Kanguru Defender Elite300

FIPS 140-2 Non-Proprietary Security Policy
Document Revision: 1.3
H.W. Version: 1.0
F.W. Version: 2.10.10 [1] and 2.11.10 [2]

Revision History

Author(s)	Version	Updates
Nate Cote, Kanguru Solutions	1.0	Initial public release.
Nate Cote, Kanguru Solutions	1.1	Updated flash support.
Nate Cote Kanguru Solutions	1.2	Added part numbers for 256GB Capacity to matrix
Ken Lee Kanguru Solutions	1.3	- Removed part numbers for 4GB and 8GB-PRO from matrix - Added entry for CKG to Approved Algorithms -Added minimum bits of entropy generated by NDRNG for use in key generation - Moved KTS to Non-approved algorithms - Added new security rule to address IG A.9 requirements for key comparison

Introduction

The Kanguru Defender Elite300, herein after referred to as "cryptographic module" or "module", (HW Version: 1.0; FW Version: 2.10.10 [1] and 2.11.10 [2]) is a FIPS 140-2 Level 2 multi-chip standalone cryptographic module that utilizes AES hardware encryption to secure data at rest. The module is a ruggedized, opaque, and tamper-evident USB token/storage device that connects to an external general purpose computer (GPC) outside of its cryptographic boundary to serve as a secure peripheral storage drive for the GPC. The module is a self-contained device that automatically encrypts and decrypts data copied to and from the drive from the externally connected GPC.

All files distributed with the module that are loaded into the GPC (client application and PC configuration data) are excluded from the validation.

The Kanguru Defender Elite300 has been specifically designed to address sensitive data concerns of Government and security conscious customers in a variety of markets.

Cryptographic Boundary

The physically contiguous cryptographic boundary is defined by the outer perimeter of the metal and plastic enclosure with the cap removed. The cryptographic module does not contain any removable covers, doors, or openings. The cryptographic module is available in a variety of Approved configurations. *See Appendix 1 for complete list of Approved capacities.*

The following photographs (Figures 1-6) define the cryptographic boundary:

Note: The exterior of all Kanguru Defender Elite300 models are the same regardless of hard drive capacity and colors. Models are available in 8GB, 16GB, 32GB, 64GB, 128GB, and 256GB. Models are available in the following colors: Green, Black, Red, and Silver.
(See Appendix 1 for more information)

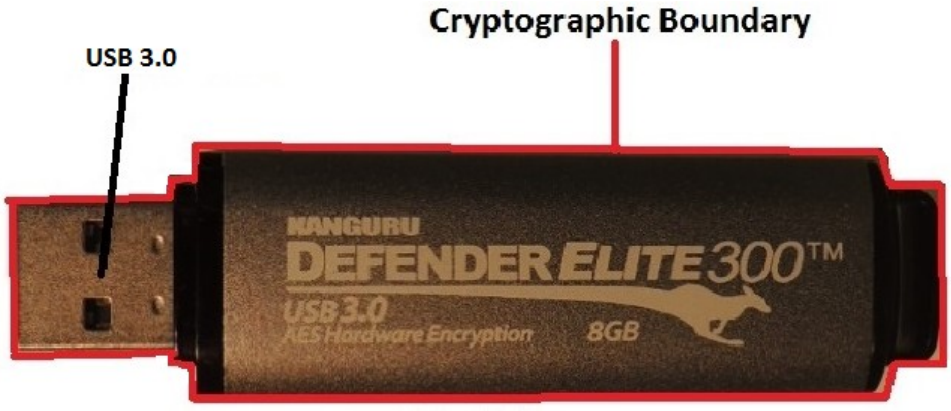

Figure 1 – Top side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

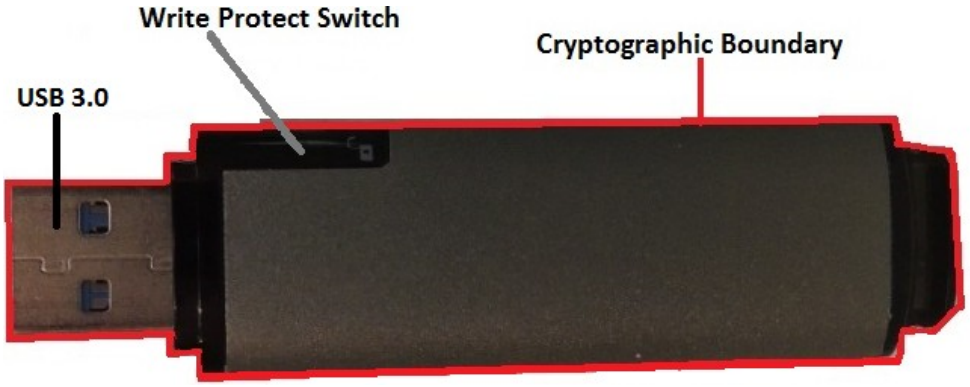

Figure 2 – Bottom side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

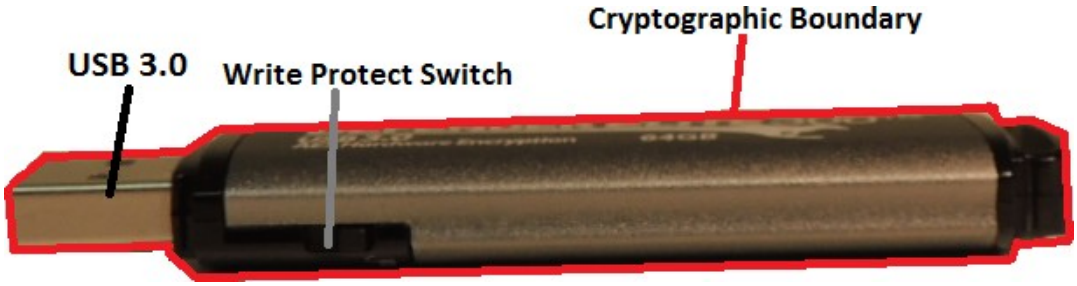

Figure 3 – Right side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

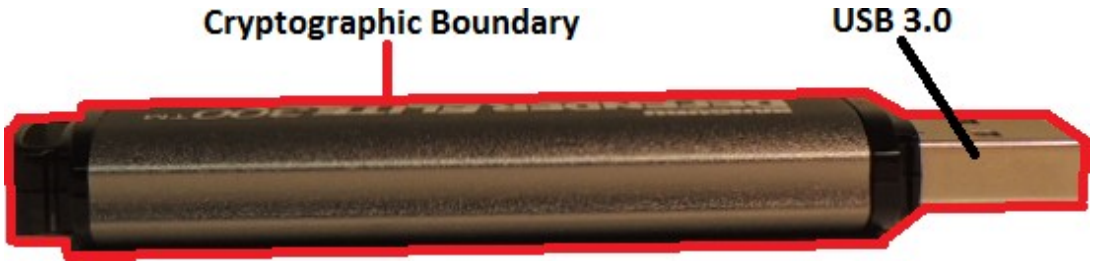

Figure 4 – Left side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

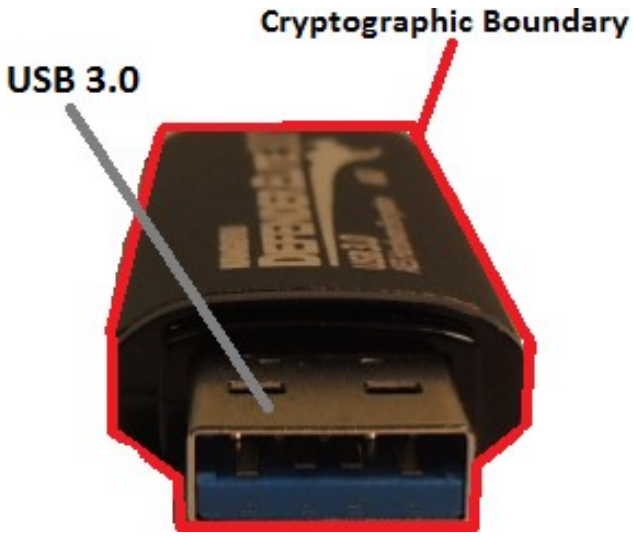

Figure 5 – Front side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

Figure 6 – Rear side of Kanguru Defender Elite300 – Model: KDFE300-8G-Silver.

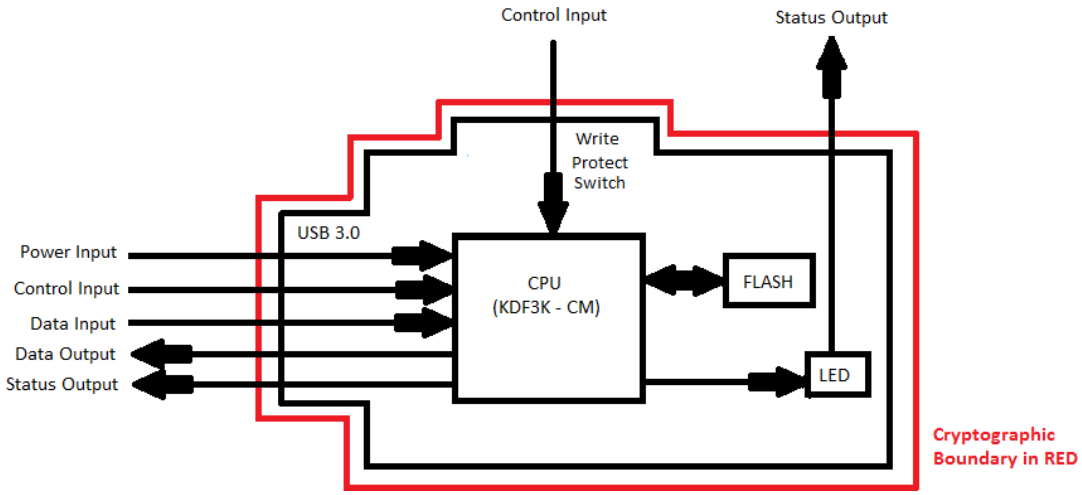

Figure 7 – Block Diagram showing data flow for Kanguru Defender Elite300 **

** NOTICE: To facilitate secure authentication, the cryptographic module supports the output of the "AES Session Key and IV" and "MAC Key of Secure Channel" RSA 2048 OAEP wrapped via the "Secure Session Public Key." The cryptographic module supports the input of the Master Disk Password and User Disk Password encrypted with AES via the "AES Session Key and IV" and authenticated with HMAC via the "MAC Key of Secure Channel" (See Exhibits 5 and 6 for more information).

With the exception of the aforementioned, all other cryptographic module services provide the associated cryptographic module I/O in plaintext.

Therefore, the Cryptographic Officer/Master, User and CD Update Officer must take special care to ensure that the module is only physically connected to a trustworthy external GPC that does not have any USB protocol analyzers attached as "all" I/O (with the exception of the aforementioned passwords and keys) is written into the module and read back from the module in plaintext form.

The cryptographic module provides no protections on any information when such information is resident inside the external GPC; any such protections are hereby explicitly disclaimed "and" hereby explicitly stated to be beyond the specific scope of this validated cryptographic module.

The methodology by which the Cryptographic Officer/Master, User and CD Update Officer determine the trustworthiness of the external GPC is beyond the specific scope of this validated cryptographic module.

Security Level Specification

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

Exhibit 1 – *Security Level Table*

Approved Algorithms

The cryptographic module supports the following Approved algorithms for secure data storage:

- AES with 256-bit key in CBC and ECB mode Encrypt/Decrypt and XTS: AES (Cert. #2962)
- SHA-256: SHS (Cert. #2491)
- HMAC-SHA256: HMAC (Cert. #1878)
- RSASSA-PKCS1_V1_5 with 2048 bit key and SHA-256 Signature Verification: RSA (Cert. #1557)
- SP 800-90A DRBG HMAC_DRBG with HMAC-SHA256 core: DRBG (Cert. #560)
- PBKDF2 (vendor affirmed); Key Establishment per Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, Special Publication 800-132, December 2010 (vendor affirmed per FIPS 140-2 IG D.6, Option 2a- The MK is used to recover the DPK through approved decryption – AES-256 (Cert. #2962); the PBKDF2 "salt" is generated by NIST SP 800-90A HMAC_DRBG and its length is 32 bytes; see password strength in "Identification and Authentication Policy" section below; The keys derived in accordance with SP 800-132 are used in storage applications only).
- CKG (vendor affirmed); In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (Vendor Affirmed). The resulting generated symmetric keys are from the unmodified output of the SP 800-90A DRBG.

Allowed Algorithms

The cryptographic module supports the following Allowed algorithms:

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

Non-Approved algorithms

The cryptographic module supports the following non-Approved algorithms:

- Hardware non-deterministic random number generator (for seeding Approved DRBG; this provides 256 bits of encryption strength)
- AES-KW (AES Cert. #2962), no security claimed

Physical Ports and Logical Interfaces

A single physical universal serial bus port (USB 3.0) is exposed on the top of the module that supports all logical interfaces (data input, data output, control input, status output, power). A light emitting diode (LED) is located inside the bottom metal enclosure for status output. A Write Protect Switch is used as a control input. The cryptographic module does not contain a maintenance interface. The following table summarizes the physical ports and logical interfaces:

Physical Port	Logical Interface
USB 3.0 port	Data Output, Data Input, Control Input, Status Output, Power
LED	Status Output
Write Protect Switch	Control Input

Exhibit 2 – *Specification of Cryptographic Module Physical Ports and Logical Interfaces*

Security rules

The following specifies security rules under which the cryptographic module shall operate in accordance with FIPS 140-2:

- The cryptographic module does not support a non-FIPS mode of operation and only operates in an Approved mode of operation. The method used to indicate the Approved mode of operation is to query the module for its firmware version number with a software tool provided by vendor and then the operator compares this value with the version number listed in this security policy.
- The cryptographic module provides logical separation between all of the data input, control input, data output, status output interfaces. The module receives external power inputs through the defined power interface.
- The cryptographic module supports identity based authentication for all services that utilize CSPs and Approved security functions.
- The data output interface is inhibited during self-tests, zeroization, and when error states exist.
- When the cryptographic module is in an error state, it ceases to provide cryptographic services, inhibits all data outputs, and provides status of the error.
- The cryptographic module does not support multiple concurrent operators.
- When the cryptographic module is powered off and subsequently powered on, the results of previous authentications are not to be retained and the cryptographic module requires the operator to be re-authenticated in an identity based fashion.
- The cryptographic module protects CSPs from unauthorized disclosure, unauthorized modification, and unauthorized substitution.

- The cryptographic module protects public keys from unauthorized modification, and unauthorized substitution.
- The cryptographic module satisfies the FCC 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).
- The cryptographic module implements the following self-tests:

  Power-up self-tests

  - Firmware integrity test (256-bit SHA256 hash verification)
  - SHA-256 KAT
  - HMAC-SHA256 KAT
  - RSA 2048 signature verification KAT
  - AES-256 CBC Encrypt KAT
  - AES-256 CBC Decrypt KAT
  - SP 800-90A DRBG KAT
  - Critical functions:
    - RSA 2048 Encrypt KAT

  Conditional self-test

  - Continuous test on SP 800-90A DRBG
  - Continuous test on non-Approved NDRNG
  - Firmware load test (via RSA 2048 with SHA256 digital signature verification)
  - Critical functions: CSP integrity test (via SHA-256-bit CRC verification)
- Manual key entry is not supported and the cryptographic module does not implement manual key entry tests.
- The cryptographic module does not support bypass capability and does not implement bypass tests.
- The status indicator output by the module when power-on self-tests succeeds is the LED flashing at 3 Hz and output of an icon to host GPC.
- The status indicator output by the module when a power-on self-test fails is flashing on the status output LED in a continuous fashion at 16Hz.
- The status indicator output by the module when a conditional self-test fails is flashing on the status output LED in a continuous fashion at 16Hz.
- The status indicator output by the module upon entry into the error state is flashing on the status output LED in a continuous fashion at 16Hz.
- Split-knowledge processes are not supported.

- All maintenance related services (i.e. maintenance role, physical maintenance interface, logical maintenance interface) are not applicable.
- Plaintext CSP output is not supported.
- The module does not support plaintext password entry. Passwords are entered encrypted with AES.
- The cryptographic module does not contain dedicated physical ports for CSP input/output
- The power interfaces cannot be used to drive power to external targets.
- The continuous comparison self-tests related to twin implementations are not applicable.
- Upon authenticating into a particular role, it is not possible to switch into another role without re-authenticating.
- The cryptographic module does not provide the means to feedback authentication data.
- The finite state machine does not support the following states: maintenance, CSP output.
- The requirements of FIPS 140-2 Section 4.6 are not applicable; there exists no support for the execution of untrusted code. All code loaded from outside the cryptographic boundary is cryptographically authenticated via RSA digital signature verification via the firmware load test.
- The cryptographic module is not a radio and does not support any wireless interfaces or OTAR.
- The requirements of FIPS 140-2 Section 4.11 are not applicable; the cryptographic module was not designed to mitigate specific attacks beyond the scope of FIPS 140-2.
- All keys generated by SP 800-90A DRBG, the key generation method complies with SP 800-133 Section 7.1, The “Direct Generation” of Symmetric keys.
- The cryptographic module performs a 256-bit comparison to ensure XTS key_1 is not equal to key_2.

Identification and Authentication Policy

The following table defines the roles, type of authentication, and associated authenticated data types supported by the cryptographic module:

Role	Type of Authentication	Authentication Data
Cryptographic Officer/Master: responsible for initialization, physical security inspection, and administrative functions.	Identity-based	Password (8 to 136 bytes)
User: the end user of the product that utilizes the module under the direction of the Cryptographic Officer/Master.	Identity-based	Password (8 to 136 bytes)
CD Update Officer: the end user of the product that utilizes the module to update the CD partition of the module.	Identity-based	RSA Signature Verification (RSA 2048 bit)

Exhibit 3 - *Roles and Required Identification and Authentication (FIPS 140-2 Table C1)*

The following table defines the strength of the implemented identity-based authentication mechanism (password verification or RSA signature verifications) by discussing the probabilities associated with random attempts and multiple consecutive attempts within a one-minute period towards subverting the implemented authentication mechanisms:

Authentication Mechanism	**Strength of Mechanism: Random attempted breach**	**Strength of Mechanism: Multiple consecutive attempts in a one-minute period**
Password verification	Less than 1 / 191,123,891,562,500	Less than 60/ 191,123,891,562,500
RSA signature verification	Less than 1 / 2^112	Less than 60/ 2 ^112

Exhibit 4 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

The upper bound for the probability of correctly guessing the password at random is:
1 / (10*26*95*95*95*95*95*95), which equates to 1 / 191,123,891,562,500. This is less than 1 / 1,000,000.

The minimum length of a password is 8 characters, which can be seen in the format of 1 / (C0 * C1 * C2 * C3 * C4 * C5 * C6 * C7). The password characters include 95 possible samples, which come from a combination of “0 – 9”, “A – Z”, “a – z”, and symbols (e.g. ! # { $).
Furthermore, the module requires that passwords meet a specific composition:
-One character of number 0 - 9 (10 possible samples)
-One character of the upper case of Letter A - Z (26 possible samples)

The module allows 60 attempts in a one-minute period, which equates to the following:
60 / 10*26*95*95*95*95*95*95 which is less than 1 / 100,000.

Access Control Policy

Exhibit 5 provides a mapping of CSPs/Public Keys to their respective services.

CSP/Public Key	Type	Service(s)
Data Encryption/Decryption Key of Private Partition Generation: Generated via SP 800-90A HMAC-SHA-256 DRBG Entry: N/A Output: N/A Storage: For each key of XTS-AES-256, it is encrypted with Key Encryption Key via AES-256 Key Wrap (SP 800-38F KW-AE(P)) where the KEK is derived by Master Disk Password via SP 800-132 PBKDF2 HMAC-SHA-256, and persistently stored in the System Area in a proprietary scrambled form where the System Area is logically allocated in the eMMC during manufacturing (plaintext from FIPS perspective)	XTS-AES-256	Set User Disk Password of Partition, Set User Disk Password of Private Partition, Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition, Create User of Private Partition, Write Mass-Storage Data to Partition, Read Mass-Storage Data to Partition, Write Mass-Storage Data to Private Partition, Read Mass-Storage Data to Private Partition, Zeroize
Data Encryption/Decryption Key of CD Area Generation: Generated via SP 800-90A HMAC-SHA-256 DRBG Entry: N/A Output: N/A Storage: Persistently stored in the System Area in a proprietary scrambled form	XTS-AES-256	Read Mass-Storage Data from CD Partition, Zeroize

where the System Area is logically allocated in the eMMC during manufacturing (plaintext from FIPS perspective)		
User Disk Password Generation: N/A Entry: User enters the value into the GPC via keyboard; enters module via USB interface Output: N/A Storage: Hashed with SHA-256 and then persistently stored in the System Area in a proprietary scrambled form where the System Area is logically allocated in the eMMC during manufacturing	8-byte to 136-byte password	Set User Disk Password of Partition, Set User Disk Password of Private Partition, User Login Into Partition, Change Disk Password of Partition, Change Disk Password of Private Partition, Create User of Partition, Create User of Private Partition, Zeroize
Master Disk Password Generation: N/A Entry: Master enters the value into the GPC via keyboard; enters module via USB interface Output: N/A Storage: Hashed with SHA-256 and then persistently stored in the System Area in a proprietary scrambled form where the System Area is logically allocated in the eMMC during manufacturing	8-byte to 136-byte password	Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, Master Login Into Private Partition, Change Disk Password of Partition, Change Disk Password of Private Partition, Create User of Partition, Create User of Private Partition, Zeroize
Key Encryption/Decryption Key of Private Partition Generation: Derived by Master Disk Password (or) User Disk	AES-256 Key Wrap * This key is used to wrap/unwrap the Data	Set User Disk Password of Partition, Set User Disk Password of Private Partition,

Password respectively via SP 800-132 PBKDF2 HMAC_SHA-256 Entry: N/A Output: N/A Storage: Data RAM	Encryption/Decryption Key of Private Partition and the Data Encryption/Decryption Key of CD Area; these keys are "never" output from the cryptographic module.	Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition, Create User of Private Partition, Zeroize
Seed Material of SP 800-90A HMAC-SHA-256 DRBG Generation: H/W NDRNG Entry: N/A Output: N/A Storage: Data RAM	Seed Material	Set User Disk Password of Partition, Set User Disk Password of Private Partition, Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition, Create User of Private Partition, Zeroize
DRBG Internal State (V and Key) Generation: Updated via SP 800-90A HMAC-SHA-256 DRBG Entry: N/A Output: N/A Storage: Data RAM	SP 800-90A	Set User Disk Password of Partition, Set User Disk Password of Private Partition, Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition, Create User of Private Partition, Zeroize
AES Session Key and IV Generation: Generated via SP 800-90A HMAC-SHA-256 DRBG Entry: N/A Output: RSA Wrapped via Secure Session Public Key	AES-256 CBC	Set User Disk Password of Partition, Set User Disk Password of Private Partition, Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition,

Storage: Data RAM		Logout From Partition, Logout From Private Partition, Change Disk Password of Partition, Change Disk Password of Private Partition, Create User of Partition, Create User of Private Partition, Write Mass-Storage Data to Partition, Read Mass-Storage Data to Partition, Write Mass-Storage Data to Private Partition, Read Mass-Storage Data to Private Partition, Zeroize
MAC Key of Secure Channel Generation: Generated via SP 800-90A HMAC-SHA-256 Entry: N/A Output: RSA Wrapped via Secure Session Public Key Storage: Data RAM	HMAC-SHA-256	Set User Disk Password of Partition, Set User Disk Password of Private Partition, Set Master Disk Password of Partition, Set Master Disk Password of Private Partition, Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition, Logout From Partition, Logout From Private Partition, Change Disk Password of Partition, Change Disk Password of Private Partition, Create User of Partition, Create User of Private Partition, Write Mass-Storage Data to Partition, Read Mass-Storage Data to Partition, Write Mass-Storage Data to Private Partition, Read Mass-Storage Data to Private Partition, Zeroize
Secure Session Public Key Generation: N/A	RSA-2048 OAEP	Master Login Into Partition, User Login Into Partition, Master Login Into Private Partition

Entry: Enters module via USB interface via Master Login Into Partition service, User Login Into Partition service, and Master Login Into Private Partition service Output: N/A Storage: Hashed with SHA-256 and then persistently stored in the System Area in a proprietary scrambled form where the System Area is logically allocated in the eMMC during manufacturing		
CD Update Public Key Generation: N/A Entry: Via Set CD Update Public Key service Output: N/A Storage: Hashed with SHA-256 and then persistently stored in the System Area in a proprietary scrambled form where the System Area is logically allocated in the eMMC during manufacturing	RSA-2048 SHA-256	CD Update, Set CD Update Public Key
Firmware Update Public Key Generation: N/A Entry: Via Start Firmware Update service Output: N/A Storage: Stored in the Firmware Area along with Firmware Code and RSA-	RSA-2048 SHA-256	Start Firmware Update

2048/SHA-256 signature where the Firmware Area is logically allocated in the eMMC during manufacturing		

Exhibit 5 – *CSPs/Public Keys with respective services*

The list of roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services are demonstrated in Exhibit 6.

Role				Service	Type(s) of Access to Cryptographic Keys & CSPs:
*No role	Crypto-graphic Officer/ Master	User	CD Update Officer		R = Read the item into memory W = Write the item into memory N/A = Not Applicable
X				**Self Tests**: Performs the full suite of required power-up self-tests.	N/A
X				**Get Device Info:** This function gets status information from the module.	N/A
X				**Set Write Protect**: This function enables or disables the module with write-protection.	N/A
	X			**Set User Disk Password of Partition**: This function sets the User Disk Password for Partition to the module to restrict access to the encrypted partition of the module. **Set User Disk Password of Partition**: (continued…)	W: User Disk Password W: Data Encryption/ Decryption Key of Private Partition W, R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV

	X			**Set User Disk Password of Private Partition**: This function sets the User Disk Password for Private Partition to the module to restrict access to the encrypted (private) partition of the module.	W: User Disk Password W: Data Encryption/ Decryption Key of Private Partition W, R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV
	X			**Set Master Disk Password of Partition**: This function sets the Master Disk Password for Partition to the module to restrict access to the encrypted partition of the module.	W: Master Disk Password W: Data Encryption/ Decryption Key of Private Partition W, R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV
	X			**Set Master Disk Password of Private Partition**: This function sets the Master Disk Password for Private Partition to the module to restrict access to the encrypted (private) partition of the module. **Set Master Disk Password of Private Partition**: (continued…)	W: Master Disk Password W: Data Encryption/ Decryption Key of Private Partition W, R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure

					Channel R: AES Session Key and IV
	X			**Master Login Into Partition**: This function opens (enables access to) the encrypted partition of module with Master Disk Password.	R: Master Disk Password W: Data Encryption/ Decryption Key of Private Partition R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV W, R: Secure Session Public Key
		X		**User Login Into Partition**: This function opens (enables access to) the encrypted partition of module with User Disk Password. **User Login Into Partition**: (Continued…)	R: User Disk Password R: Data Encryption/ Decryption Key of Private Partition R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV W, R: Secure Session Public Key
	X			**Master Login Into Private Partition**: This function opens (enables access to) the encrypted (private) partition of	R: Master Disk Password R: Data Encryption/

				module with Master Disk Password.	Decryption Key of Private Partition W: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG R: MAC Key of Secure Channel R: AES Session Key and IV W, R: Secure Session Public Key
	X	X		**Logout From Partition**: This function closes (disables access to) the encrypted partition of module.	R: MAC Key of Secure Channel R: AES Session Key and IV
	X	X		**Logout From Private Partition**: This function closes (disables access to) the encrypted (private) partition of module.	R: MAC Key of Secure Channel R: AES Session Key and IV
	X	X		**Change Disk Password of Partition**: This function changes the Master Disk Password (or) User Disk Password of partition from old password to new password.	R: MAC Key of Secure Channel R: AES Session Key and IV W, R: Master Disk Password (or) User Disk Password
	X	X		**Change Disk Password of Private Partition**: This function changes the Master Disk Password (or) User Disk Password of Private partition from old password to new password.	R: MAC Key of Secure Channel R: AES Session Key and IV W, R: Master Disk Password (or) User Disk Password
	X			**Create User of Partition**: This function creates the User and associated passwords for accessing the partition. **Create User of Partition**: (Continued…)	R: Master Disk Password R: AES Session Key and IV R: MAC Key of Secure Channel W: User Disk Password

	X			**Create User of Private Partition**: This function creates the User and associated passwords for accessing the Private partition.	R: Master Disk Password R: MAC Key of Secure Channel R: AES Session Key and IV W: User Disk Password W: Data Encryption/ Decryption Key of Private Partition W: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (V and Key), Seed Material of SP 800-90A HMAC-SHA-256 DRBG
	X	X		**Write Mass-Storage Data to Partition** This function writes data to the (encrypted) partition.	R: MAC Key of Secure Channel R: AES Session Key and IV R: Data Encryption/ Decryption Key of Private Partition
	X	X		**Read Mass-Storage Data to Partition:** This function reads data from the (encrypted) partition.	R: MAC Key of Secure Channel R: AES Session Key and IV R: Data Encryption/ Decryption Key of Private Partition
	X	X		**Write Mass-Storage Data to Private Partition:** This function writes data to the private (encrypted) partition.	R: MAC Key of Secure Channel R: AES Session Key and IV R: Data Encryption/ Decryption Key of Private Partition
	X	X		**Read Mass-Storage Data to Private Partition:** This function reads data from the private (encrypted) partition. **Read Mass-Storage Data to Private Partition:** (Continued…)	R: MAC Key of Secure Channel R: AES Session Key and IV R: Data Encryption/ Decryption Key of Private Partition

X				**Read Mass-Storage Data from CD Partition:** This function reads data from the public CD partition.	R: Data Encryption/ Decryption Key of CD Area
X				**Show Status**: This function gets the status from specified partition.	N/A
			X	**CD Update**: This function enables writing of data to the CD partition.	R: CD Update Public Key
			X	**Set CD Update Public Key**: This function updates the 2048-bit RSA public key used to verify the signature of the data written to CD partition.	W, R: CD Update Public Key
	X			**Start Firmware Update**: This function enables the secure firmware update via RSA 2048 with SHA-256 digital signature verification (limited operational environment firmware load test).	W, R: Firmware Update Public Key
X				**Zeroize**: This function zeroizes all the CSPs, and puts module into un-initialized state.	W: All CSPs

Exhibit 6 – *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4)* * No role means that the associated services in the Exhibit 6 are non-security relevant, unauthenticated, and can be accessed by any operator.

Physical Security Policy

The following physical security mechanisms are implemented by the cryptographic module:

- Production grade components.
- Opaque tamper evident metal and plastic enclosure without any gaps or openings.
- Strong adhesive materials that prevent dismantling the module without high probability of causing severe damage and visible tamper evidence.
- Chips and pin connectors are coated with epoxy.

NOTICE: The FIPS 140-2 Area 5 physical security testing was performed at ambient temperature; Kanguru Solutions does not claim any FIPS 140-2 Area 5 physical security protection beyond the ambient temperature.

The following table summarizes the actions required by the Cryptographic Officer/Master Role to ensure that physical security is maintained.

Physical Security Mechanisms	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
Production grade components	N/A	N/A
Opaque non-removable metal enclosure with strong adhesive materials	Upon each usage	Inspect the entire perimeter for scratches, scrapes, gouges, cuts and any other signs of tampering. Remove the unit from service when any such markings are found.

Exhibit 7 - *Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)*

Mitigation of Other Attacks Policy

The cryptographic module has not been including the security mechanisms implemented to mitigate the attacks.

Other Attacks	**Mitigation Mechanism**	**Specific Limitations**
N/A	N/A	N/A

Exhibit 8 - *Mitigation of Other Attacks (FIPS 140-2 Table C6)*

References

- **FIPS PUB 140-2**
- **FIPS PUB 140-2 DTR**
- **FIPS PUB 140-2 Implementation Guidance**
- **FIPS 197 – AES**
- **FIPS 198 - HMAC**
- **FIPS 180-4 - SHS**
- **RSA PKCS#1 V2.1**
- **SP 800-90A Rev.1**
- **SP 800-132**
- **SP 800-38E**
- **SP 800-133**

Appendix 1 – Part Number Matrix

(Kanguru Defender Elite300: Hardware Version 1.0; Firmware Version: 2.10.10 [1] and 2.11.10 [2])

Storage Capacity	Part Number
8GB	KDFE300-8G-Green [1, 2]
8GB	KDFE300-8G-Black [1, 2]
8GB	KDFE300-8G-Red [1, 2]
8GB	KDFE300-8G-Silver [1, 2]
16GB	KDFE300-16G-Green [1, 2]
16GB	KDFE300-16G-Black [1, 2]
16GB	KDFE300-16G-Red [1, 2]
16GB	KDFE300-16G-Silver [1, 2]
32GB	KDFE300-32G-Green [1, 2]
32GB	KDFE300-32G-Black [1, 2]
32GB	KDFE300-32G-Red [1, 2]
32GB	KDFE300-32G-Silver [1, 2]
64GB	KDFE300-64G-Green [1, 2]
64GB	KDFE300-64G-Black [1, 2]
64GB	KDFE300-64G-Red [1, 2]
64GB	KDFE300-64G-Silver [1, 2]
128GB	KDFE300-128G-Green [1, 2]
128GB	KDFE300-128G-Black [1, 2]
128GB	KDFE300-128G-Red [1, 2]
128GB	KDFE300-128G-Silver [1, 2]
256GB	KDFE300-256G-Green [2]
256GB	KDFE300-256G-Black [2]
256GB	KDFE300-256G-Red [2]

Exhibit 9 – *Module Part Numbers*