iStorage Ltd.
iStorage diskAshur PRO² Level 3 Secure Storage Drive

FIPS 140-2 Non-Proprietary Security Policy

Version *1.0*

This document may be freely reproduced and distributed, but only in its entirety and without modification

TABLE OF CONTENTS

This document may be freely reproduced and distributed, but only in its entirety and without modification

INTRODUCTION

The iStorage diskAshur PRO² Level 3 Secure Storage Drive (diskAshur PRO²) is an encrypted storage device that provides a secure way to store and transfer data. User authentication is self-contained via an on-board keypad. User data is protected by hardware-based 256-bit AES encryption to secure sensitive information in the event that the drive is lost or stolen.

The data encryption key (DEK) and other cryptographic parameters are generated within the module on first use through a NIST approved DRBG (ref: SP800-90A). The seed for the DRBG is also produced within the module from a hardware-based entropy generator.

Table 1 - All iStorage diskAshur PRO² Level 3 Versions

Capacity	Hardware Version	EC Firmware Version	SC Firmware Version
512 GB	IS-DAP2-256-500-C-X	IS_EC_FW_2_59_1X	3.1
1 TB	IS-DAP2-256-1000-C-X	IS_EC_FW_2_59_1X	3.1
2 TB	IS-DAP2-256-2000-C-X	IS_EC_FW_2_59_1X	3.1
3 TB	IS-DAP2-256-3000-C-X	IS_EC_FW_2_59_1X	3.1
4 TB	IS-DAP2-256-4000-C-X	IS_EC_FW_2_59_1X	3.1
5 TB	IS-DAP2-256-5000-C-X	IS_EC_FW_2_59_1X	3.1
128 GB	IS-DAP2-256-SSD-128-C-X	IS_EC_FW_2_59_1X	3.1
256 GB	IS-DAP2-256-SSD-256-C-X	IS_EC_FW_2_59_1X	3.1
512 GB	IS-DAP2-256-SSD-512-C-X	IS_EC_FW_2_59_1X	3.1
1 TB	IS-DAP2-256-SSD-1000-C-X	IS_EC_FW_2_59_1X	3.1
2 TB	IS-DAP2-256-SSD-2000-C-X	IS_EC_FW_2_59_1X	3.1
4 TB	IS-DAP2-256-SSD-4000-C-X	IS_EC_FW_2_59_1X	3.1

1. CRYPTOGRAPHIC MODULE SPECIFICATION

1.1 SECURITY LEVEL

The module meets the overall requirements of FIPS 140-2 Level 3.

Table 2 - Module Security Level

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	3
2	Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3

This document may be freely reproduced and distributed, but only in its entirety and without modification

6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

1.2 Modes of Operation

The iStorage diskAshur PRO² Module operates only in a FIPS Approved mode. There does not exist a non-Approved mode of operation. The module indicates that it is in an approved mode of operation by displaying a solid red LED.

1.3 Specifications

The diskAshur PRO² is a multi-chip standalone cryptographic module as defined by FIPS 140-2. It consists of a USB 3.0 capable encryption controller, HDD/SSD with SATA interface, a security controller, a keypad controller, a 5V DC Input, and a user interface with three (3) LED status indicators and a user-interface alphanumeric keypad with thirteen (13) buttons. The module is encapsulated within an opaque, production grade integrated circuit package. The security components are protected by epoxy against physical tamper attacks. The cryptographic boundary is defined by the diskAshur PRO² entire device, which contains all the components.

2. MODULE PORTS AND INTERFACES

The cryptographic module exposes the following physical ports and logical interfaces:

Table 3 - Physical Ports and Logical Interfaces

Physical Port	Logical Interface	Description
USB Port	Data input Data output Control input Status output Power input	The USB port connects the module to the host computer and is used to exchange decrypted user data as well as control and status information for the USB protocol. There is no direct connection between the USB port and the security controller.
Alphanumeric Keypad (0-9)	Data input	The ten (10) alphanumeric labelled keypad buttons, connected to keypad controller button inputs, are used to enter the Standard User or Administrative User PINs.
Unlock, Lock and Shift Buttons	Control input	The three (3) buttons are connected to the keypad controller button inputs, and are used to control UI flow, including selecting the role.

This document may be freely reproduced and distributed, but only in its entirety and without modification

Physical Port	Logical Interface	Description
Red, Green and Blue LEDs	Status output	Refer to Table 4.
USB Power	External power	The USB VBUS (+5) powers the module when it is available.

Table 4 - LED Status Output

LED Behaviour	Module State	Status Description
LEDs off	Disconnected	The module is powered off.
Red LED solid	Locked	Standby State. Waiting for entering Administrative User PIN.
Red LED solid	Reset	Reset State. Waiting for setting up an Administrative User PIN.
All three LEDs blink simultaneously	Locked	Waiting for Standard User/Self-destruct PIN to unlock. Administrative User PIN is set.
All three LEDs solid	Locked	Device Inactive State. Anti-brute-force attack mechanism is invoked
Red Green and Blue blink alternatively	Locked	Factory reset is initiated. Module waiting for confirmation code.
Green and Blue LEDs blinking	Locked	Waiting for Administrative User PIN to enter Administrative User mode.
Blue LED solid	Locked	Administrative User Mode. Ready to accept Administrator commands.
The LEDs illuminate alternately from Red to Green and then to Blue, followed by Red LED blinking two seconds, same pattern repeats	Failed	SC KATs fail
A faded illumination of Red and Blue LEDs	Failed	SC Firmware Integrity Test fail
Green LED blinks constantly	Failed	EC KATs fail or EC Firmware Integrity Test fail
Green LED blinking quickly	Locked	Adding Standard User/Self-Destruct PINs in progress
Blue LED blinking quickly	Locked	Adding Administrative User PIN in progress
Blue LED solid and Green Blinking	Locked	Ready to accept new PIN.
Green and Blue LEDs blink alternately	Locked	Unlocking in progress
Green LED solid	Unlocked	Unlocked. No communication or data transfer or via USB
Green LED blinks	Unlocked	Unlocked. Communicating or transferring data in progress

3. ROLES, SERVICES, AND AUTHENTICATION

3.1 ROLES AND SERVICES

The iStorage diskAshur PRO² supports two distinct and separate identities and roles: Standard User and Administrative User. An identity can be assigned to either a Standard User or Administrative User role. Both can access the private partition and user data stored in the device.

The role is explicitly selected during authentication (refer to Table 6)

Table 5 defines all services and operations that can be performed by the diskAshur PRO² module.

Table 5 - Services Authorized for Each Role

Operator	Services	Accessible CSP	CSP Access
Standard User Role	Open private partition for read/write access of user data	Standard User PIN Standard User KEK Standard User PBKDF SALT DEK	READ
	Read or write private partition with user data		
	Configure the partition as write-protect		
	Check Firmware Version		
	Change User PIN	Standard User PIN SP 800-90A state variables Standard User KEK Standard User PBKDF SALT DEK	READ/WRITE
	Lock private partition to prevent read/write access to user data	N/A	N/A
Administrative User Role	Open private partition for read/write access of user data	Administrative User PIN Administrative User KEK Administrative User PBKDF SALT DEK	READ
	Read or write private partition with user data		
	Configure the partition as write-protect		
	Check Firmware Version		
	Set unattended auto-lock time		
	Check unattended auto-lock time		
	Set User PIN policy		
	Check User PIN policy		

Operator	Services	Accessible CSP	CSP Access
	Change Admin/User/SD PIN	Standard User PIN Administrative User PIN SD PIN SP 800-90A state variables Standard User KEK Standard User PBKDF SALT Administrative User KEK Administrative User PBKDF SALT SD KEK SD PBKDF SALT DEK	READ/WRITE
	Add User/SD PIN		
	Delete User/SD PIN		
	Lock private partition to prevent read/write access to user data	N/A	N/A
Unauthenticated Services (no authenticated role required)	Show locked/unlocked status	N/A	N/A
	Show whether an Administrative User PIN has been set		
	Run test functions		
	Factory reset to clear all Critical Security Parameters (CSPs)	Standard User KEK Standard User PBKDF SALT Administrative User KEK Administrative User PBKDF SALT SD KEK SD PBKDF SALT	WRITE

3.2 AUTHENTICATION

The diskAshur PRO² supports identity-based authentication. The module supports a single Administrative User and a single Standard User who are authenticated via the module's keypad interface. The module does not output authentication data outside of the cryptographic boundary.

From the factory, the diskAshur PRO² drive comes with a default, pre-set Administrative User PIN of 1-1-2-2-3-3-4-4, a data encryption key generated by the module, and is pre-formatted for immediate use. The Administrative User must change the default password.

Table 6 - Authentication for IDs

Identity	Identification	Authentication	Description
Administrative User	Identified by entering the UNLOCK + 1 Key Combination	Enters 7 to15 digit PIN	This identity has full access to all Administrative User services.
Standard User	Identified by pressing the UNLOCK button	Enters 7 to15 digit PIN	This identity has full access to all Standard User services.

3.2.1 Initialization

After zeroization such as a factory reset, the module must be initialized before it can operate in an approved mode. The initialization procedure is specified in the User Manual.

3.2.2 Strength of Authentication

Authentication strength of Administrative User/Standard User is determined by PIN which must be between 7 (minimum) and 15 (maximum) digits long. The SHIFT key can be used for additional combinations, "SHIFT+1" is a separate value than just 1. Therefore, the probability of a successful, random guess of a PIN is approximately one in 20^7 or 1: 1,280,000,000. Both the Administrative User and Standard User are locked out of the module after fifteen (15) consecutive failed authentication attempts. In the unlikely event that an attacker makes fifteen attempts in one minute, the probability of successfully guessing a Standard User or Administrative User PIN before the drive disables the role is 3: 256,000,000. Furthermore, identity-based authentication further decreases the rate of false acceptance and the probability of a successful random attempt.

The Standard User PIN strength can be enhanced via a policy set by the Administrative User. The policy mandates a specific minimum length (from 7 to 15 digits) to be set, as well as the option to extend the keyboard character set to include the input of a "Special Character". The "Special Character" functions as "SHIFT + digit".

3.2.3 Self-Destruct Feature

The diskAshur PRO² has been designed with a self-destruct feature that zeroizes all plaintext secret keys and CSPs. The Administrative User creates an additional self-destruct PIN in administrative mode. When the self-destruct PIN is authenticated, the module will delete the encryption key, all data, and Admin/User PINs, it will generate a new encryption key and unlock the drive. Activating this feature will cause the self-destruct PIN to become the new Standard User PIN and the diskAshur PRO² will need to be partitioned and formatted before any new data can be added to the drive.

To trigger the self-destruct function, the user is required to press "UNLOCK" button before entering the self-destruct PIN, similar to the process for authenticating a user PIN. The strength requirements for Admin/User PINs are also applicable to self-destruct PIN. The administrator is entitled to set up or remove this feature.

This document may be freely reproduced and distributed, but only in its entirety and without modification

3.3 SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 Level 3:

- The cryptographic module provides two distinct roles: Standard User and Administrative User.
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid role or is in an error state, the operator shall not have access to any cryptographic service.
- The operator can command the module to perform the power-up self-test at any time.
- Data output is inhibited during self-tests, zeroization, key generation, authentication and error states.
- No CSPs are output from the module in any form.
- The module uses a solid red LED to indicate that it is in an approved mode of operation.

4. PHYSICAL SECURITY

The diskAshur PRO² Module is a multi-chip standalone device whose cryptographic boundary is defined as the perimeter of the outer enclosure that contains a single PCB and either a hard disk drive (HDD) or solid- state storage device (SSD) of various memory sizes. The opaque outer enclosure provides tamper evidence in the event the enclosure is opened. Regular inspections of the outer enclosure should be conducted for evidence of tampering.

Two tamper-evident design concepts have been implemented in the diskAshur PRO² enclosure. Firstly, all screws are underneath the "Pressed Metal Top Cover" which is adhered to the "Top Moulding" using a strong adhesive. If an attempt is made to open the enclosure, in order to access the internal components, the "Pressed Metal Top Cover" will be deformed thereby making it evident that someone has tampered with the product. Secondly, the "Pressed Metal Top Cover" incorporates breakaway plastic clips on both sides that leave further evidence of tamper if the enclosure is opened.

To prevent the security integrity circuits from being physically attacked, all critical components are covered by an epoxy resin on diskAshur PRO² PCB. Trying to remove any component is practically impossible without damaging them. The epoxy also adds another layer of tamper-evidence to the products.

5. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 (Operational Environment) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

6. CRYPTOGRAPHIC KEY MANAGEMENT

6.1 CSPs AND KEYS

No secret keys or CSPs are established or output by the module. PINs are entered into the module in plaintext via the keypad, but no secret keys or other CSPs are entered into the module. KEKs are derived from a PBKDF and may only be used in storage applications.

Table 7 - Secret Keys and Critical Security Parameters

CSP/Key	Use	Generation	Storage	Zeroization
Standard User PIN	Input to PBKDF to allow generation of Standard User KEK	Created by Standard User	RAM (plaintext during input and processing, deleted immediately after use)	Zeroized on lock, unlock, timeout, power-off, Factory Reset, or sufficient failed authentication attempts
Administrative User PIN	Input to PBKDF to allow generation of Administrative User KEK	Created by Administrative User	RAM (plaintext during input and processing, deleted immediately after use)	Zeroized on lock, unlock, timeout, power-off, Factory Reset, or sufficient failed authentication attempts
SD PIN	Input to PBKDF to allow generation of SD KEK	Created by Administrative User	RAM (plaintext during input and processing, deleted immediately after use)	Zeroized on lock, unlock, timeout, power-off, Factory Reset, or sufficient failed authentication attempts
Standard User KEK	256-bit AES key used to wrap the XTS-AES data encryption key (DEK)	Derived by the PBKDFv2 algorithm which uses the Standard User PIN along with Standard User Salt data	RAM (plaintext, temporarily available during execution)	Zeroized on lock, unlock, timeout, Factory Reset, or sufficient failed authentication attempts
Standard User PBKDF SALT	Input to PBKDF to allow generation of Standard User KEK	Generated by internal SP 800-90A CTR-DRBG	Plaintext in NVM	Zeroized via PIN changed/deleted, SD PIN verified, User PIN policy changed, Factory Reset, or sufficient failed authentication attempts

CSP/Key	Use	Generation	Storage	Zeroization
Administrative User KEK	256-bit AES key used to wrap the XTS-AES data encryption key (DEK)	Derived by the PBKDFv2 algorithm which uses the Administrative User PIN along with Administrative User Salt data	RAM (plaintext, temporarily available during execution)	Zeroized on lock, unlock, timeout, Factory Reset, or sufficient failed authentication attempts
Administrative User PBKDF SALT	Input to PBKDF to allow generation of Administrative User KEK	Generated by internal SP800-90A CTR-DRBG	Plaintext in NVM	Zeroized via PIN changed/deleted, SD PIN verified, User PIN policy changed, Factory Reset, or sufficient failed authentication attempts
SD KEK	256-bit AES key used to wrap the XTS-AES data encryption key (DEK)	Derived by the PBKDFv2 algorithm which uses PIN created by an Administrative User in addition to SD PBKDF Salt	RAM (plaintext, temporarily available during execution)	Zeroized on lock, unlock, timeout, Factory Reset, or sufficient failed authentication attempts
SD PBKDF SALT	Input to PBKDF to allow generation of SD KEK	Generated by internal SP800-90A CTR-DRBG	Plaintext in NVM	Zeroized via PIN changed/deleted, SD PIN verified, User PIN policy changed, Factory Reset, or sufficient failed authentication attempts
DEK	XTS-AES 256-bit Data Encryption Key (DEK) used to encrypt/ decrypt data to be stored/ retrieved from storage device	Generated by internal SP800-90A CTR-DRBG	RAM (plaintext, temporarily available during execution), wrapped with each authorized user's KEK	Zeroized on lock, unlock, power-off, timeout, Factory Reset, or sufficient failed authentication attempts
SP 800-90A CTR-DRBG state variables (seed, V, and key)	State variables for SP 800-90A CTR -DRBG	Generated internally by the module's NDRNG	RAM (plaintext, temporarily available during execution)	Zeroized via Factory Reset or sufficient failed authentication attempts

6.1.1 ZEROIZATION

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The security controller firmware will erase any temporary variables as soon as they are not required. For example, the PIN buffer is immediately cleared when the authentication is done.

All values stored in the security controller NVM provide no clues to the PIN, the DEK, or the KEK values. When resetting the device or deleting a user, the related NVM values will be sanitized to guarantee there is no possibility of revoking the accounts. More specifically, the zeroization involves two rounds of complete overwrites of the memory content.

There is no non-volatile memory available in the encryption controller, thus any sensitive data passed to the encryption controller will not be stored. The temporary variables are erased as soon as no longer required.

Factory reset (zeroization) is initiated by the following procedure:

- *In Standby state, press and hold "0" button until all LEDs blink alternatively on and off*
- *Press and hold down "2 + 7" buttons until all LEDs become solid for a second and then to a solid RED LED*

In addition, if an incorrect PIN is entered 15 (3 x 5 PIN clusters) consecutive times, the module's Brute Force Defense Mechanism (zeroization) is activated, and then all data including, Admin/User/SD PINs, the encryption key and all CSPs will be deleted and lost forever.

6.2 ALGORITHMS

6.2.1 FIPS APPROVED ALGORITHMS

Table 8 lists all the approved algorithms used in the module.

Table 8 - FIPS Approved Algorithms

Certificate	Algorithm	Standard(s)	Modes/Methods	Key Lengths, Curves, or Moduli	Use
4642	AES	FIPS 197, NIST SP 800-38A SP 800-38E	CBC, ECB, XTS	256 bits[1]	Encryption Controller: User data encryption and decryption
5179	AES	FIPS 197, NIST SP 800-38A NIST SP 800-38F	CTR, ECB, KW	256 bits	Security Controller: ECB and CTR modes are used as the basis of the CTR-DRBG and the KW mode. KW mode is implemented to wrap and recover the data key and for user authorization.
Vendor affirmed	CKG	SP 800-133			The unmodified output of the DRBG is used for symmetric key generation
1954	DRBG	NIST SP 800-90A	AES-256 based CTR-DRBG	256 bits	Security Controller: Random number generator for encryption keys and salts.
3435	HMAC	FIPS 198-1	HMAC-SHA-256	256 bits	Security Controller: Algorithmic basis of PBKDF.

[1] 128 bit AES is included in the CAVS certificate, but is not used by any of the module's services

This document may be freely reproduced and distributed, but only in its entirety and without modification

Certificate	Algorithm	Standard(s)	Modes/Methods	Key Lengths, Curves, or Moduli	Use
Vendor Affirmed	PBKDF	RFC 2898, NIST SP 800-132 (supports option 2a of section 5.4)	HMAC-SHA-256 (Cert. 3435)	256 bits	Security Controller: This algorithm accepts the user's PIN as input and generates the KEK.
4183	SHS	FIPS 180-4	SHA-256	256 bits	Security Controller: Algorithmic basis of PBKDF.

6.2.2 FIPS ALLOWED ALGORITHMS

Table 9 lists all the non-approved algorithms used in the module.

Table 9 - FIPS Allowed Algorithms

Algorithm	Use
NDRNG	Security Controller: Entropy source for seed to CTR-DRBG

7. EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

8. SELF-TESTS

When the module is powered on, it performs initialization and runs a sequence of self-tests. If any of these tests fails, the module transitions to an error state. In this state, the module cannot perform any cryptographic services and is not usable. Table 10 summarizes the power-up self-tests.

Table 10 - Power-Up Self-Tests

Tested Function	Self-Test	Error State	Error Indicator	Access	Resolving Error
Firmware Integrity Tests					
SC Firmware Integrity Test	Cyclic Redundancy Check - CRC-32	Power-Up Self-Test Failed	A faded illumination of Red and Blue LEDs	All SC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.
EC Firmware Integrity Test	Cyclic Redundancy Check - CRC-16	Power-Up Self-Test Failed	Green LED blinks constantly	All EC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.

Known Answer Tests (KATs)					
CTR-DRBG	DRBG KATs include the following: • Instantiate • Generate • Reseed	Power-Up Self-Test Failed	The LEDs illuminate alternately from Red to Green and then to Blue, followed by Red LED blinking two seconds, same pattern repeats	All SC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.
PBKDF	PB KDF KAT includes: • SHA-256 KAT • HMAC-SHA-256 KAT	Power-Up Self-Test Failed		All SC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.
AES (Cert. #5179)	AES SC Encrypt KAT AES SC Decrypt KAT	Power-Up Self-Test Failed		All SC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.
AES Key Wrap (Cert. #5179)	KW-AE KAT KW-AD KAT	Power-Up Self-Test Failed		All SC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.
AES (Cert. #4642)	AES EC Encrypt KAT AES EC Decrypt KAT	Power-Up Self-Test Failed	GREEN LED Blinks constantly	All EC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful.

Table 11 - Conditional Self-Tests

Tested Function	Self-Test	Initiation	Error State	Error Indicator	Access	Resolving Error
Conditional Tests						
NDRNG	FIPS 140-2 Continuous RNG test to ensure output is different than the previous value	Initiated on every call to instantiate/reseed [SP 800-90A] CTR-DRBG	Conditional Self-test failed	The device is securely reset	All cryptographic operations and data output are inhibited	Power cycle the device to reinitiate it. Module can be used if power-up and conditional self-tests are successful.

Tested Function	Self-Test	Initiation	Error State	Error Indicator	Access	Resolving Error
Conditional Tests						
AES-XTS-256	FIPS 140-2 implementation guidance A.9 XTS-AES Key Generation test	Initiated on every call to generate a DEK	Conditional Self-test failed	The device is securely reset	All EC cryptographic operations and data output are inhibited	Power cycle the device to reinitiate it and initiate another call to re-generate a XTS-AES Key

9. APPENDIX A: REFERENCES

Table 12 – References

Reference Number	Reference Title	Publishing Entity	Publication Date
[1]	Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program.	NIST	March 2018
[2]	SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation.	NIST	January 2018
[3]	Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.	NIST	January 2016
[4]	FIPS 197: Specification for the ADVANCED ENCRYPTION STANDARD (AES).	NIST	November 2001
[5]	SP 800-38A: Recommendation for Block Cipher Modes of Operation.	NIST	December 2001
[6]	SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices.	NIST	January 2010
[7]	SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.	NIST	December 2012
[8]	SP 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators.	NIST	June 2015
[9]	FIPS 180-4: Secure Hash Standard (SHS).	NIST	August 2015
[10]	FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC).	NIST	July 2008
[11]	SP 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications.	NIST	December 2010

10. APPENDIX B: ABBREVIATIONS AND DEFINITIONS

Table 13 – Abbreviations and Definitions

Term	Definition
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
CRC	Cyclic Redundancy Check
ADMIN	Administrative User
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EC	Encryption Controller
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FSM	Finite State Model
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
HDD	Hard Disk Drive
KW	Key Wrap
KAT	Known Answer Test
KEK	Key Encryption Key
KC	Keypad Controller
LED	Light Emitting Diode
NVM	Non-Volatile Memory
PBKDF	Password Based Key Derivation Function
PIN	Personal Identification Number
RAM	Random Access Memory
SALT	Random value used to improve security of cryptographic algorithms
SC	Security Controller
SD	Self-Destruct
SHA	Secure Hash Algorithm
SSD	Solid State Drive
NDRNG	Non-Deterministic Random Number Generator
USB	Universal Serial Bus