SECURE USB FLASH DRIVE
datAshur Pro 3.0

Non-Proprietary Security Policy

FIPS 140-2 SECURITY POLICY VERSION 1

Contents

1 Definitions and Acronyms

AES	Advanced Encryption Standard
CMAC	Cipher-Based Message Authentication Code
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CSP	Cryptographic Security Parameter
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
EBC	Electronic Code Book
EC	Encryption Controller
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Protocol
HMAC	Hash-Based Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
NVRAM	Non-Volatile Random Access Memory
PBKDFv2	Password Based Key Derivation Algorithm Version 2
PIN	Personal Identification Number
RAM	Random Access Memory
Salt	Random value used to improve security of cryptographic algorithms
SC	Security Controller
SHA	Secure Hash Algorithm
SIV	Synthetic Initialization Vector
USB	Universal Serial Bus

2 Product Overview

iStorage datAshur Pro 3.0 Secure USB Flash Drive ("iStorage datAshur Pro" or "datAshur Pro") 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 the use of a NIST approved DRBG (ref: SP800-90A). The seed for the DRBG is also produced within the module from a hardware-based entropy generator.

Capacity	Hardware Revision	EC Firmware Revision	SC Firmware Revision
8 GB	IS-FL-DA3-256-8	MPALL_F1_6600_v384_0A-0002	v1.11
16 GB	IS-FL-DA3-256-16	MPALL_F1_6600_v384_0A-0002	v1.11
32 GB	IS-FL-DA3-256-32	MPALL_F1_6600_v384_0A-0002	v1.11
64 GB	IS-FL-DA3-256-64	MPALL_F1_6600_v384_0A-0002	v1.11

Figure 1: iStorage datAshur Pro cryptographic boundary showing input buttons and status LEDs

2.1 Validation Level

The cryptographic module meets the overall requirements applicable to Level 3 Security of FIPS 140-2.

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

Table 1: Module Security Level Specification

3 Modes of Operation

The iStorage datAshur Pro 3.0 Secure USB Flash Drive supports only a single, FIPS approved mode of operation.

4 Cryptographic Algorithms

The following algorithms are implemented in all datAshur Pro modules:

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Length(s)	Use
3749	XTS-AES	NIST SP 800-38E	*ECB*	*256*	*Encryption Controller* Encryption of user data within storage application only.
1032	DRBG	NIST SP 800-90A	*CTR*	--	*Security Controller* Random number generator for encryption keys and salts
3757	AES[1]	FIPS 197	*CMAC* *ECB* *CTR*	*256*	*Security Controller* Block cipher basis of CTR-DRBG. Algorithmic basis of SIV.
3127	SHS	FIPS 180-4	*SHA-1*	--	*Security Controller* Algorithmic basis of HMAC-SHA1
2459	HMAC-SHA-1	FIPS 198-1	--	*160*	*Security Controller* Algorithmic basis of PBKDFv2
Vendor Affirmation	PBKDFv2	NIST SP 800-132	--	--	*Security Controller* Deriving keys for storage application only. Key encryption key generation. Password is the same as the User/CO PIN with a minimum length of 7 digits 0-9. Depends on HMAC-SHA1. It is conformant to FIPS 140-2 Implementation Guidance (IG) D.6: the module supports option 2a as documented in NIST SP 800-132, Section 5.4.

Table 2: Approved Algorithms

Algorithm	Reference	Caveat	Use
NDRNG – Entropy source internal to the module		The module generates cryptographic keys with 256-bit minimum entropy strength	*Security Controller* Entropy source for seed to CTR-DRBG

Table 3: Allowed Algorithms

[1] *Other modes are also available but not used within the module*

5 Cryptographic Module Specification

The datAshur Pro is a multi-chip standalone cryptographic module as defined by FIPS 140-2. It consists of a USB 3.0 capable encryption controller, eMMC memory, a security controller, a non-replaceable battery, and a user interface with three LED and eleven (11) buttons. The module is encapsulated within an opaque, production grade integrated circuit package. The cryptographic boundary is defined by the module's metal enclosure. See Figure 1 and Figure 2.

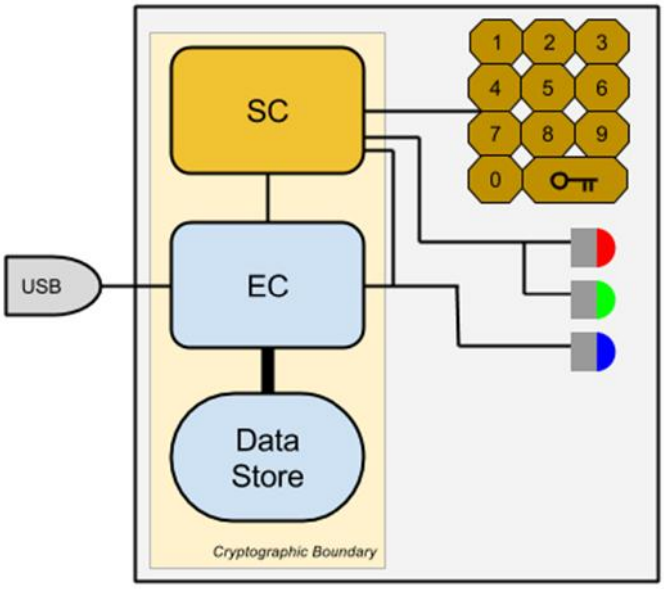

Figure 2: datAshur Pro module architecture

6 Ports and Interfaces

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

Physical Port	Logical Interface	Description
USB Port	Data input Data output Control input Status output	Connects the module to the host computer. 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. When the drive is locked this USB interface is disabled.
Alphanumeric Keypad (0-9)	Data input	Ten alphanumeric labeled buttons that connect to security controller button inputs. Used to enter User or CO PIN.
KEY button	Control input	KEY button that connects to security controller button input. Used to awaken the module from low-power sleep and to control UI flow including participation in selecting the role.
Red, green and blue LEDs	Status output	See Table 5.
USB Power	External power	The USB VBUS (+5) charges the battery and will power the module when it is available.

Table 4: Physical Ports and Logical Interfaces

LED Behavior	Module State	Status Description
LEDs off	Disconnected	Low-power sleep mode
All three LEDs blink once simultaneously	-	Awakened from low-power sleep, all LEDs operational and firmware integrity test passed
No LEDs illuminate on pressing the KEY button when the module is in low-power sleep.	-	The battery may be fully discharged in which case it must be charged for at least one minute before being used. Pressing other buttons while pressing KEY or pressing KEY several times quickly may prevent the module from awakening. If the module fails the firmware integrity test, the LEDs will not illuminate.
LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates and then fades off.	Failed	Either KAT failed, NDRNG failed a self-test, or the DRBG failed a self-test.
Red LED blinking	Locked	Waiting for User PIN to unlock
Red and blue LEDs blinking	Locked	Waiting for User PIN to unlock. CO PIN is set.
Red LED on solidly	Locked	Module verifying User PIN
Green LED on solidly	Disconnected	Unlocked and ready to connect to PC
Green LED on solidly with a single blink every 2 seconds	Disconnected	Unlocked and ready to connect to PC. Drive configured in read-only mode.
Green LED on solidly and blue LED blinking	Connected	Unlocked, connected to PC via USB, and communicating or transferring data
Green and blue LEDs on solidly	Connected	Unlocked and connected to PC via USB
Blue LED blinking	Disconnected	Ready to accept new User PIN
Green LED blinking after entering new User/CO PIN	Disconnected	Ready to accept new PIN a second time as confirmation
Red and blue LEDs blinking	Unlocked and disconnected	Ready to accept new CO PIN
Red and green LEDs blinking	Locked	Waiting for CO PIN to unlock. User PIN is set.
Red and green LEDs blinking	Unlocked and disconnected	Unlocked as CO and ready to connect to PC
Blue LED blinking	Locked	No User PIN
Blue LED blinking slowly	Locked and connected	Battery charging
Red and green LEDs blinking alternately	Disconnected	Factory reset initiated. Module waiting for confirmation code.
Red LED illuminates and then fades out	Disconnected	Module locked and disconnected

Table 5: LED Status Output

The operator knows that the module is in good working order if, when pressing the KEY button to awaken the module the three LEDs blink simultaneously and one of the non-error states is shown by the module LEDs.

7 Roles and Services

The datAshur Pro supports level 3 identity-based authentication.

Role	User ID	Authentication Data	Description
User	Identifies as a user by pressing the 'KEY' button	7-15 digit PIN	User has full access to all services.
CO	Identifies as a CO by pressing the 'KEY' + '1'	7-15 digit PIN	CO has full access to all services. Unlocking module as CO will zeroize User PIN.

Table 6: Roles and required identification and authentication

From the factory, the datAshur Pro drive comes with a default, preset 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 iStorage datAshur Pro supports two distinct and separate roles: User and cryptographic officer. The role is explicitly selected during authentication:

- User
  - Press and release KEY button
  - Enter correct User PIN
  - Press and release KEY button
- CO
  - Press and hold '1' button
  - Press and release KEY button
  - Release '1' to identify as CO
  - Enter correct CO PIN
  - Press and release KEY button

Operator	Services	ID
User role	- Open private partition for read/write access of user data - Lock private partition to prevent read/write access to user data - Set User PIN - Read or write private partition with user data	1 2 3 4
CO role	- Open private partition for read/write access of user data - Lock private partition to prevent read/write access to user data - Set User PIN - Read or write private partition with user data - Set CO PIN - Zeroize User PIN	1 2 3 4 5 6
Unauthenticated (no role required)	- Show locked/unlocked status - Show whether or not drive is initialized. - Show whether or not User PIN has been set - Run self-tests - Factory reset to zeroize all CSPs	7 8 9 10 11

Table 7: Services authorized for each role

7.1 Initialization

After zeroization such as a factory reset, the module must be initialized before it will operate in an approved mode. The initialization procedure is as follows:

- Awaken drive with KEY press
- Enter default PIN, 1-1-2-2-3-3-4-4.
- Press and hold the '1' button.
- Double press and release KEY button. Release '1' button.
- Observe that red and blue LEDs are blinking.
- Enter new CO PIN.
- Double press KEY button.
- Observe that green LED is blinking.
- Enter new CO PIN a second time.
- Double press KEY button.
- Observe red LED is on steadily for a couple of seconds while the CO CSPs are updated.

At any point, if the procedure does not appear to execute properly, press and hold KEY button for 3 seconds to power-off the module.

7.2 Authentication

The Crypto Officer and User roles authenticate via the module's keypad interface. The module does not output CO or User authentication data outside of the cryptographic boundary.

7.2.1 PIN Strength

Authentication strength of both User and CO is determined by PIN that is at a minimum 7 digits long. The probability of a successful, random guess of a PIN is approximately 10^7 or 10,000,000:1[2]. Both the User and CO are locked-out of the module after ten (10) consecutive failed authentication attempts. The probability of successfully guessing a User or CO PIN before the drive disables the role is 1,000,000:1.

A PIN may be up to 15 digits long.

2 Sequential and repeating PINs are not allowed. For example, the module will reject a PIN of 1-2-3-4-5-6-7 or 6-5-4-3-2-1-0. Attempts to define such a PIN will cause the module to indicate an error.

8 Critical Security Parameters

CSP	Use	Source	Storage	Creation / Destruction	Access	Role
CTR-DRBG state (seed, V, key)	Generating random values for CSPs *Services: Initialization, 1, 2, 11*	Entropy generator and CTR-DRBG	RAM	Created when DRBG is seeded i.e. every time the module initializes *Services: Initialization*	Read Write	All
				Destroyed on lock, unlock, successful generation of CSPs *Service: Initialization, 1, 2, 11*	Zeroize	
User PIN/Password	Input to PBKDFv2 to allow generation of the User KEK. *Services: 1, 2, 3, 6, 11*	Keypad entry	RAM	Created by User *Services: 1, 2, 3*	Read Write	User
				Destroyed on lock, unlock, timeout *Services: 1, 2, 6, 11*	Zeroize	
CO PIN/Password	Input to PBKDFv2 to allow generation of the CO KEK. *Services: 1, 2, 5, 6, 11*	Keypad Entry	RAM	Created by CO *Services: 1, 2, 5*	Read Write	CO
				Destroyed on lock, unlock, timeout *Services: 1, 2, 11*	Zeroize	
User Salt	Input to PBKDFv2 to generate key to wrap DEK. *Service: 3, 6, 11*	CTR-DRBG	NVRAM	Created when User changes PIN *Services: 3*	Read Write	User
				Destroyed on PIN change, zeroization *Services: 3, 6, 11*	Zeroize	
CO Salt	Input to PBKDFv2 to generate key to wrap DEK. *Service: 5, 11*	CTR-DRBG	NVRAM	Created when CO changes PIN *Services: 5*	Read Write	CO
				Destroyed on PIN change, zeroization *Services: 5, 11*	Zeroize	
XTS-AES DEK	Encryption of user data *Services: 2, 3, 5*	CTR-DRBG	RAM	Created when first password, either User or CO, is set *Services: 3, 5*	Read Write	All
				Destroyed on lock, timeout, entering low-power mode *Services: 2*	Zeroize	
User KEK	Encryption (wrapping) of DEK *Services: 1, 2*	User PIN, User Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK. *Services: 1, 2*	Read Write	User
				Destroyed immediately after use. *Services: 1, 2*	Zeroize	
CO KEK	Encryption (wrapping) of DEK *Services: 1, 2*	CO PIN, CO Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK. *Services: 1, 2*	Read Write	CO
				Destroyed immediately after use. *Services: 1, 2*	Zeroize	
HMAC-SHA-1	PBKDFv2 *Services: 1, 2*	DRBG	RAM	Created before encrypting or decrypting the DEK. *Services: 1, 2*	Read Write	All
				Destroyed immediately after use. *Services: 1, 2*	Zeroize	

AES CTR AES CMAC	SIV *Services: 1, 2*	PBKDFv2	RAM	Created during authentication to the module, before encrypting or decrypting the DEK. *Services: 1, 2*	Read Write	All
				Destroyed immediately after use. *Services: 1, 2, 11*	Zeroize	
AES CTR	DRBG *Service: Initialization*	NDRNG	RAM	Generated for seeding the DRBG *Service: Initialization*	Read Write	All
				Destroyed immediately after use. *Service: Initialization*	Zeroize	

Table 8: Critical security parameters

8.1 Zeroization

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle on NVRAM to zeroize CSPs. RAM copies of CSPs are erased by setting the memory to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

Factory reset is initiated by the following procedure:

- Press and hold '7' button.
- Press and release KEY button to awaken drive.
- Observe red and green LEDs are lighting alternately.
- Enter confirmation code 9-9-9.
- Press and hold '7' button.
- Press and release KEY button to confirm factory reset.
- Observe red and green LEDs on steadily for several seconds while CSPs are zeroized.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User authentication credentials, the salts and SIV outputs for the User and the CO. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User PIN.

The second kind of brute-force attack is against the CO PIN. Ten consecutive failed attempts to unlock the module as CO will zeroize all CSPs including the CO and User credentials and the DEK leaving the module in the factory reset state.

9 Self-Tests

When the module awakens from low-power mode, it performs module initialization and runs a sequence of self-tests. If any of these tests fails, the drive will signal an error and enter an error state. The module cannot perform any cryptographic services and is not usable in this state. The module also performs continuous self-tests. Table 9 summarizes the self-tests.

Self-Test	Component	When Executed	Relevant Certificate
Firmware CRC	SC	Module initialization	N/A
CTR-DRBG KATs -- Instantiate KAT -- Generate KAT CTR-DRBG Uninstantiate (Includes AES ECB)	SC	Module initialization	CAVP Validation #1032 CAVP Validation #3757
PBKDFv2 KAT (Includes HMAC-SHA-1)	SC	Module initialization	CAVP Validation #3127 CAVP Validation #2459
SIV KAT (Includes AES ECB and CMAC)	SC	Module initialization	CAVP Validation #3757
Firmware CRC	EC	Module unlocked	N/A
XTS-AES; encrypt & decrypt	EC	Module unlocked	CAVP Validation #3749

Table 9: Self-tests

The EC only receives power after a correct PIN has been entered and the module unlocks. Immediately after receiving power, the EC performs its self-tests. If any test fails, the EC will not connect the module data store to the host computer and the SC will return the module to the low-power mode after 30 seconds.

The continuous self-tests summarized in Table 10 are performed as required by the FIPS PUB SP-800 90A.

Self-Test	Component
CTR-DRBG Continuous Test	SC
NDRNG Continuous Test	SC

Table 10: Continuous Self-tests

10 Security Rules

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

1. The cryptographic module provides two distinct operator roles: User and Cryptographic Officer.
2. The cryptographic module provides identity-based authentication.
3. 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.
4. The operator is capable of commanding the module to perform the power-up self-test at any time by awakening the module from low-power mode.
5. Data output is inhibited during self-tests, zeroization, key generation and authentication.
6. No CSPs are output in any form from the module.
7. The module generates cryptographic keys with 256-bit minimum entropy strength.

11 Physical Security Policy

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

- Production grade components
- Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components
- SC memory protection enabled to prevent read-out of the SC firmware, RAM, or NVRAM

The operator should, on a periodic basis, visually inspect the module to determine if it has been compromised. The following steps should be followed:

- Grasp module in one hand and lightly pull the lanyard with the opposite hand
- If the module separates, the operator should suspect that the module has been tampered
- If the module remains intact, no tamper should be suspected

Note: The module epoxy hardness testing was only performed at ambient temperature; no assurance is provided for level 3 hardness conformance at any other temperature.

12 Mitigation of Other Attacks Policy

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

13 References

Reference Number	Reference Title
[1]	FIPS PUB 140-2 Security Requirements for Cryptographic Modules / NIST May 2001
[2]	Derived Test Requirements for FIPS PUB 140-2 – Security Requirements for Cryptographic Modules
[3]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program / NIST May 10, 2016
[4]	NIST SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015
[5]	FIPS 197 – Advanced Encryption Standard (AES)
[6]	FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)
[7]	FIPS 180-4 – Secure Hash Standard (SHS)
[8]	NIST SP 800-132 – Recommendation for Password-Based Key Derivation
[9]	RFC 5297 Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)