Defender 2000 Cryptographic Module

FIPS 140-2 Security Policy
Document Revision: 1.2
H.W. Version: 1.0
F.W. Version: 2.02.10

Revision History

Author(s)	Version	Updates
Nate Cote, Kanguru Solutions	1.2	Initial public release.

Introduction

The Kanguru Defender 2000, herein after referred to as "cryptographic module" or "module", (HW Version: 1.0; FW Version: 2.02.10) 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, 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 Elite has been specifically designed to address sensitive data concerns of Government and security conscious customers in a variety of markets.

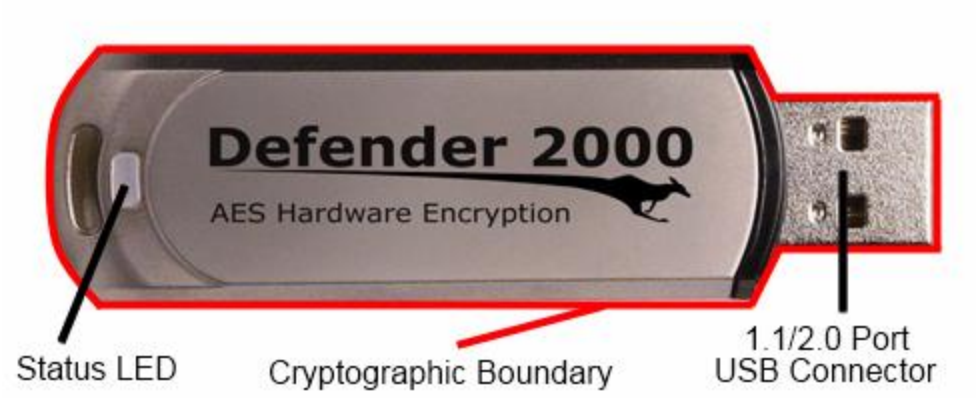
Cryptographic Boundary

The physically contiguous cryptographic boundary is defined by the outer perimeter of the metal enclosure. The cryptographic module does not contain any removable covers, doors, or openings. The cryptographic module is available in a variety of Approved configurations:

Kanguru Defender 2000

Capacity	2GB	4GB	8GB
Module Part Number	KDF2000-2G	KDF2000-4G	KDF2000-8G

The following photographs define the cryptographic boundary:



Kanguru Defender Elite – Models: KDF2000-xG
x = 2,4,8

Exhibit 1– *Specification of Cryptographic Boundary*

Exhibit 2– *Specification of Cryptographic Boundary*

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 3 – *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 (Cert. #1623)
- SHA-256 (Cert. #1432)
- HMAC-SHA256 (Cert. #954)
- RSASSA-PKCS1_V1_5 with 2048 bit key and SHA-256 Signature Verification (Cert. #801)
- SP800-90 DRBG HMAC_DRBG with HMAC-SHA256 core (Cert. #86)
- PBKDF (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. #1623); the PBKDF "salt" is generated by NIST SP800-90 HMAC_DRBG and its length is 32 bytes; see password strength in "Identification and Authentication Policy" section below; The keys derived in accordance with SP800-32 are used in storage applications only).

Allowed algorithms

The cryptographic module supports the following Allowed algorithms:

- **RSA 2048 Key Transport (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)

Physical Ports and Logical Interfaces

A single physical universal serial bus port (USB 1.1/2.0) 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. The cryptographic module does not contain a maintenance interface. The following table summarizes the physical ports and logical interfaces:

Physical Port	**Logical Interface**
USB 1.1/2.0 port	Data Output, Data Input, Control Input, Status Output, Power
LED	Status Output

Exhibit 4 – *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 ("Get Device Info"), 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 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
  - RSA2048 signature verification KAT
  - AES-256 CBC Encrypt/Decrypt KAT
  - SP800-90 DRBG KAT
  - Continuous test on non-Approved NDRNG
  - Critical functions:
    - RSA2048 Encrypt KAT

  Conditional self-test

  - Continuous test on SP800-90 DRBG
  - Continuous test on non-Approved NDRNG
  - Firmware load test (via RSA2048 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 3.125 Hz, and outputs an icon to host PC.

- 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, 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.

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
Master/ Cryptographic Officer: responsible for initialization, physical	Identity-based	Password (8 to 136 bytes)

security inspection, and administrative functions.		
User: the end user of the product that utilizes the module under the direction of the 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 5 - *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 / 256^8	Less than 60/ 256 ^8
RSA signature verification	Less than 1 / 2^112	Less than 60/ 2 ^112

Exhibit 6 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

Access Control Policy

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.

Exhibit 7 – *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 7 below are non-security relevant, unauthenticated, and can be accessed by any operator.

Role				Service	Type(s) of Access to CSPs: 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
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.	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 (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel
	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 (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel

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 (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel
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.	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 (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel
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 (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel

	X	**User Login Into Partition**: This function opens (enables access to) the encrypted partition of module with User Disk Password.	R: User Disk Password R: Data Encryption/ Decryption Key of Private Partition R: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel
X		**Master Login Into Private Partition**: This function opens (enables access to) the encrypted (private) partition of module with Master Disk Password.	R: Master Disk Password R: Data Encryption/ Decryption Key of Private Partition W: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (K and V) R: MAC Key of Secure Channel R: AES Session Key of Secure Channel
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 of Secure Channel
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 of Secure Channel
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 of Secure Channel R/W: 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 of Secure Channel R/W: Master Disk Password (or) User Disk Password
X		**Create User of Partition**: This function creates the User and associated passwords for accessing the partition.	R: Master Disk Password, R: AES Session Key of Secure Channel, 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 of Secure Channel W: User Disk Password W: Data Encryption/ Decryption Key of Private Partition W: Key Encryption/ Decryption Key of Private Partition W: DRBG Internal State (K and V)
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 of Secure Channel 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 of Secure Channel 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 of Secure Channel 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.	R: MAC Key of Secure Channel R: AES Session Key of Secure Channel 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/Public Partition
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.	R, W: 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).	R,W: Firmware Update Public Key
X				**Zeroize**: This function zeroizes all the CSPs, and puts module into un-initialized state.	W: All CSPs

Exhibit 7 – *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4) Cont'd*

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.

The following table summarizes the actions required by the Master/Cryptographic Officer 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 8 - *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 9 - *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 180-3 - SHS**
- **RSA PKCS#1 V2.1**

- **SP800-90**

Appendix 1 – Part Number Matrix
(Kanguru Defender 2000: Hardware Version 1.0; Firmware version: 2.02.10)

Capacity	2GB	4GB	8GB
Module Part Number	KDF2000-2G	KDF2000-4G	KDF2000-8G

Exhibit 10 – *Module Part Numbers*