PICOfreedom

Security Policy

Document *Version 1.11*

Stonewood Electronics Ltd.

Revision Date: 8/19/2008

TABLE OF CONTENTS

1. Module Overview

The PICOfreedom (HW P/N# 8A-SFS-0000-09P, Version A and Version 2; FW Versions 6.600 and 6.612) provides FIPS 140-2 Approved security functionality to the DiskOnKey USB flash drives. The PICOfreedom cryptographic module employs validated Federal Information Processing Standard (FIPS 140-2) encryption and key management functionality to ensure the protection of data stored on external DiskOnKey FLASH memory. The module is a multi-chip embedded cryptographic module, as defined by FIPS 140-2, and consists of the S2 controller and 8k of attached EEPROM. Both components are encased in a hard, opaque, production grade integrated circuit packaging. The cryptographic boundary contains the module's microcontroller, 8k of attached EEPROM, and a single interconnect between the two components. The data connection between the components is encapsulated in epoxy and the PCB on which the components are soldered. No hardware or firmware components of the module are excluded from the requirements of FIPS 140-2.

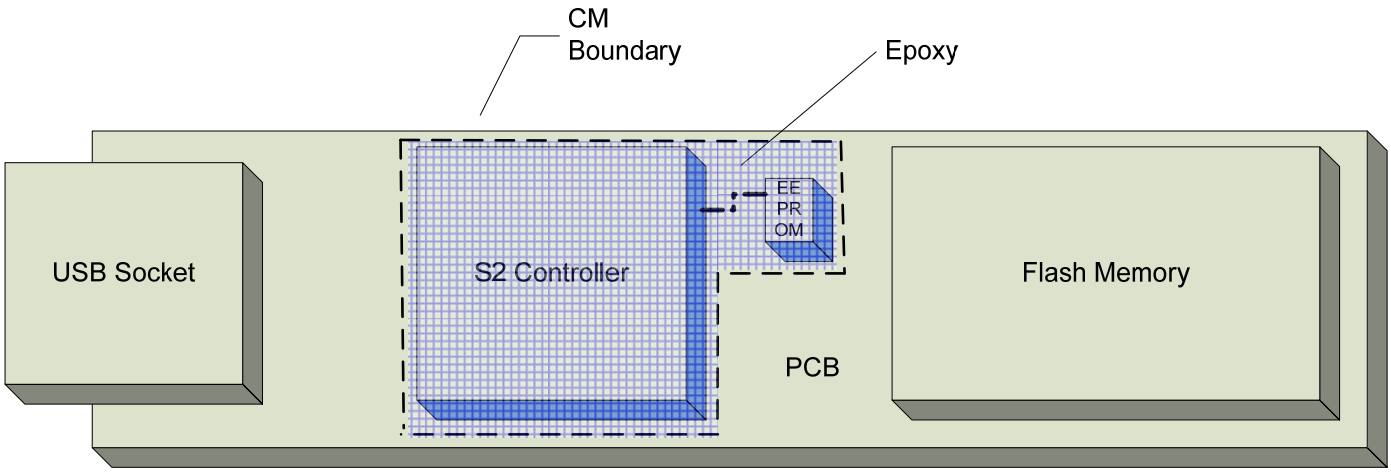

Figure 1 – PICOfreedom Crypto-Processor

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

Security Requirements Section	Level
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 PICOfreedom 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 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 (ECB) – Certificate No. 464
    - Data Encryption/Decryption
- RSA PSS 1024 (Certificate No. 200)
    - Signature Verification
- SHA-1 for hashing (Certificate No. 555)

Furthermore the S2 microcontroller in FIPS mode offers key generation services:

- AES Key generation

For random number generation of all cryptographic keys, the S2 microcontroller employs an implemented deterministic random number generator (DRNG) that is compliant with ANSI

X9.31 Appendix 2.4. This DRNG is FIPS Approved and has been issued Certificate #263.

Non-Approved Algorithms

- Seed and seed key for the DRNG will be generated by the S2's NDRNG which is implemented in Hardware. The NDRNG is used in FIPS and non-FIPS mode of operation.
- RSA Encrypt/Decrypt: 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	The purpose of the USB core is to receive and send the data and control information.
Flash Memory	- Data input - Data output	The purpose of the Advanced NAND Flash Controller (ANFC) is to provide interface to the NAND Flash memory (Flash) and the crypto module.
ISO7816 Interface	- Data input - Data Output - Status output - Control input	This interface supports ISO7816 as well as RS232 which is multiplexed over this physical port.
Clock	- Control input	External crystal input.
Power Interface	- Power Input	Physical port for external power input.

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 Only: The module persistently stores the password hashed and AES encrypted in FLASH, which is outside of the cryptographic boundary.	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 Only: The module persistently stores the password hashed and AES encrypted in FLASH, which is outside of the cryptographic boundary.	The User has full Access to all services except the zeroize service.
Firmware Update Officer	Role-based operator authentication	RSA 1024 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
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/62^4, which is less than 1/1,000,000. The user is locked out after no more than 100 contiguous login failures, therefore the random success rate for multiple retries is 1/62^4 divided by a customer specified number ≤ 100[1], which is less than 1/100,000.
RSA Signature	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^80, which is less than 1/1,000,000. The module only allows one attempt every 10 seconds. Therefore, the probability that a random attempt will be successful within a one minute period is 6/2^80, which is less than 1/100,000.

Table 4 – Strengths of Authentication Mechanisms

[1] This is a configuration setting that is set in manufacturing. The maximum number of attempts configurable is 100.

6. Access Control Policy

Roles and Services

The S2 microcontroller supports three distinct separate Roles, a User, Cryptographic Officer, and Firmware Update Officer. The role selected is explicitly selected during authentication and is determined by the interface used to authenticate. 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 Protected 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 1024 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 have been zeroized. o CD Emulation: Provides a CD emulation service o Get Error status: Provides the operator with the error state indicator o Get Version: This allows the operator to retrieve the module versioning information o Show status: Provides current module status

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	Used to encrypt on-the-fly all data stored on the public area on the flash memory.
User Private Area 1 AES key	User AES-256 key to encrypt private data on private area 1.
User Private Area 2 AES key	User AES-256 key to encrypt private data on private area 2.
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 DRNG
DRNG Seed	NDRNG output used as the seed into the ANSI X9.31 DRNG

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.
- O - Output: the CSP is output from 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 LFSR hardware

CSP	User Role				CO Role		Firmware Update Officer Role
	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, D*	*E*		*Z*	
User Private Area 1 AES key	*I, O, G**		*E, D*			*Z*	
User Private Area 2 AES key	*I, O, 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 S2 module's design corresponds to the S2 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-1 Known Answer Test
      c. RSA Pairwise Consistency Test
      d. DRNG Known Answer Test
   2. Firmware Integrity Test (RSA 1024 signature verification)

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

- Production-grade components (S2, EEPROM).
- Data path between S2 and EEPROM is completely covered by epoxy and has no vias.
- Opaque Epoxy encapsulation of all 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 not has 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]	PAN ASIC Top-Level Specification Version 0.2 / M-Systems, March 2005
[3]	PKCS#1: RSA Encryption Standard v1.5, November 1993 / RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs
[4]	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

CSP – Critical Security Parameter

DRNG – Deterministic Random Number Generator

ECB – Electronic Code Book

FIPS – Federal Information Processing Standard

NDRNG – Non-deterministic Random Number Generator

RNG – Random Number Generator

RSA – Rivest, Shamir and Adleman Algorithm

SHA – Secure Hash Algorithm