DATALOCKER, INC., K350

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

TABLE OF CONTENTS

List of Tables

List of Figures

1 GENERAL

1.1 OVERVIEW

This document defines the Security Policy for the DataLocker, Inc., (DataLocker) K350 module, hereafter "the module".

The physical form of the module is depicted in Figure 1. The module is a multi-chip standalone embodiment as defined by FIPS 140-3 and conforms to Security Level 3.

1.2 SECURITY LEVELS

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

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The module, depicted in Figure 1 below, is an encrypted portable storage device, featuring three crypto processors, which provide layers of cryptographic protection. It requires no additional software or drivers to be installed on the host PC. As shown in Figure 2, the three processors are STMicroelectronics STM32L452VE, NXP

JCOP3, and Fujitsu/Socionext MB86C31. The module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated encrypted storage.

Figure 1: K350

Purpose and Use:
The K350 is a portable encrypted storage drive.

Module Type: Hardware

The K350 is defined as hardware module (*refer to ISO/IEC 19790, Section 7.2.2*).

Module Embodiment: MultiChipStand
The K350 is defined as a multiple chip standalone cryptographic module.

Module Characteristics:
The critical components within the module are encapsulated inside a hard, opaque, production grade epoxy.

Cryptographic Boundary:
The cryptographic boundary is defined as the perimeter of the epoxy that encapsulates all the module's components on the printed circuit board (PCB).

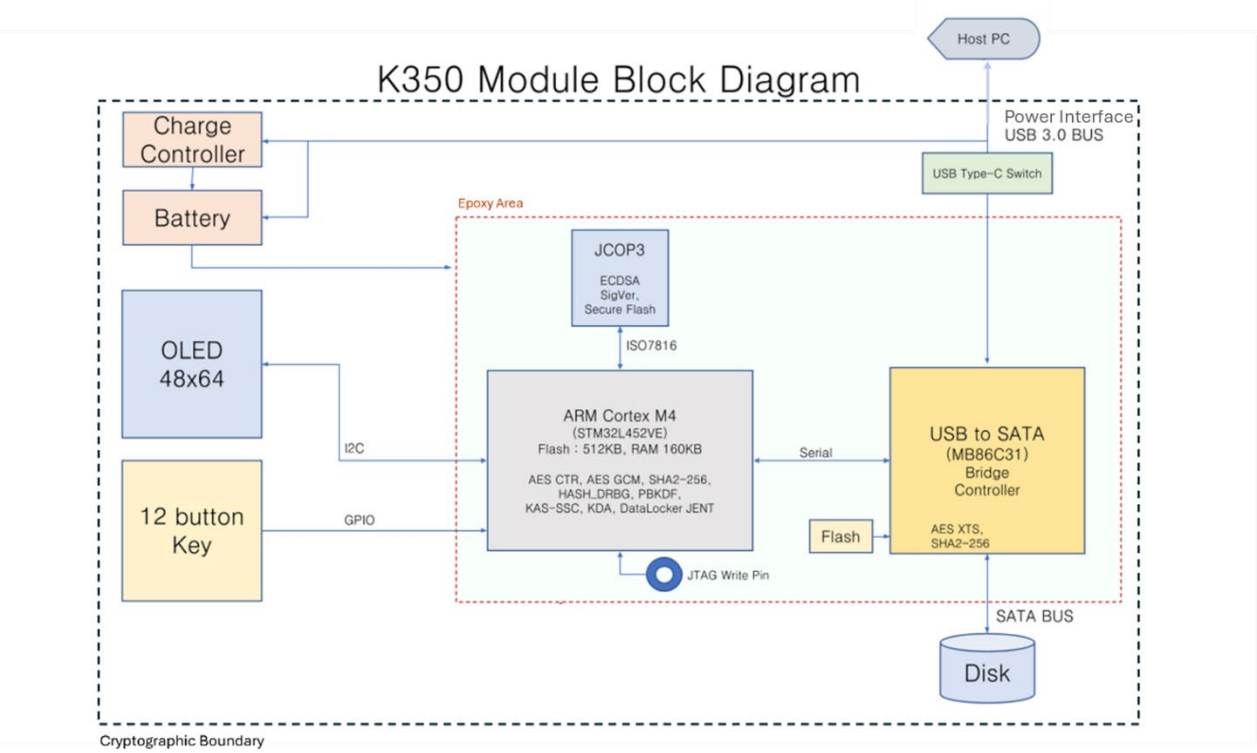

Figure 2: Block Diagram

N.B. The JTAG Write PIN Interface shown in Figure 2 is used to write firmware on debug devices. On production devices, the configuration setting is such that the JTAG interface cannot be used to read, erase, or program the STM32 flash memory.

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The K350 cryptographic module is designed to meet the requirements of FIPS 140-3 Security Level 3 (refer to Table 1). The module is available in the following configuration (refer to Table 2):

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
SK350-016-FE	K350 - 16GB	App: 3.07 Bootloader: 1.03	STMicroelectronics STM32L452VE	16GB
SK350-064-FE	K350 - 64GB	App: 3.07 Bootloader: 1.03	STMicroelectronics STM32L452VE	64GB
SK350-128-FE	K350 - 128GB	App: 3.07 Bootloader: 1.03	STMicroelectronics STM32L452VE	128GB
SK350-256-FE	K350 - 256GB	App: 3.07 Bootloader: 1.03	STMicroelectronics STM32L452VE	256GB
SK350-512-FE	K350 - 512GB	App: 3.07 Bootloader: 1.03	STMicroelectronics STM32L452VE	512GB

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 EXCLUDED COMPONENTS

No components within the cryptographic boundary are excluded from the requirements of FIPS 140-3 under AS02.13 & AS02.14.

2.4 MODES OF OPERATION

Modes List and Description:

The module only supports an Approved mode of operation and cannot be configured to operate in a non-Approved mode. Once the operator has authenticated, the unlocked screen will display “FIPS 140-3 Level 3 AES-256-bit XTS” along with the evaluated firmware version, “K350 3.07”. The Bootloader Version (1.03) can be verified via the SDK.

Mode Name	Description	Type	Status Indicator
Approved	Only Approved services are supported	Approved	Global Indicator

Table 3: Modes List and Description

The device will not respond to service calls before it has entered its approved mode of operation.

2.5 ALGORITHMS

The K350 cryptographic module supports the approved cryptographic algorithms shown in Table 4.

Approved Algorithms:
The module supports the following approved cryptographic algorithms.

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	AES 3971	Key Length - 128, 192, 256	SP 800-38A
AES-GCM	AES 3971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-XTS	AES 5695	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
ECDSA KeyGen (FIPS186-5)	A5176	Curve - P-256 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5176	Curve - P-256	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5176	Curve - P-256 Hash Algorithm - SHA2-256	FIPS 186-5
Hash DRBG	A5176	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA2-256	HMAC 2589	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5176	Domain Parameter Generation Methods - P-256 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA OneStep Sp800-56Cr1	A5176	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 256-2048 Increment 8	SP 800-56C Rev. 2
PBKDF	A5176	Iteration Count - Iteration Count: 1000-10000 Increment 1 Password Length - Password Length: 8-64 Increment 1	SP 800-132
SHA2-256	SHS 3275	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	SHS 3299	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256	SHS 4565	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA3-256	A4438	Message Length - Message Length: 0-65536 Increment 8	FIPS 202

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module supports the following vendor affirmed algorithms (refer to Table 5).

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	SP 800-133r2 and IG D.G per Section 4 example 1, Section 5.2, and Section 6.1.
CKG XTS	Key Type:Symmetric	N/A	SP 800-133r2 and IG D.H per Section 6.3 approved method 1 and Section 4 example 1. Applicable to AES-XTS

Name	Properties	Implementation	Reference
			compliant to IG C.I because Key_1 and Key_2 are concatenated prior to usage.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Name	Type	Description	Properties	Algorithms
CSP Decryption	BC-Auth	Symmetric Decryption	Standard:NIST SP 800-38D	AES-GCM: (AES 3971) Key Type: Symmetric Key Size: 256-bit
CSP Encryption	BC-Auth	Symmetric Encryption	Standard:NIST SP 800-38D	AES-GCM: (AES 3971) Key Type: Symmetric Key Size: 256-bit
DEC	BC-UnAuth	Symmetric Decryption	Standard:FIPS 197	AES-CTR: (AES 3971) Key Size: 256 AES-XTS: (AES 5695) Key Size: 256
DRBG Generate	DRBG	Random Number Generation using HASH_DRBG based on SHA2-256	Standard:NIST SP 800-90A	Hash DRBG: (A5176) Mode: SHA2-256 Returned Bits: 256
EG	ENT-ESV	Entropy Generation	Standard:NIST SP 800-90B	SHA3-256: (A4438) Message Length Max: 65536 bits
ENC	BC-UnAuth	Symmetric Encryption	Standard:FIPS 197	AES-CTR: (AES 3971) Key Size: 256

Name	Type	Description	Properties	Algorithms
				AES-XTS: (AES 5695) Key Size: 256
Integrity	SHA	Message Digest	Standard:FIPS 180-4	SHA2-256: (SHS 4565) Message Length Max: 51200 bits
KAS	KAS-Full	Key Agreement for establishing secure session	Standard:NIST SP 800-56Ar3, NIST SP 800-56Cr1 IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides 128 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5176) Scheme: Ephemeral Unified Curve: P-256 KDA OneStep Sp800-56Cr1: (A5176) Derived Key Length: 2048
KAS-KG	CKG KAS-KeyGen	Asymmetric key generation during KAS	Standard:NIST SP 800-56Ar3	ECDSA KeyGen (FIPS186-5): (A5176) Curve: P-256 CKG: () Key Type: Symmetric and Asymmetric
PBKDF	PBKDF	Password Based Key Derivation Option 1a	Standard:NIST SP 800-132	PBKDF: (A5176) Salt Length: 256 bits Password Length: 8 - 64 bytes HMAC-SHA2-256: (HMAC 2589) SHA2-256: (SHS 3275)
PKV	AsymKeyPair-PubKeyVal	Public key validation	Standard:NIST SP 800-56Ar3, FIPS 186-5	ECDSA KeyVer (FIPS186-5): (A5176) Curve: P-256
SigVer	DigSig-SigVer	Signature Verification	Standard:FIPS 186-5	ECDSA SigVer (FIPS186-5): (A5176) Curves: P-256 SHA2-256: (SHS 3299)

Name	Type	Description	Properties	Algorithms
				Message Length Max: 51200 bits
SymKG	CKG	Symmetric Key Generation	Standard:NIST SP 800-133r2	CKG: () Key Type: Symmetric and Asymmetric Hash DRBG: (A5176)

Table 6: Security Function Implementations

2.7 ALGORITHM SPECIFIC INFORMATION

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Algorithm Validation Program (CAVP).

The module's AES-GCM implementation conforms to IG C.H scenario 2. The module uses the approved Hash DRBG to generate the IV with a length of 96-bits. The entropy source producing the DRBG seed is located inside the module's cryptographic boundary.

Per NIST SP 800-38E, AES-XTS is used for storage applications only. The module's AES-XTS implementation conforms to IG C.I. The module checks explicitly that Key_1 ≠ Key_2 before using the keys in the XTS-Algorithm to process data with them. The length of the AES-XTS data unit does not exceed 2^{20} blocks.

The PBKDF algorithm is used to derive the Key Encryption Key (KEK) via Option 2a per NIST SP 800-132 with AES-GCM (AES Cert. #3971) as the approved authenticated encryption algorithm. Per IG D.N, the PBKDF iteration count is selected to be a value between 1,000 and 10,000. It utilizes the highest possible value, as long as the time required to generate the key using the entered password is acceptable for the users. The Key Encryption Key (KEK) is the only key derived via PBKDF and may only be used for storage applications.

Compliance to SP 800-56ARev3 assurances:

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2). The key derivation function complies with NIST SP 800-56Cr2 (i.e., One-Step KDF). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of NIST SP 800-56Ar3. For KAS-ECC, the module uses C(2e,0s), thus no static key pairs are used as a part of the KAS schemes per NIST SP 800-56Ar3. Full public key validation is implemented (NIST SP 800-56Ar3 Section 5.6.2.3.3). No key confirmation is implemented.

2.8 RBG AND ENTROPY

The module incorporates a NIST SP 800-90A CTR-DRBG (Cert. #A5176) that is seeded from the module's NIST SP 800-90B validated entropy source. The unmodified output of the DRBG is used for generating cryptographic key material or random nonces.

Cert Number	Vendor Name
E131	DataLocker, Inc.

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
DataLocker JENT	Non-Physical	STMicroelectronics STM32L452VE	256 bits	Full entropy	SHA3-256 Cert. #A4438

Table 8: Entropy Sources

2.9 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90Ar1 conforming DRBG (Cert. #A5176) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-5 for the verification of digital signatures, or for the facilitation of key agreement in conformance with NIST SP 800-56Ar3.

2.10 KEY ESTABLISHMENT

The module supports the establishment of cryptographic keys using elliptic curve cryptography (ECC) in conformance with NIST SP 800-56Ar3. The module implements KAS-ECC-SSC per NIST SP 800-56Ar3 (Cert. #A5176), used in conjunction with KDA per NIST SP 800-56Cr1 (Cert. #A5176). Key establishment methodology provides at least 128 bits of encryption strength. This is used to establish secure communication sessions.

2.11 INDUSTRY PROTOCOLS

The module relies upon the standard USB and other serial protocols for communication with general purpose computer (GPC) systems.

3 CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

The module incorporates physical ports and logical interfaces. The physical ports are defined within Table 9 below:

Physical Port	Logical Interface(s)	Data That Passes
OLED Display	Data Output Status Output	Configuration data output, and status output
USB Port	Data Input Data Output Control Input Status Output Power	Plaintext data for encryption/storage and retrieval, status, command inputs
LED	Status Output	Status
Keypad	Data Input Control Input	Authentication and configuration data inputs

Table 9: Ports and Interfaces

4 ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

The module supports authentication methods for the Cryptographic Officer roles. These roles have separate authentication methods as indicated in Table 10. The authentication method of both Crypto Officer (CO) Admin and Crypto Officer (CO) Standard is the password-based authentication technique known as a Memorized Secret in conformance with NIST SP 800-140E and NIST SP 800-63B (*refer to Section 5.1.1*).

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password Verification	Username and minimum 8-character password	Password between 8 and 64 characters in length. The password is selected from 46 possible symbols, inclusive of numbers, letters, and special characters (!, *, -, %, ~, #, . , @, &, $). The password is not allowed to be linear (e.g., "12345678") or repetitive (e.g., "11111111").	The probability that a random authentication attempt will succeed is at most one in 46^8 - 118 (which is less than one in 1,000,000). The reason is that, out of 46^8 possible passwords, there are 118 linear and repetitive passwords, which are disallowed.	The module will self-destruct and zeroize all CSPs if enough consecutive failed authentication attempts are made. The number of failed authentication attempts allowed is between 10 and 50, depending on the selected configuration. Therefore, the probability that a brute force attack will succeed in one minute is at most 50 in 46^8 - 118, which is less than the required probability of one in 100,000.

Table 10: Authentication Methods

4.2 ROLES

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO) Admin	Identity	Cryptographic Officer	Password Verification
Crypto Officer (CO) Standard	Identity	Cryptographic Officer	Password Verification
Unauthenticated	Role	Unauthenticated	None

Table 11: Roles

The module does not support concurrent operators. Only one operator is allowed to access the device at any time. Operator authentication does not persist beyond power-cycling the module. The selection of roles is implicit.

4.3 APPROVED SERVICES

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Change Password	Update operator passphrase and SilentKill Code	Successful service completion.	New Password	Status	ENC DEC DRBG Generate PBKDF CSP Encryption	Crypto Officer (CO) Admin - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): E - System Base Key (SBK): E Crypto Officer (CO) Standard - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): E - System Base Key (SBK): E
Change Settings	Configure the module	Successful service completion	Configuration parameters e.g. Lockout time lengths, minimum password length, screen brightness, etc.	Status	ENC DEC	Crypto Officer (CO) Admin - System Base Key (SBK): E
Create Secondary Account	Create Secondary CO Standard account	Successful service completion	Password	Status	ENC DEC SymKG DRBG Generate	Crypto Officer (CO) Admin - System Base Key (SBK): E - Passphrase: W - DRBG-State: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CSP Encryption	- Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): G,E
Decrypt Data	Decrypt operator data in persistent storage	Successful service completion.	None	Plaintext data	ENC DEC	Crypto Officer (CO) Admin - Data Encryption Key (DEK): E Crypto Officer (CO) Standard - Data Encryption Key (DEK): E
Encrypt Data	Encrypt operator data in persistent storage	Successful service completion.	Plaintext data	None	ENC DEC	Crypto Officer (CO) Admin - Data Encryption Key (DEK): E Crypto Officer (CO) Standard - Data Encryption Key (DEK): E
Firmware Update	Update the firmware or Virtual CD-ROM contents (VCD); the VCD is not firmware and only contains data	Successful service completion.	Digitally signed firmware	Status	ENC DEC SigVer	Crypto Officer (CO) Admin - VCD-Load-Pub: E - FW-Load-Pub: E - System Base Key (SBK): E Crypto Officer (CO) Standard - VCD-Load-Pub: E - FW-Load-Pub: E - System Base Key (SBK): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Info	Retrieve device information, such as firmware version and serial number	Successful service completion.	None	Module information data e.g. Module name, version	None	Crypto Officer (CO) Admin Crypto Officer (CO) Standard
Lock Device	Log out the operator and lock the device	Successful service completion.	None	Status	None	Crypto Officer (CO) Admin - Session Encryption Key (SEK): Z - KAS-ECC Private Key (KAS-pr): Z - KAS-ECC Public Key (KAS-pub): Z - KAS-ECC Peer Public Key (KAS-peer-pub): Z Crypto Officer (CO) Standard - Session Encryption Key (SEK): Z - KAS-ECC Private Key (KAS-pr): Z - KAS-ECC Public Key (KAS-pub): Z - KAS-ECC Peer Public Key (KAS-peer-pub): Z
Login	Authenticate to the module via the keypad	Successful service completion.	Operator ID and Password	Status	PBKDF CSP Decryption	Crypto Officer (CO) Admin - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key (DEK): E - System Base Key (SBK): E Crypto Officer (CO) Standard - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): E - System Base Key (SBK): E
Remount	Dismount and remount the private partition	Successful service completion.	None	Status	CSP Decryption	Crypto Officer (CO) Admin - Data Encryption Key (DEK): E Crypto Officer (CO) Standard - Data Encryption Key (DEK): E
Reset	Soft Reset. The equivalent of power cycling	Successful service completion.	None	None	None	Crypto Officer (CO) Admin - Key Encryption Key (KEK): Z - Session Encryption Key (SEK): Z - KAS-ECC Private Key (KAS-pr): Z - KAS-ECC Public Key (KAS-pub): Z - KAS-ECC Peer Public Key (KAS-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						peer-pub): Z Crypto Officer (CO) Standard - Key Encryption Key (KEK): Z - Session Encryption Key (SEK): Z - KAS-ECC Private Key (KAS-pr): Z - KAS-ECC Public Key (KAS-pub): Z - KAS-ECC Peer Public Key (KAS-peer-pub): Z
Secure Channel	Establish an AES-CTR encrypted secure channel with Host PC	Successful service completion.	None	Status	PKV ENC DEC DRBG Generate KAS-KG KAS	Crypto Officer (CO) Admin - DRBG-State: E - System Base Key (SBK): E - Session Encryption Key (SEK): G,E - KAS-ECC Private Key (KAS-pr): G,E - KAS-ECC Public Key (KAS-pub): G,E,R - KAS-ECC Peer Public Key (KAS-peer-pub): E,W - Shared Secret (Z): G,E Crypto Officer (CO) Standard - DRBG-State: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- System Base Key (SBK): E - Session Encryption Key (SEK): G,E - KAS-ECC Private Key (KAS-pr): G,E - KAS-ECC Public Key (KAS-pub): G,E,R - KAS-ECC Peer Public Key (KAS-peer-pub): E,W - Shared Secret (Z): G,E
Self-Destruct	The module may be configured to either destroy device (DEK and firmware are destroyed) or destroy data only (DEK is destroyed and data is lost)	Successful service completion.	None	None	None	Crypto Officer (CO) Admin - DRBG-State: Z - Data Encryption Key (DEK): Z Crypto Officer (CO) Standard - DRBG-State: Z - Data Encryption Key (DEK): Z
Self-Tests	Reset the module by power-cycling to invoke self-tests on demand	Successful service completion.	None	Status	Integrity SigVer	Unauthenticated
Show Status	Status via OLED Display and LEDs	Successful service completion.	None	Module status	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show System	Show the current system configuration	Successful service completion	None	Module configuration parameters	DEC	Crypto Officer (CO) Admin - System Base Key (SBK): E Crypto Officer (CO) Standard - System Base Key (SBK): E
SilentKill	Destroys all copies of the DEK, invalidates passphrases, and generates a new DEK	Successful service completion.	Silent Kill code	Status	ENC DEC SymKG DRBG Generate EG PBKDF	Crypto Officer (CO) Admin - DRBG-EI: G,E - DRBG-State: G,E,Z - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): G,Z - System Base Key (SBK): E Crypto Officer (CO) Standard - DRBG-EI: G,E - DRBG-State: G,E,Z - Passphrase: W,E - Key Encryption Key (KEK): G,E - Data Encryption Key (DEK): G,Z - System Base Key (SBK): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Zeroize Drive	Destroys all copies of the DEK, invalidates passphrases, and generates a new DEK. If the command is received via the SDK, then the module may be configured to destroy device instead (DEK and firmware are destroyed).	Successful service completion	None	Status	ENC DEC SymKG DRBG Generate EG	Crypto Officer (CO) Admin - DRBG-State: G,E,Z - Passphrase: G,E,Z - Key Encryption Key (KEK): Z - Data Encryption Key (DEK): G,E,Z - KAS-ECC Private Key (KAS-pr): Z - Session Encryption Key (SEK): Z - System Base Key (SBK): G,E,Z - DRBG-EI: G,E

Table 12: Approved Services

4.4 NON-APPROVED SERVICES

N/A for this module.

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

The module supports firmware updates by the Cryptographic Officer role (both Crypto Officer (CO) Admin and Crypto Officer (CO) Standard) through a secure firmware-loading mechanism. Upon authentication of the Cryptographic Officer, a Secure Channel (via the *Secure Channel* service) is established to logically isolate and to protect the confidentiality and integrity of the firmware image during transfer. The *Firmware Update* service should then be called. The firmware image is digitally signed using ECDSA P-256 and verified within the module using an embedded public key prior to installation. The module inhibits all data output interfaces during the firmware update, and no cryptographic operations are performed. Only after successful verification does the module write the updated firmware to protected memory and perform a controlled power-cycle to activate the firmware. This mechanism provides assurance that only authenticated, integrity-verified firmware can be loaded, satisfying the controls and isolation requirements of ISO/IEC 19790 Annex B and FIPS 140-3 IG 10.3.A.

5 SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

The module includes the following firmware components that include separate firmware integrity tests:

- Bootloader: Signature Verification (ECDSA, Cert. #A5176), P-256
- Firmware: Signature Verification (ECDSA, Cert. #A5176), P-256

The module will transition to its error state upon the failure of either firmware integrity test.

5.2 INITIATE ON DEMAND

Self-tests may be initiated on demand by power cycling the module or invoking a soft reset via the services.

6 OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module does not contain a modifiable operational environment. The module's operational environment is limited. The module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the module defined by this Security Policy or covered by this validation.

7 PHYSICAL SECURITY

7.1 MECHANISMS AND ACTIONS REQUIRED

The K350 is protected by an opaque epoxy and conforms to FIPS 140-3 Level 3 physical security requirements.

The operator is required to physically inspect the module for indications of tampering attempts at intervals specified by their organization's policies. The fascia can be removed without tamper evidence and should be inspected when examining for tamper evidence.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	Each use	Examine the outer enclosure for evidence of tampering.

Table 13: Mechanisms and Actions Required

7.2 EFP/EFT INFORMATION

The module does not support environmental failure protection (EFP) mechanisms for high/low voltage and temperature extremes. The module underwent environmental failure testing (EFT) instead (refer to Table 14).

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-90°C	EFT	Shutdown
HighTemperature	135°C	EFT	Shutdown
LowVoltage	3.7V	EFT	Shutdown
HighVoltage	8.1V	EFT	Shutdown

Table 14: EFP/EFT Information

7.3 HARDNESS TESTING TEMPERATURE RANGES

The module has been tested at the operational, storage and distribution temperatures listed in Table 15. The module's epoxy hardness is assured within these ranges.

Temperature Type	Temperature
LowTemperature	-20°C
HighTemperature	60°C

Table 15: Hardness Testing Temperatures

8 NON-INVASIVE SECURITY

8.1 MITIGATION TECHNIQUES

The module does not provide protections against non-invasive security methods.

9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

9.1 STORAGE AREAS

The module supports both volatile and persistent storage of SSPs within internal RAM and Flash.

Storage Area Name	Description	Persistence Type
RAM	Plaintext in volatile memory	Dynamic
Flash (Encrypted)	Encrypted with the KEK in the ARM Cortex secure flash along with a SHA2-256 hash	Static
Flash (Plaintext)	Plaintext in the ARM Cortex secure flash	Static

Table 16: Storage Areas

9.2 SSP INPUT-OUTPUT METHODS

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
I1	Outside the module	RAM	Plaintext	Manual	Direct	PBKDF (A5176)
I2	Outside the module	RAM	Plaintext	Automated	Electronic	KAS
I3	Outside the module	Flash (Plaintext)	Plaintext	Automated	Electronic	
O1	RAM	Outside the module	Plaintext	Automated	Electronic	KAS

Table 17: SSP Input-Output Methods

9.3 SSP ZEROIZATION METHODS

The zeroization methods described within Table 18 are supported by the module. Zeroization services explicitly overwrite SSPs with zero values.

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroised by module after use	Immediately overwrites SSPs with 0s	Automatically after use

Zeroization Method	Description	Rationale	Operator Initiation
Z2	Zeroisation, SilentKill, self-destruct sequence	Immediately overwrites SSPs with 0s	Zeroisation, SilentKill, or Self-Destruct Sequence
Z3	Full Factory Zeroisation	Immediately overwrites SSPs with 0s	Select 'Zeroize Drive' from the 'Menu' and then select 'Yes'

Table 18: SSP Zeroization Methods

9.4 SSPS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Encryption Key (DEK)	Key used to encrypt user data for persistent storage.	256 - 256	Symmetric - CSP	SymKG		DEC ENC
DRBG-EI	DRBG entropy input to the Hash_DRBG.	512 - 512	ESV - CSP	EG		DRBG Generate
DRBG-State	Hash_DRBG internal state secrets, namely V and C.	994 - 256	DRBG - CSP	Hash DRBG (A5176)		DRBG Generate
FW-Load-Pub	ECDSA P-256 Public Key for firmware integrity and upgrade signature verification. Also used to verify bootloader integrity.	P-256 - 128	ECDSA - PSP	Externally		SigVer
KAS-ECC Peer Public Key (KAS-peer-pub)	ECC P-256 key used to establish the Session Encryption Key	P-256 - 128	ECDSA - PSP	Externally		KAS
KAS-ECC Private Key (KAS-pr)	ECC key used to establish the Session Encryption Key.	P-256 - 128	KAS - CSP	KAS-KG		KAS
KAS-ECC Public Key (KAS-pub)	ECC P-256 key used to establish the Session Encryption Key.	P-256 - 128	ECDSA - PSP	KAS-KG		KAS
Key Encryption Key (KEK)	Key derived from the passphrase using PBKDF2. The Key Encryption Key is used to encrypt the Data Encryption Key.	256 - NA	Symmetric - CSP		PBKDF	CSP Decryption CSP Encryption
Passphrase	Operator authentication passphrase	8-64 characters - Varies	Authentication - CSP	Externally		PBKDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Session Encryption Key (SEK)	Symmetric key is established by KAS-ECC and used for encryption of the USB session with the client application	256 - 128	Symmetric - CSP		KAS	DEC ENC
Shared Secret (Z)	The shared secret calculated per NIST SP800-56A-rev3. Used as input to the SP800-56C-rev1 KDA to establish the Session Encryption Key.	256 - 128	Shared Secret - CSP		KAS	KAS
System Base Key (SBK)	Symmetric key used to encrypt system configuration data.	256 - 256	Symmetric - CSP	SymKG		DEC ENC
VCD-Load-Pub	ECDSA P-256 Public Key for update of the Virtual CD-ROM contents (operator data stored in a restricted volume).	P-256 - 128	ECDSA - PSP	Externally		SigVer

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Data Encryption Key (DEK)		Flash (Encrypted):Encrypted	Until use	Z2 Z3	Key Encryption Key (KEK):Encrypted by DRBG-State:Generated from
DRBG-EI		RAM:Plaintext	Persists only for the life of the DRBG instantiation process	Z1	DRBG-State:Derives
DRBG-State		RAM:Plaintext	Until use	Z2 Z3	DRBG-EI:Derived From
FW-Load-Pub	I3	Flash (Plaintext):Plaintext	Until use	N/A	
KAS-ECC Peer Public Key (KAS-peer-pub)	I2	RAM:Plaintext	Until use	Z1 Z2 Z3	Shared Secret (Z):Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KAS-ECC Private Key (KAS-pr)		RAM:Plaintext	Until Use	Z1 Z2 Z3	KAS-ECC Public Key (KAS-pub):Paired With DRBG-State:Generated from Shared Secret (Z):Derives
KAS-ECC Public Key (KAS-pub)	O1	RAM:Plaintext	Until use	Z1 Z2 Z3	KAS-ECC Private Key (KAS-pr):Paired With DRBG-State:Generated from
Key Encryption Key (KEK)		RAM:Plaintext	Until use	Z1 Z2 Z3	Passphrase:Derived From Data Encryption Key (DEK):Encrypts
Passphrase	I1	RAM:Plaintext	Until use	Z1 Z2 Z3	Key Encryption Key (KEK):Derives
Session Encryption Key (SEK)		RAM:Plaintext	Until use	Z1 Z2 Z3	Shared Secret (Z):Derived From
Shared Secret (Z)		RAM:Plaintext	Until Use	Z1 Z2 Z3	Session Encryption Key (SEK):Derives KAS-ECC Peer Public Key (KAS-peer-pub):Derived From KAS-ECC Private Key (KAS-pr):Derived From
System Base Key (SBK)		Flash (Plaintext):Plaintext	Until use	Z1 Z2 Z3	DRBG-State:Generated from
VCD-Load-Pub	I3	Flash (Plaintext):Encrypted	Until use	N/A	

Table 20: SSP Table 2

10 SELF-TESTS

10.1 PRE-OPERATIONAL SELF-TESTS

All self-tests must be completed successfully prior to any other use of cryptography by the module. If one of the self-tests fails, the module enters the error state and will output an error message to the attached screen prior to shutting down; otherwise, the module indicates successful completion by presenting the login screen.

If an error is encountered during self-tests, operators must power-cycle the device to reinitiate the power-up self-tests. The module automatically assumes the Approved mode of operation upon successful completion of the self-tests.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity of Bootloader	ECDSA (Cert. #A5176) P-256	ECDSA Signature Verification	SW/FW Integrity	Success: No Error Code; Failure: Error Code	ECDSA P-256 Digital Signature Verification
Firmware Integrity of Firmware	ECDSA (Cert. #A5176) P-256	ECDSA Signature Verification	SW/FW Integrity	Success: No Error Code; Failure: Error Code	ECDSA P-256 Digital Signature Verification

Table 21: Pre-Operational Self-Tests

10.2 CONDITIONAL SELF-TESTS

The following conditional tests are performed upon power-up, on-demand and periodically.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR Encrypt (AES 3791)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Encrypt KAT	Power-up, Periodically & on-demand
AES-CTR Decrypt (AES 3971)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Decrypt KAT	Power-up, Periodically & on-demand
AES-GCM Encrypt (AES 3971)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Encrypt KAT	Power-up, Periodically & on-demand
AES-GCM Decrypt (AES 3971)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Decrypt KAT	Power-up, Periodically & on-demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Encrypt (AES 5695)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Encrypt KAT	Power-up, Periodically & on-demand
AES-XTS Decrypt (AES 5695)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Decrypt KAT	Power-up, Periodically & on-demand
ECDSA SigVer (FIPS186-5) (A5176)	P-256	KAT	CAST	Success: No Error Code; Failure: Error Code	ECDSA Signature Verification KAT	Power-up, Periodically & on-demand
Entropy Source	N/A	APT, RCT	Critical Function	Success: No Error Code; Failure: Error Code	APT and RCT	Continuous
Hash DRBG (A5176)	N/A	KAT	CAST	Success: No Error Code; Failure: Error Code	Performs a fixed input KAT and all SP 800-90A health test monitoring functions	Power-up, Periodically & on-demand
KAS-ECC-SSC Sp800-56Ar3 (A5176)	P-256	KAT	CAST	Success: No Error Code; Failure: Error Code	KAS-ECC Shared Secret Computation KAT per IG D.F	Power-up, Periodically & on-demand
KDA OneStep Sp800-56Cr1 (A5176)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	KDA KAT	Power-up, Periodically & on-demand
PBKDF (A5176)	Salt: 256-bits	KAT	CAST	Success: No Error Code; Failure: Error Code	PBKDF KAT, which also satisfies HMAC SHA2-256 KAT	Power-up, Periodically & on-demand
SHA2-256 (SHS 3275)	N/A	KAT	CAST	Success: No Error Code; Failure: Error Code	SHA2-256 KAT	Power-up, Periodically & on-demand
SHA2-256 (SHS 3299)	N/A	KAT	CAST	Success: No Error Code; Failure: Error Code	SHA2-256 KAT	Power-up, Periodically & on-demand
SHA2-256 (SHS 4565)	N/A	KAT	CAST	Success: No Error Code;	SHA2-256 KAT	Power-up, Periodically & on-demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Failure: Error Code		
SHA3-256 (A4438)	N/A	KAT	CAST	Success: No Error Code; Failure: Error Code	SHA3-256 KAT	Power-up, Periodically & on-demand
AES-XTS Key1 does not equal Key2	N/A	N/A	Critical Function	Success: No Error Code; Failure: Error Code	Occurs anytime the module generates the DEK. Per IG C.I this check explicitly that Key_1 and Key_2 are distinct.	AES-XTS Key Generation
Firmware Load Test	ECDSA P-256	Digital Signature Verification	SW/FW Load	Success: No Error Code; Failure: Error Code	Firmware load test occurs during 'Firmware Update' service.	During Firmware Updates
Public Key Validation	P-256	N/A	Critical Function	Success: No Error Code; Failure: Error Code	Occurs during KAS upon receipt of the connected host application public key (KAS-ECC Peer Public Key).	During key agreement
ECC CDH Pair Wise Consistency Test	P-256	PCT	PCT	Success: No Error Code; Failure: Error Code	Occurs during KAS upon the generation of the KAS-ECC private and public keypair.	During key agreement

Table 22: Conditional Self-Tests

10.3 PERIODIC SELF-TEST INFORMATION

The module will perform periodic self-tests at every power-on.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity of Bootloader	ECDSA Signature Verification	SW/FW Integrity	Every Power-On	Automatic invocation of self-test service
Firmware Integrity of Firmware	ECDSA Signature Verification	SW/FW Integrity	Every Power-On	Automatic invocation of self-test service

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR Encrypt (AES 3791)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-CTR Decrypt (AES 3971)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-GCM Encrypt (AES 3971)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-GCM Decrypt (AES 3971)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-XTS Encrypt (AES 5695)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-XTS Decrypt (AES 5695)	KAT	CAST	24 hours	Automatic invocation of self-test service
ECDSA SigVer (FIPS186-5) (A5176)	KAT	CAST	24 hours	Automatic invocation of self-test service
Entropy Source	APT, RCT	Critical Function	Continuous	N/A
Hash DRBG (A5176)	KAT	CAST	24 hours	Automatic invocation of self-test service
KAS-ECC-SSC Sp800-56Ar3 (A5176)	KAT	CAST	24 hours	Automatic invocation of self-test service
KDA OneStep Sp800-56Cr1 (A5176)	KAT	CAST	24 hours	Automatic invocation of self-test service
PBKDF (A5176)	KAT	CAST	24 hours	Automatic invocation of self-test service
SHA2-256 (SHS 3275)	KAT	CAST	24 hours	Automatic invocation of self-test service
SHA2-256 (SHS 3299)	KAT	CAST	24 hours	Automatic invocation of self-test service

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (SHS 4565)	KAT	CAST	24 hours	Automatic invocation of self-test service
SHA3-256 (A4438)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-XTS Key1 does not equal Key2	N/A	Critical Function	N/A	N/A
Firmware Load Test	Digital Signature Verification	SW/FW Load	N/A	N/A
Public Key Validation	N/A	Critical Function	N/A	N/A
ECC CDH Pair Wise Consistency Test	PCT	PCT	N/A	N/A

Table 24: Conditional Periodic Information

10.4 ERROR STATES

The module incorporates a single error state (refer to Table 25).

Name	Description	Conditions	Recovery Method	Indicator
Error State	The module supports a single error state that is entered upon identification of a fatal error. Once the error state is entered, an error message is logged and displayed on the screen and the module will shutdown. No cryptographic operations are available within the Error state. The last error is displayed to the authorized operator upon each power-on until cleared.	Failure of any self-test	Power cycle	Error message on OLED display

Table 25: Error States

10.5 OPERATOR INITIATION OF SELF-TESTS

Self-tests may be invoked on demand by power cycling the module or invoking a soft reset through the services.

11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements.

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The module does not include a default passphrase. Upon first use, the module enforces the Crypto Officer (CO) Admin to configure their own during initialization. If the optional secondary Crypto Officer (CO) Standard role is created, the Crypto Officer (CO) Standard must also configure a passphrase. There are no other instructions for initializing the module for use in the Approved mode of operation.

11.2 ADMINISTRATOR GUIDANCE

Before the first use a Cryptographic Officer (Admin) password (8 – 64 characters) must be set (this password should not be disclosed). After this is done, the module is ready for operation.

The module's administrator's guide is shipped with the module.

Performing zeroisation will restore the drive to its factory state (blank and unformatted). A new DEK is generated when the first Password is set.

11.3 NON-ADMINISTRATOR GUIDANCE

There are no non-administrator roles.

11.4 DESIGN AND RULES

The following security rules, except for the very last one, are enforced by the cryptographic module to ensure the FIPS 140-3 security requirements are met.

1. The module provides two distinct, authenticated operator roles: Cryptographic Officer (CO) Admin and Cryptographic Officer (CO) Standard.
2. The module provides identity-based authentication and clears previous authentications on power cycle.
3. The module does not provide any feedback mechanisms when entering passwords.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. Data output is inhibited during password entry, key generation, self-tests, zeroisation, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which unprotected SSPs are zeroised by the zeroisation service.
8. The module does not support concurrent operators, a maintenance interface, or maintenance role.
9. The module does not have any proprietary external input/output devices used for entry/output of data.
10. The module does not output intermediate key values or plaintext CSPs; plaintext operator passwords are entered directly via the keypad.
11. All CSPs are protected from unauthorized disclosure, modification, and substitution.
12. All PSPs are protected from unauthorized modification and substitution.
13. When the module is in an error state, the operator does not have access to any cryptographic service.
14. Operators must not disclose their passwords.

11.5 END OF LIFE

Zeroise the module and dispose of it at a proper e-waste facility.

12 MITIGATION OF OTHER ATTACKS

The module is not purposefully designed to mitigate any attacks beyond the scope of FIPS 140-3 requirements.