

8. Security Rules

The Cruzer Enterprise FIPS edition module's design corresponds to the Cruzer Enterprise FIPS edition 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 three distinct operator roles. These are the User role, Cryptographic-Officer, and Firmware Update Officer roles.
2. The cryptographic module shall provide role-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1) Cryptographic algorithm tests:

      a. AES Known Answer Test

      b. SHA-256 Known Answer Test

      c. RSA Known Answer Test

      d. RNG Known Answer Test

   2) Firmware Integrity Test (first-time RSA 2048 signature verification or afterwards: AES-CMAC comparison with previously generated result)

   B. Conditional Self-Tests:

   3) Continuous Random Number Generator (RNG) test

      a. Non-Approved HW RNG.

      b. Approved RNG ANSI X9.31 Appendix 2.4

   4) Firmware load test – RSA signature verification of externally loaded code.
5. The operator shall be capable of commanding the module to perform the power-up self-test at any time by power cycling the module, or by sending the module a self-test command (the latter always performs RSA 2048 firmware signature verification).
6. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The RSA Encrypt/Decrypt algorithm shall not be used in the FIPS mode of operation. Use of this algorithm will cause the module to transition into the non-FIPS mode of operation.

9. Physical Security Policy

Physical Security Mechanisms

The multi-chip embedded cryptographic module includes the following physical security mechanisms:

- Production-grade components (S3, FLASH).
- Data path between S3 and FLASH is completely covered by epoxy and has no vias.
- Opaque Epoxy encapsulation of all security-relevant components within the boundary.

The operator should on a periodic basis visually inspect the module to determine if it has been compromised. The epoxy and PCB should not show any evidence of tampering including scratches, chips, and holes.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

11. References

Reference Number	Reference Title
[1]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules / National Institute of Standards and Technology (NIST), May 2001
[2]	PKCS#1: RSA Encryption Standard v1.5, November 1993 / RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs
[3]	ANSI X9.31-1998: Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) / American Bankers Association, 1998

12. Definitions and Acronyms

AES – Advanced Encryption Standard

CMAC – Cipher-based Message Authentication Code

CSP – Critical Security Parameter

DRNG – Deterministic Random Number Generator

CBC – Cipher Block Chaining

FIPS – Federal Information Processing Standard

LED – Light Emitting Diode

NDRNG – Non-deterministic Random Number Generator

PCB – Printed Circuit Board

RNG – Random Number Generator

RSA – Rivest, Shamir and Adleman Algorithm

SHA – Secure Hash Algorithm

USB – Universal Serial Bus

PSS – Probabilistic Signature Scheme

ANSI – American National Standards Institute