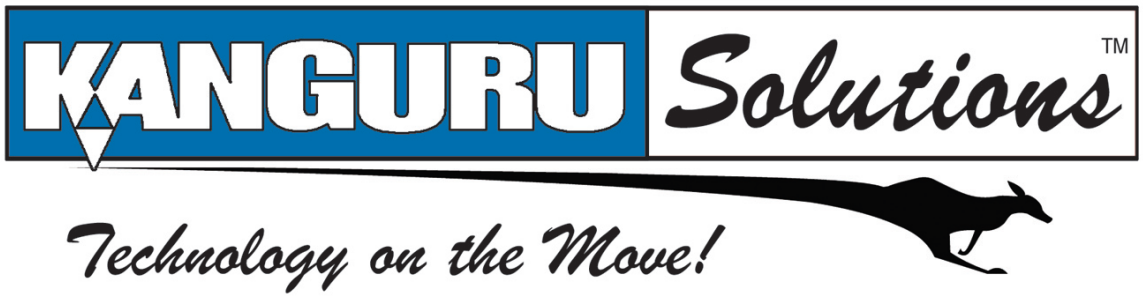


Defender Elite/Elite+ Cryptographic Module

FIPS 140-2 Security Policy
Document Revision: 1.2
H.W. Version: (Referenced in Appendix 1)
F.W. Version: (Referenced in Appendix 1)

Revision History

Author(s)	Version	Updates
Nate Cote, Kanguru Solutions	1.0	Initial public release.
Nate Cote, Kanguru Solutions	1.1	Updated dates & capacities
Nate Cote, Kanguru Solutions	1.2	Added firmware versions and Elite+ models

Introduction

The Kanguru Defender Elite/Elite+, herein after referred to as "cryptographic module" or "module", (HW Version: See Appendix 1 below; FW Version: See Appendix 1 below) 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. The Kanguru Defender Elite and Kanguru Defender Elite+ use the same cryptographic components, and the only difference is that the Kanguru Defender Elite uses MLC FLASH while the Kanguru Defender Elite+ uses SLC FLASH.

Files distributed with the module mounted within the CD Drive, Public Drive, and/or Private Drive are excluded from the validation.

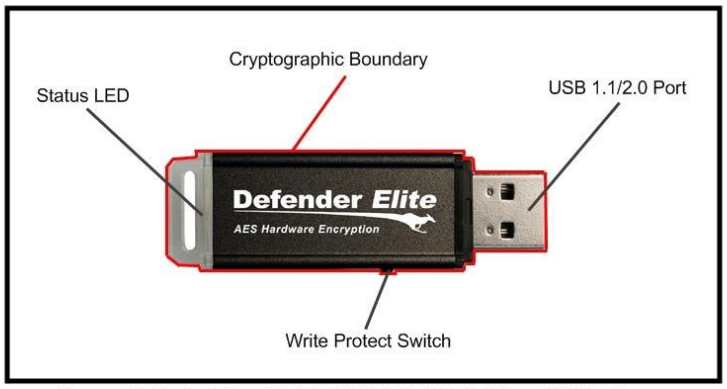
The Kanguru Defender Elite/Elite+ has been specifically designed to address sensitive data concerns of Government and security conscious customers in a variety of markets.

Cryptographic Boundary

The physically contiguous cryptographic boundary is defined by the outer perimeter of the metal and plastic enclosure with a plastic cap on the bottom. 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 below for complete list of approved capacities and colors

The following photographs define the cryptographic boundary:



Kanguru Defender Elite - Models: KDFE-*x*G, KDFE-1Ga-*y*, KDFE-*x*G-*y*

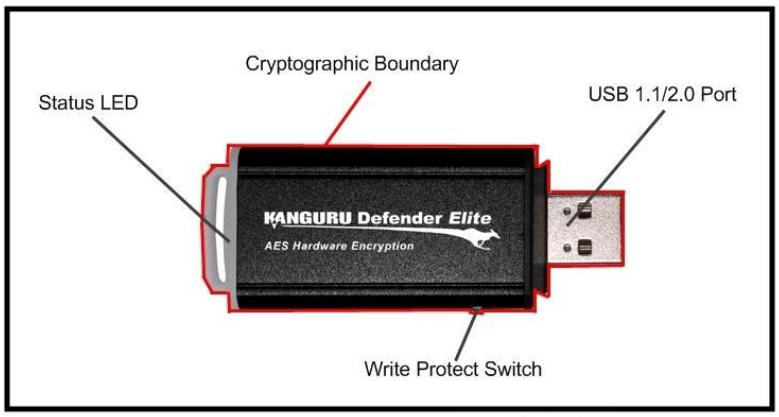
x = 1a, 2, 4, 8, 16

y = Red, Green, Blue, Yellow Tan, Gray, Silver

Exhibit 1.1 – *Specification of Cryptographic Boundary*

Small enclosure with either 1GB, 2GB, 4GB, 8GB, or 16GB capacity.

(Please note: Standard model is Black and does not have a color suffix at the end of the part number)



Kanguru Defender Elite - Models: KDFE-*x*G-L, KDFE-xG-y-L

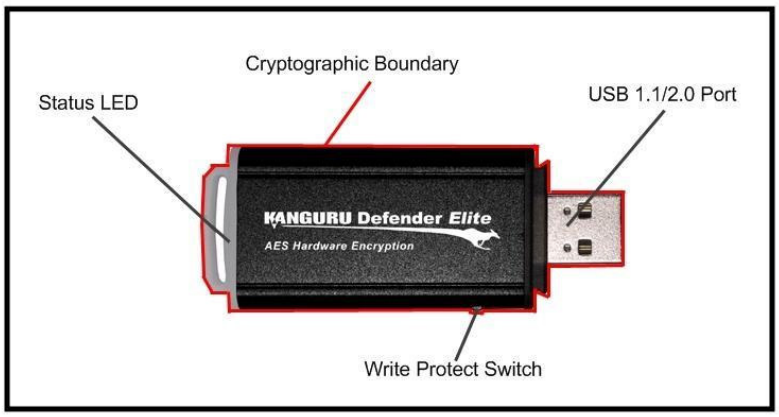
x = 4, 8, 16

y = Red, Green, Blue, Yellow,Tan, Gray, Silver

Exhibit 1.2 – *Specification of Cryptographic Boundary*

Large enclosure with either 4GB, 8GB, or 16GB capacity.

(Please note: Standard model is Black and does not have a color suffix at the end of the part number)



Kanguru Defender Elite - Models: KDFE-*x*G, KDFE-*x*G-*y*

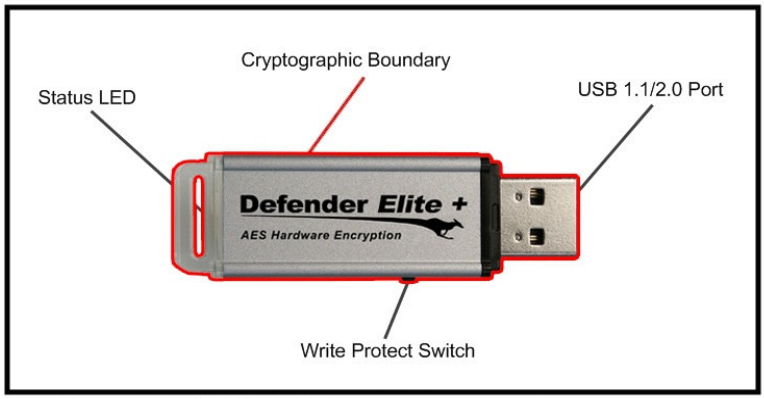
x = 32, 64, 128

y = Red, Green, Blue, Yellow,Tan, Gray, Silver

Exhibit 1.3 – *Specification of Cryptographic Boundary*

Large enclosure with either 32GB, 64GB, or 128GB capacity.

(Please note: Standard model is Black and does not have a color suffix at the end of the part number)



Kanguru Defender Elite+ Models: KDFEP-xG, KDFEP-xG-y

x = 1, 2, 4, 8

y = Red, Green, Blue, Yellow, Black, Tan

Exhibit 1.4 – *Specification of Cryptographic Boundary*
Small enclosure with either 1GB, 2GB, 4GB, or 8GB capacity.
(Please note: Standard model is gray and does not have a color suffix at the end of the part number)

Exhibit 2 - *Specific supported colors of enclosures*

Color	Pantone
Black	Black C
Gray	424C
Silver	428C
Red	187C
Green	3435C
Blue	286C
Tan	464C
Yellow	102C

Security Level Specification

Exhibit 3 – *Security Level Table*

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

Approved algorithms

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

- AES with 256-bit key in CBC mode Encrypt/Decrypt (Cert# 1066)
- SHA-1 (Cert#1009)
- SHA-256 (Cert# 1009)
- RSASSA-PKCS1_V1_5 with 1024 bit key and SHA-1 (Cert# 506)
- ANSI X9.31 DRNG with AES 256-bit core (Cert# 603)

Non-Approved algorithms

The cryptographic module supports the following non-Approved algorithms:

- Hardware non-deterministic random number generator (for seeding Approved DRNG)
- RSA-512 (non-compliant; used in the KDE Channel service and provides no confidentiality, integrity, and does not satisfy any security objective; this is not relied upon to modify any critical settings that would compromise the module and is considered as plaintext from FIPS 140-2 perspective).

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 write-protect switch (mechanical switch) is located on the side as a control input to lock and unlock the device. A light emitting diode (LED) is located inside the bottom plastic cap 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 Input
USB 1.1/2.0 port	Data Output
• USB 1.1/2.0 port • Write-protect switch	Control Input
• USB 1.1/2.0 port • LED	Status Output
USB 1.1/2.0 port	Power

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

  - AES CBC Encrypt/Decrypt KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - RSA signature verification KAT
  - ANSI X9.31 DRNG KAT
  - Firmware integrity test (16-bit checksum verification)

  Conditional self-test

  - Continuous test on ANSI X9.31 DRNG
  - Continuous test on non-Approved NDRNG
  - Firmware load test (via RSA digital signature verification)
  - Critical functions: CSP integrity test (via 16-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 module ensures that the seed and seed key are not equal by performing a comparison.

- 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 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 supports plaintext password entry.
- 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: responsible for initialization, physical security inspection, and administrative functions.	Identity-based	Password (Sixteen character)

User: the end user of the product that utilizes the module under the direction of the Master.	Identity-based	Password (Sixteen character)
Cryptographic Officer: responsible for performing secure firmware updates.	Identity-based	RSASSA-PKCS1_V1_5 with 1024 bit key and SHA-1 digital signature verification

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) and identity based authentication mechanism (RSA digital signature verification) 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 / 94^16	Less than 60/ 94 ^16
RSASSA-PKCS1_V1_5 with 1024 bit key and SHA-1 digital signature verification	Less than 1/ 2^80	Less than 8.8/ 2^80

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	Cryptographic Keys & CSPs	Type(s) of Access to CSPs
*No role	Crypto-graphic Officer	Master	User			
X				**SelfTests**: performs the full suite of required power-up self-tests.	N/A	N/A
X				**InitAPI**: This function initializes the API.	N/A	N/A
X				**CloseAPI**: This function shuts down the API and frees the memory.	N/A	N/A
X				**KDEChannel:** This function enables communication I/O with external PC (to facilitate read/write between external PC and the cryptographic module for CDROM content and configuration data; this service uses non-compliant RSA-512 and provides no confidentiality, integrity, and does not satisfy any security objective; this service is not relied upon to modify any critical settings that would compromise the module; this service is considered as plaintext from FIPS 140-2 perspective).	N/A	N/A
X				**ListTokens:** This function gets the drive letters of external devices from PC and switches the external devices to HID mode.	N/A	N/A
X				**GetDeviceInfo:** This function gets status information from the module.	N/A	N/A
X				**SetWriteProtect**: This function enables or disables the module with write-protection.	N/A	N/A
X				**GetWriteProtect**: This function gets the status whether the device has been write-protected or not.	N/A	N/A

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

		X	X	**SetPassword**: This function sets the Master Password and User Password to the module to restrict access to the encrypted (private) area of the module.	Master Password of Private Area User Password of Private Area Data Encryption/ Decryption Key of Private Area	Enter, Store Enter, Store Generate, Store
		X		**MasterLogin**: This function opens (enables access to) the encrypted (private) area of module with Master Password.	Master Password of Private Area Data Encryption/ Decryption Key of Private Area	Enter, Verify Execute
			X	**UserLogin**: This function opens (enables access to) the encrypted (private) area of module with User Password.	User Password of Private Area Data Encryption/ Decryption Key of Private Area	Enter, Verify Execute
		X	X	**Logout**: This function closes (disables access to) the encrypted (private) area of module that this area cannot be accessed.	N/A	N/A
		X		**ChangeMasterPassword**: This function changes the Master Password from old password to new password.	Master Password of Private Area	Enter, Verify, Update
			X	**ChangeUserPassword**: This function changes the User Password from old password to new password.	User Password of Private Area	Enter, Verify, Update
X				**Zeroization_And_Reinitialization**: This function sets new Master Password and User Password to the private (encrypted) area forcibly overwriting/zeroizing all CSPs and keys.	Master Password of Private Area User Password of Private Area Data Encryption/ Decryption Key of Private Area ANSI X9.31 DRNG K, DT, V, R	Zeroize,Enter, Update Zeroize, Enter, Update Zeroize, Generate, Update Zeroize, Generate, Update

		X		**ReAssignNewUserPassword**: This function re-assigns new User Password after the Master Password has been verified successfully.	Master Password of Private Area User Password of Private Area	Enter, Verify Enter, Update
X				**ShowStatus**: This function gets the status from specified partition.	Firmware Update Public Key	Output
X				**OpenSDK**: This function enables communication with software running on the external PC.	N/A	N/A
X				**CloseSDK**: This function disables communication with the software running on the external PC.	N/A	N/A
X				**OpenPublicArea:** This function enables access to the public partition, to read and write non-security relevant items.	N/A	N/A
X				**Close PublicArea:** This function disables access to the public partition.	N/A	N/A
X				**Destructive_Zeroization**: This function zeroizes all the CSPs, and puts module into a permanent unrecoverable error state. This function is not available in the mainstream unit, but can be made available if required as an option.	Data Encryption/ Decryption Key of Private Area Master Password of Private Area User Password of Private Area ANSI X9.31 DRNG K, DT, V, R	Zeroize Zeroize Zeroize Zeroize
	X			**StartFirmwareUpdate**: This function enables the secure firmware update via RSA 1024 with SHA-1 digital signature verification (limited operational environment firmware load test).	Firmware Update Public Key	Execute

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 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 metal and plastic 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**
- **ANSI X9.31 – DRNG**

Appendix 1 – Part Number Matrix
(Kanguru Defender Elite: Hardware Version 1.0; Firmware versions: 1.0, 2.01.10 or 2.01.15)

			Capacity					
Product/Color	1GBa	2GB	4GB	8GB	16GB	32GB	64GB	128GB
Kanguru Defender Elite - Black	KDFE-1Ga	KDFE-2G	KDFE-4G	KDFE-8G	KDFE-16G	KDFE-32G	KDFE-64G	KDFE-128G
Kanguru Defender Elite - Red	KDFE-1Ga-Red	KDFE-2G-Red	KDFE-4G-Red	KDFE-8G-Red	KDFE-16G-Red	KDFE-32G-Red	KDFE-64G-Red	KDFE-128G-Red
Kanguru Defender Elite - Green	KDFE-1Ga-Green	KDFE-2G-Green	KDFE-4G-Green	KDFE-8G-Green	KDFE-16G-Green	KDFE-32G-Green	KDFE-64G-Green	KDFE-128G-Green
Kanguru Defender Elite - Blue	KDFE-1Ga-Blue	KDFE-2G-Blue	KDFE-4G-Blue	KDFE-8G-Blue	KDFE-16G-Blue	KDFE-32G-Blue	KDFE-64G-Blue	KDFE-128G-Blue
Kanguru Defender Elite - Yellow	KDFE-1Ga-Yellow	KDFE-2G-Yellow	KDFE-4G-Yellow	KDFE-8G-Yellow	KDFE-16G-Yellow	KDFE-32G-Yellow	KDFE-64G-Yellow	KDFE-128G-Yellow
Kanguru Defender Elite - Tan	KDFE-1Ga-Tan	KDFE-2G-Tan	KDFE-4G-Tan	KDFE-8G-Tan	KDFE-16G-Tan	* N/A	* N/A	* N/A
Kanguru Defender Elite - Gray	KDFE-1Ga-Gray	KDFE-2G-Gray	KDFE-4G-Gray	KDFE-8G-Gray	KDFE-16G-Gray	* N/A	* N/A	* N/A
Kanguru Defender Elite - Silver	KDFE-1Ga-Silver	KDFE-2G-Silver	KDFE-4G-Silver	KDFE-8G-Silver	KDFE-16G-Silver	KDFE-32G-Silver	KDFE-64G-Silver	KDFE-128G-Silver

* N/A = Product/Color/Capacity is Not Applicable.

Additional Large Housing Capacities/Colors (Appendix 1, Cont'd)
(Kanguru Defender Elite: Hardware Version 1.0; Firmware versions: 1.0, 2.01.10 or 2.01.15)

		Capacity	
Product/Color	4GB	8GB	16GB
Kanguru Defender Elite - Black	KDFE-4G-L	KDFE-8G-L	KDFE-16G-L
Kanguru Defender Elite - Red	KDFE-4G-Red-L	KDFE-8G-Red-L	KDFE-16G-Red-L
Kanguru Defender Elite - Green	KDFE-4G-Green-L	KDFE-8G-Green-L	KDFE-16G-Green-L
Kanguru Defender Elite - Blue	KDFE-4G-Blue-L	KDFE-8G-Blue-L	KDFE-16G-Blue-L
Kanguru Defender Elite - Yellow	KDFE-4G-Yellow-L	KDFE-8G-Yellow-L	KDFE-16G-Yellow-L
Kanguru Defender Elite - Silver	KDFE-4G-Silver-L	KDFE-8G-Silver-L	KDFE-16G-Silver-L

Part number designation glossary for Kanguru Defender Elite (Appendix 1, Cont'd)

KDFE = Base part number
KDFE-xG: "x" is the capacity
KDFE-xG-y: "y" is the color of the enclosure (if different from the standard model black color)

Part Number Matrix (Appendix 1, Cont'd)
(Kanguru Defender Elite+: Hardware Version 1.0; Firmware versions: 2.01.10 or 2.01.15)

Kanguru Defender Elite+ -Gray	KDFEP-1G	KDFEP-2G	KDFEP-4G	KDFEP-8G
Kanguru Defender Elite+ - Red	KDFEP-1G-Red	KDFEP-2G-Red	KDFEP-4G-Red	KDFEP-8G-Red
Kanguru Defender Elite+ - Green	KDFEP-1G-Green	KDFEP-2G-Green	KDFEP-4G-Green	KDFEP-8G-Green
Kanguru Defender Elite+ - Blue	KDFEP-1G-Blue	KDFEP-2G-Blue	KDFEP-4G-Blue	KDFEP-8G-Blue
Kanguru Defender Elite+ - Yellow	KDFEP-1G-Yellow	KDFEP-2G-Yellow	KDFEP-4G-Yellow	KDFEP-8G-Yellow
Kanguru Defender Elite+ - Tan	KDFEP-1G-Tan	KDFEP-2G-Tan	KDFEP-4G-Tan	KDFEP-8G-Tan
Kanguru Defender Elite+ -Black	KDFEP-1G-Black	KDFEP-2G-Black	KDFEP-4G-Black	KDFEP-8G-Black

Part number designation glossary for Kanguru Defender Elite+ (Appendix 1, Cont'd)

KDFEP = Base part number
KDFEP-xG: "x" is the capacity
KDFEP-xG-y: "y" is the color of the enclosure (if different from the standard model gray color)