RDX SATA III FIPS 140-2 Cryptographic Module Non-Proprietary

Security Policy

Revision: B
December 2018

Table of Contents

List of Tables

List of Figures

References

Table 1: References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 19 January 2018
[SATA]	*SATA-IO Serial ATA Rev 3.0, June 2009*
[SCSI Block]	*SCSI Block Commands Rev15 (SBC-3)*
[SCSI Core]	*SCSI Primary Commands-4 Rev 33 (SPC-4)*
[SP 800-90A]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, December 2010*
[SSC]	*SCSI Stream Commands-3 Rev 22 (SSC-3)*
[ACS]	*INITCS 482-2012 ATA/ATAPI Command Set – 2 (ACS-2)*

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
ATA	Advanced Technology Attachment
CBL	Customer Build Level
CSP	Critical Security Parameter, see [FIPS 140-2]
HDD	Hard Disk Drive
KAT	Known Answer Test
LBA	Logical Block Address
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
PSP	Public Security Parameter
SATA	Serial ATA
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SID	Security Identifier
SSC	SCSI Stream Commands
SSD	Solid-state Drive

1 Overview

This document defines the Security Policy for the Tandberg Data RDX SATA III cryptographic module, hereafter denoted as *the Module*. The Module is a multiple chip embedded docking station compliant with SSC, SCSI, and SATA specifications.

The Module is intended to interact with a computer host and a storage cartridge that may be inserted or ejected from the Module; storage cartridges are not considered to be part of the cryptographic boundary.

The FIPS 140-2 security levels for the Module are as follows:

Table 3: Security Level of Security Requirements

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

1.1 Versions, Configurations, and Modes of Operation

There are two Approved Modes. Following successful completion of power-on self-tests, the Module automatically transitions into the Approved No Cartridge Accessible (NCA) Mode. If a cartridge is inserted in the Module at any point during operation, the Module automatically performs the necessary self-tests to transition into the Approved Cartridge Accessible (CA) Mode.

If the Module is not configured as specified in Section 9.3, it is then in a non-Approved Mode. When switching from the NCA Mode to the CA mode, non-Approved algorithms are used to validate the inserted cartridge and are considered to only be available during the Module initialization period as specified in IG 9.5.

Table 4: Module Configurations

	HW Part Number	FW Version	HW Version (CBL)	Description
1	8812-RDX	0253	3078-0006	RDX QuikStor Internal 3.5 SATA 3 SINGLE PACK Tandberg Data
2	8813-RDX	0253	3079-0006	RDX QuikStor Internal 5.25 SATA 3 SINGLE PACK Tandberg Data
3	8815-RDX	0253	3080-0006	RDX QuikStor Internal 5.25 SATA 3 10 PACK Tandberg Data
4	8816-RDX	0253	3081-0006	RDX QuikStor Internal 3.5 SATA 3 10 PACK Tandberg Data
5	8826	0253	3095-0003	RDX QuikStor Internal 5.25 SATA 3 SINGLE PACK Quantum
	1022445	N/A	N/A	Tamper-Evident Seals

1.2 Hardware and Physical Cryptographic Boundary

The Module is provided as a multi-chip embedded cartridge dock with several internal form factors, as listed in Table 4. The Module block diagram is depicted in Figure 1. In the figure, the red outline depicts the physical cryptographic boundary. The following components are non-security relevant and have been excluded from FIPS 140-2 requirements:

- LVDS clock generator
- Coil inductor
- FERRITE CHIP (x2)
- Resistor (x7)
- Jumper
- Test point (x23)
- Capacitor (x6)
- Diode (x2)
- FET
- HALL EFFECT SWITCH

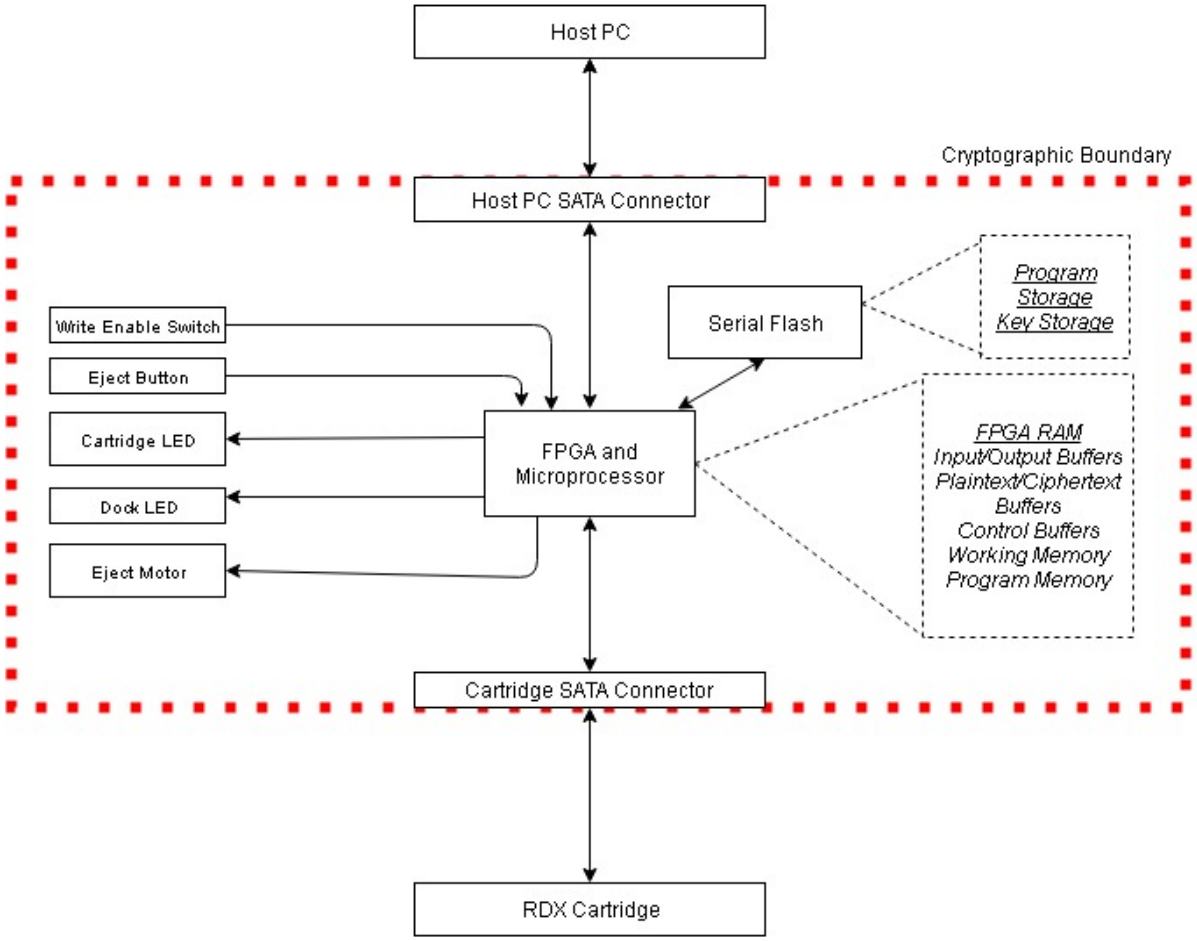

Figure 1: Block Diagram

The dock enclosure is the physical boundary as shown in Figure 2 (5.25-inch configuration) and Figure 3 (3.5-inch configuration). These figures represent the different hardware model configurations described by the Security Policy. Other model numbers differ only by silkscreen labeling and branding as well as whether they are bundled with other units in a shipment. I/O and Power ports are exposed as well as Control Inputs and Status Outputs.

Figure 2: Tandberg Data RDX SATA III 5.25 Inch Configuration

Figure 3: Tandberg Data RDX SATA III 3.5 Inch Configuration

The module only has one processor which is implemented within the Altera Arria II GX FPGA. Specifically, the Module boundary contains the soft-core Altera Nios Classic.

- The Module implements two SATA interfaces used for control, status and data I/O.
- The module stores keys and CSPs in internal flash and RAM.
- HW used to store data can vary and is specific to the cartridge inserted into the Module. Cartridges inserted into the Module are considered to be outside the cryptographic boundary.

Table 5: Ports and Interfaces

Port	Description	Logical Interface Type
Host SATA	Host SATA Connector	Control in, Data in, Data out, Status out
Cartridge SATA	HDD SATA Connector	Control in, Data in, Data out
SATA Power	Power Connector	Power
Eject Button	Cartridge eject button	Control Input
Emergency Eject	Emergency cartridge eject pinhole	Control Input
Write Enable	Write Enable Switch	Control Input
Dock LED	Error LED	Status Output
Cartridge LED	Light Pipe sent from the dock through the cartridge	Status Output

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below. Refer to Section 11 for a mapping of algorithms utilized in each Approved Mode.

Table 6: Approved Cryptographic Functions

Algorithm	Reference	Description	Cert #
AES	[FIPS 197, SP 800-38A]	Functions: Encryption, Decryption Mode: ECB Key Size: 256 bits	#4811
	[SP 800-38E]	Functions: Encryption, Decryption Mode: XTS Key Size: 256 bits * XTS-AES is only used for storage applications	#4813
CKG	[SP 800-133 Section 7.1]	Direct Symmetric Key generation using unmodified DRBG output	Vendor Affirmed IG D.12
DRBG	[SP 800-90A]	Function: Hash DRBG Security Strength: 256 bits	#1673
HMAC	[FIPS 198-1]	Functions: Generation, Verification SHA Size: SHA-256	#3216
PBKDF	[SP 800-132]	Option: Option 2a Function: HMAC-based KDF using SHA-256 *Keys derived from PBKDF are only used for storage applications	Vendor Affirmed IG D.6
RSA	[FIPS 186-4, PKCS #1 v2.1]	Function: Signature Verification Key Size: 2048 bits, SHA-256	#2635
SHA	[FIPS 180-4]	Functions: Digital Signature Verification, non-Digital Signature Applications SHA Size: SHA-256	#3955

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Reference	Description
NDRNG	[IG G.13]	Hardware True Random Number Generator; minimum of 32 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.

The non-Approved cryptographic algorithms listed below are used by the Module. These algorithms are used automatically during the initialization period when transitioning from the NCA to the CA Approved Mode:

- XTEA
- RSA 1024 signature verification; implemented for purposes other than legacy-use

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs and PSPs is described in the services detailed in Table 14. To identify the CSPs accessed in each approved Mode, refer to the services in Section 11 and compare to the CSP Accesses in Table 15.

Table 8: Critical Security Parameters

CSP	Description / Usage
TRNG-OUT	384-bit TRNG output used to derive DRBG-SEED. Provides 327.552 bits of entropy.
DRBG-NONCE	256-bit nonce used to derive DRBG-SEED. Provides 218.368 bits of entropy.
DRBG-SEED	440-bit entropy input used to derive the initial value of DRBG-STATE.
DRBG-STATE	Hash DRBG internal state consisting of a 440-bit value (V), a 440-bit constant (C) and an 8-bit reseed counter.
MK	512-bit XTS-AES/ HMAC Master Key used to wrap/unwrap and authenticate the DPK.
DPK	512-bit XTS-AES Data Protection Key used to encrypt/decrypt data stored on a cartridge.
PH	512-bit password hash[1] used to derive MK.
Dock PH	512-bit DRBG output used to derive MK. Dock PH is used in place of PH if the Module is configured for automatic decryption.

[1] The module does not ensure PH is a hash, but in practice it always will be.

2.2 Public Security Parameters

Table 9: Public Security Parameters

Key	Description / Usage
FW-SVK	2048-bit public component of an RSA key pair, used for signature verification by the FW download service.
MK-SALT	256-bit salt used to derive MK.
PH-SALT	256-bit password hash salt. Sent to the host as a public input parameter to derive PH.

3 Roles, Authentication, and Services

The module supports the User, Cryptographic Officer (CO), and FW load roles. A User or CO role is defined by the permissions assigned to a given key slot, and each role will have its own key slot and password. The cryptographic module enforces the separation of roles by enforcing re-authentication with the appropriate password hash or digital signature when changing roles.

Table 10 lists all operator roles supported by the module. The Module does not support concurrent operators, bypass, or a maintenance role. Authentication is cleared on each power cycle.

Table 10: Authenticated Roles

Role Name	Description / Corresponding Roles	Authentication Data	Authentication Type
CO	The cryptographic officer that initializes the Module on first-time use. This role exists to creates and delete key slots.	Password Hash	Role-based
User	The everyday user of the Module.	Password Hash	Role-based
FW Load	An operator loading FW into the Module.	Public Key, Digital Signature	Identity-based

3.1 Authentication

The module enforces password hash authentication for the User and CO roles, and signature verification for the FW Load role. The strength of authentication is described in Table 11.

Table 11: Authentication Description

Authentication Method	Description
Password Hash	Password Hashes are 512 bits, providing 2^{512} possible values. The probability that a random attempt succeeds is $1/2^{512}$. Password Hash verification takes at least one (1) second per attempt. Therefore, the probability that a false acceptance occurs over a one-minute interval is at most $60/2^{512}$.
Signature Verification	RSA-2048 w/ SHA-256 PKCS #1 v2.1 signature verification is used to authenticate an operator loading FW to the Module. The probability that a random attempt succeeds is $1/2^{2048}$. Signature verification takes more than 300ms per attempt, not counting overhead in SCSI packets. Therefore, the probability that a false acceptance occurs over a one-minute interval is at most $200/2^{2048}$.

3.2 Services

All services implemented by the Module in the Approved Mode are listed in Table 12 and Table 13. CSP usage for each Approved Mode service described is specified in Table 15. Refer to Section 11 for a mapping of services utilized in each Approved Mode.

Table 12: Unauthenticated Services

Service	Description
Initialize First Key Slot	CO initialization procedures to setup User and CO authentication credentials on a cartridge inserted into the Module. The Authenticate service is called as part of establishing authentication credentials.
Zeroize	SECURITY PROTOCOL OUT SCSI command used to write zeroes to the Dock PH stored in flash. All other keys/CSPs are stored only in RAM and can be cleared by power cycling the Module.
Authenticate	An operator attempts to authenticate to the Module as either a CO or User role. Authenticating a role locks the encryption key to the key slot being authenticated.
Show Status	LOG SENSE SCSI command used to send status messages, as well as the dock LED (FIPS errors) and light pipe (generic errors) output.
Read Encrypted Data	The module may send encrypted data from the cartridge to the host on request. This service is only useful if the host has the password hash necessary to derive the DPK.
Read Data (unauthenticated)	Decrypt and read encrypted data stored on a cartridge inserted into the Module. This service does not create, disclose or modify CSPs and is only available if the CO allows it via the Configure Automatic Decryption service.
Write Data (unauthenticated)	Write and encrypt data onto a cartridge inserted into the Module. This service does not create, disclose or modify CSPs and is only available if the CO allows it via the Configure Automatic Decryption service.
Self-Tests	SEND DIAGNOSTIC SCSI command used for an operator to perform all algorithm self-tests on demand. All power-on self-tests, including the FW integrity test can be performed on demand by power cycling the Module.
Provide Authentication Parameters	SECURITY PROTOCOL IN SCSI command used to send MK-SALT, PH-SALT and the PBKDF2 iteration count to host software which uses these parameters to transform the password to a Password Hash (PH). The Provide Authentication Parameters service can also tell you whether you are currently locked to an auto decrypt slot.
Delete Key Slot (unauthenticated)	Deletes a key slot. Note that deleting the last key slot will cause a cartridge's encrypted data to become unreadable. This service is only available to an unauthenticated or User role if a CO sets the permissions to allow it.
Non Security Related SCSI/ATA Commands	Non-security related SCSI and ATA commands. See Sections 10.1 and 10.2 respectively. All commands listed are unauthenticated.

Table 13: Authenticated Services

Service	Description	CO	User	FW Load
Configure Automatic Decryption	This service configures the Read Data and Write Data services to be either authenticated or unauthenticated. Each configuration is specific to the cartridge inserted into the Module. This service is only available to the User role if a CO sets the permission to allow it. A User/CO may configure the Read Data and Write Data services to be unauthenticated on a specific Module and cartridge pair for one of the following two reasons: 1. The User/CO has decided the data stored on the cartridge does not have sensitive information and therefore can be considered publicly available. 2. The User/CO has confirmed that unauthorized physical and remote access to the Module (and its associated host computer) is sufficiently restricted while the cartridge is inserted.	X		
Create Additional or Modify Key Slot	Create an additional key slot or modify an existing key slot. This service creates new User and CO roles.	X		
Delete Key Slot (authenticated)	Deletes a key slot. Note that deleting the last key slot will cause a cartridge's encrypted data to become unreadable.	X	X	
Read Data (authenticated)	Decrypt and read encrypted data stored on a cartridge inserted into the Module.	X	X	
Write Data (authenticated)	Write and encrypt data onto a cartridge inserted into the Module.	X	X	
Provide Encrypted DPK	SECURITY PROTOCOL IN SCSI command used to obtain the encrypted DPK associated with a given key slot used for host side password validation. Only allowed when authentication is successful.	X	X	
FW Download	DOWNLOAD MICROCODE SCSI command used to load a firmware image. All firmware loaded into the Module is authenticated with RSA Signature Verification performed over the entire firmware image. Loaded firmware only executes if the firmware load test is successful. The version of the loaded firmware must be listed on the Module's FIPS certificate to remain in an Approved Mode.			X

Services available in the non-Approved Mode are listed in Table 14. Note that non-Approved Mode services are a subset of the services available in the Approved Mode aside from the Read Plaintext Data and Write Plaintext Data services.

Table 14: Services in the Non-Approved Mode

Service	Description
Initialize First Key Slot	CO initialization procedures to setup User and CO authentication credentials on a cartridge inserted into the Module. The Authenticate service is called as part of establishing authentication credentials.
Zeroize	SECURITY PROTOCOL OUT SCSI command used to write zeroes to the Dock PH stored in flash. All other keys/CSPs are stored only in RAM and can be cleared by power cycling the Module.
Authenticate	An operator attempts to authenticate to the Module as either a CO or User role. Authenticating the role locks the encryption key to the key slot being authenticated.
Show Status	LOG SENSE SCSI command used to send status messages, as well as the dock LED (FIPS errors) and light pipe (generic errors) output.
Read Plaintext Data	Read the plaintext data stored on a cartridge inserted into the Module.
Write Plaintext Data	Write the plaintext data onto a cartridge inserted into the Module.
Self-Tests	SEND DIAGNOSTIC SCSI command used for an operator to perform all algorithm self-tests on demand. All power-on self-tests, including the FW integrity test can be performed on demand by power cycling the Module.
Provide Authentication Parameters	SECURITY PROTOCOL IN SCSI command used to send MK-SALT, PH-SALT and the PBKDF2 iteration count to host software which uses these parameters to transform the password to a Password Hash (PH).
Delete Key Slot	Deletes a key slot.
Non Security Related SCSI/ATA Commands	Non-security related SCSI and ATA commands. See Sections 10.1 and 10.2 respectively. All commands listed are unauthenticated.
Create Additional or Modify Key Slot	Create an additional key slot or modify an existing key slot.
Provide Encrypted DPK	SECURITY PROTOCOL IN SCSI command used to obtain the encrypted DPK associated with a given key slot used for host side password validation and DPK calculation. Only allowed when authentication is successful.
FW Download	DOWNLOAD MICROCODE SCSI command used to load a firmware image. All firmware loaded into the module is authenticated with RSA Signature Verification performed over the entire firmware image. Loaded firmware only executes if the firmware load test is successful. The version of the loaded firmware must be listed on the Module's FIPS certificate to remain in an Approved Mode.

Table 15: Key and CSP Access within Services

Service	CSPs/ PSPs										
	TRNG-OUT	DRBG-NONCE	DRBG-SEED	DRBG-STATE	MK	DPK	PH	Dock PH	FW-SVK	MK-SALT	PH-SALT
Initialize First Key Slot	G,X	G,X	G,X	G,X	G,X,W	G,O,X	X	-	-	G,X,O	I,O
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	-	-	-
Authenticate[1]	-	-	-	-	G,X,W	I,W	I,X	R,X[2]	-	I,X	-
Read Encrypted Data	-	-	-	-	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-	-	-
Self-Tests	G,X	G,X	G,X	G,X	-	-	-	-	-	-	-
Provide Authentication Parameters	-	-	-	-	-	-	-	-	-	I,O	I,O
Non-Security Related SCSI/ATA Commands	-	-	-	-	-	-	-	-	-	-	-
Provide Encrypted DPK	-	-	-	-	-	O	-	-	-	-	-
Configure Automatic Decryption	G,X	G,X	G,X	G,X	G,X,W	R,O,X	-	G,W,X	-	-	-
Create Additional or Modify Key Slot	G,X	G,X	G,X	G,X	G,X,W	R,O,X	X	-	-	G,X,O	I,O
Delete Key Slot (unauthenticated)	-	-	-	-	-	-	-	-	-	-	-
Delete Key Slot (authenticated)	-	-	-	-	-	-	-	-	-	-	-
Read Data (authenticated)	-	-	-	-	-	X	-	-	-	-	-
Read Data (unauthenticated)	-	-	-	-	-	X	-	-	-	-	-
Write Data (authenticated)	-	-	-	-	-	X	-	-	-	-	-
Write Data (unauthenticated)	-	-	-	-	-	X	-	-	-	-	-
FW Download	-	-	-	-	-	-	-	-	X,I	-	-

[1] Note that the Authenticate service does not authenticate to the Module when automatic decryption is configured; rather, the Module authenticates to the cartridge.

[2] Dock PH will only be executed in place of PH if automatic decryption is configured.

Definitions of symbols used in this table:

- **G** = Generate: The Module generates or derives the Key/ CSP.
- **R** = Read: The Module reads the parameter from nonvolatile XTS hardware registers or flash.
- **X** = Execute: The Module executes the parameter; the parameter is used internally by the Module.
- **W** = Write: The Module writes the parameter to nonvolatile XTS hardware registers or flash.
- **I** = Input: The Module receives the parameter input from either the cartridge or the host.
- **O** = Output: The Module outputs the parameter to either the cartridge or the host.
- **Z** = Zeroize: The module zeroizes the parameter.
- **–** = Not accessed by the service.

4 Self-Test

4.1 Power-On Self-Tests

On power-on or reset, the Module performs self-tests as described in Table 16. The individual self-tests performed in each Approved Mode are specified in Section 11.

All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module may attempt to recover either by re-performing self-tests on request using the SCSI SEND DIAGNOSTICS command or by cycling the power.

Table 16: Power-On Self-Tests

Test Target	Description
Firmware Integrity	32-bit CRC performed over all code located in flash.
DRBG	Performs a fixed input DRBG Hash KAT, inclusive of the instantiate, generate and reseed health tests.
TRNG	The SP 800-90B Repetition Count Test and Adaptive Proportion Test are performed on power-up.
RSA-2048	Performs RSA Signature Verification KAT using an RSA 2048 bit key.
HMAC	Performs HMAC w/ SHA-256 KAT.
SHA-256	Tested as part of the DRBG Hash KAT and HMAC KAT.
XTS-AES	Performs a fixed input XTS-AES KAT.

4.2 Conditional Self-Tests

- On every call to the HW TRNG, the Module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.
- SP 800-90B Repetition Count Test (RCT).
- SP 800-90B Adaptive Proportion Test (APT).
- Periodic DRBG generate health test as specified in SP 800-90A.
- IG A.9 XTS key comparison test.
- When new firmware is loaded into the Module using the FW Download service, the Module verifies the integrity of the new firmware using RSA 2048 w/ SHA-256 signature verification.

5 Physical Security Policy

The Module is a multi-chip embedded implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by a steel dock enclosure.

For physical security, the Module requires tamper-evident seals to allow detection of the opening of the device. The Crypto Officer shall install the tamper evident seals for the module to operate in the Approved Mode of operation.

Seals are available for order from Tandberg Data (www.tandbergdata.com): part number 1022445.

Tamper-evident seal application procedure:

- Clean and dry the module surfaces where the seals are to be applied.
- Using finger/thumb pressure, slowly roll back the liner (backing material) to expose the adhesive side (underside) of the seal, taking care not to touch the adhesive with your fingers – otherwise the seal may show as being tampered with.
- Place seal on module by applying very firm pressure across the entire seal surface. Start pressure at one corner to ensure no air bubbles form.
- A curing time is required for maximum adhesion. We recommend 1 hour minimum. Full adhesion is achieved after 24 hours.

Apply the seals on the Module at enclosure locations shown below depending on the size of the RDX hardware configuration.

5.1 RDX 3.5 Inch (Two (2) Tamper-Evident Seals Required)

The SATA III RDX 3.5” has two (2) tamper-evident seals applied to the bottom of the module (Figure 4).

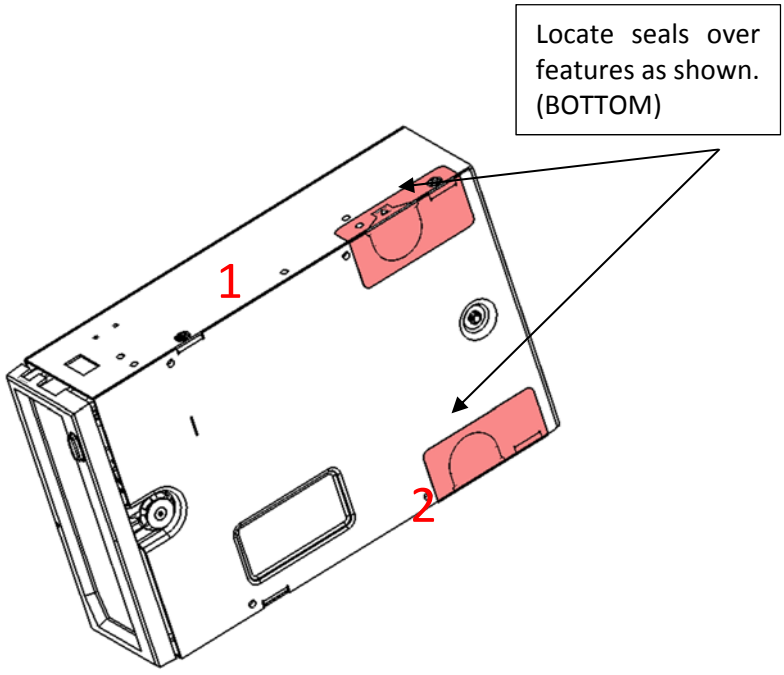

Figure 4: RDX 3.5 Inch Tamper-Evident Seal Locations

5.2 RDX 5.25” (Four (4) Tamper-Evident Seals Required)

The SATA III RDX 5.25 Inch has four (4) tamper-evident seals applied to the module, two on the top and two on the bottom (Figure 5).

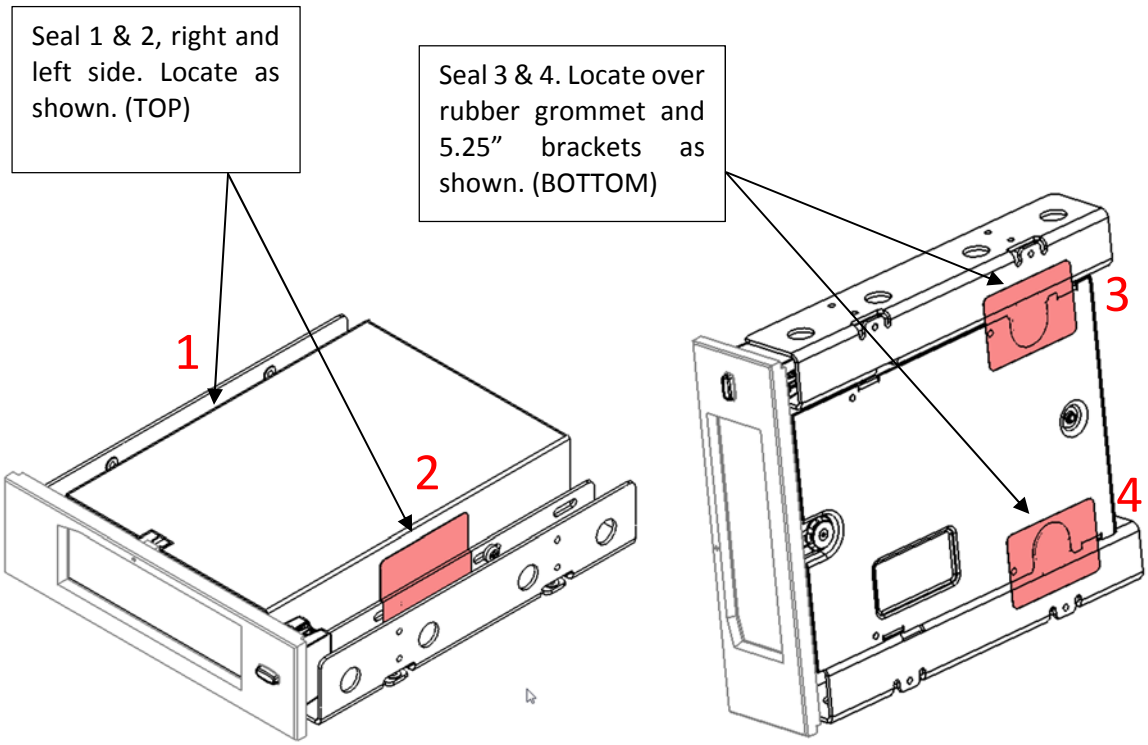

Figure 5: RDX 5.25 Inch Tamper-Evident Seal Locations

The Crypto Officer must inspect the device and tamper evident seals on a periodic basis to ensure that they are intact.

The Crypto Officer is responsible for securing and always having control of all the unused security seals.

The Crypto Officer is responsible for the direct control and observation of any changes to the device, such as reconfigurations where the tamper evident seals are removed or installed to ensure the security of the Module is maintained during such changes and the device is returned to a FIPS approved state. Upon discovery of tamper evidence, the module should be removed from service.

6 Operational Environment

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Electromagnetic Interference and Compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 Mitigation of Other Attacks Policy

The Module does not implement any mitigation of attacks outside the scope of FIPS 140-2.

9 Security Rules and Guidance

This section documents the security rules enforced by the Module and the Cryptographic Officer instructions that are necessary to implement to maintain compliance with FIPS 140-2 security requirements.

9.1 Invariant Rules

The Module implementation enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9.2 Procedural Rules

The following security rules are enforced by policy:

- The CO shall initialize the Module as specified in Section 10.3 below.
- If the Configure Automatic Decryption service is used to configure Read Data and Write Data as unauthenticated services for a specific cartridge, it is the CO's responsibility to ensure that either 1) data stored on the cartridge is not sensitive and may be considered public, or 2) physical and remote access to the Module (and the associated host computer) is sufficiently restricted during the time the cartridge is inserted. The CO shall not configure Read Data and Write Data to be unauthenticated services under any other circumstances.
- An operator shall ensure CSPs are not shared between the Approved Mode and non-Approved Mode by zeroizing the Module when switching between password protection and XTS encryption configurations. For more information please refer to the RDX Manager Product Manual section "Delete Automatic Drive Media Authentication from RDX Drive."

9.3 Cryptographic Officer Initialization

The Module is initialized by the Cryptographic Officer (CO) when a cartridge that does not already have authentication credentials available is inserted into the Module. The CO shall format the cartridge, create a key slot, select XTS-AES encryption for the slot and enter in a password hash to generate the MK. For more information please refer to the RDX Manager Product Manual section "Enable Cartridge Encryption or Password Protection." The DPK is encrypted by the MK and stored on the cartridge. The generated DPK is used for all other key slots the CO may choose to create. If the CO configures a key slot for password protection in place of XTS-AES encryption the Module is in a non-Approved Mode.

10 Non-security Related Services

10.1 Non-security Related SCSI Commands

Command Name	Operation Code
INQUIRY	12h
LOG SELECT	4Ch
LOG SENSE	4Dh
MODE SELECT (6)	15h
MODE SELECT (10)	55h
MODE SENSE (6)	1Ah
MODE SENSE (10)	5Ah
PREVENT ALLOW MEDIA REMOVAL	1Eh
READ BUFFER	3Ch
RECEIVE DIAGNOSTIC RESULTS	1Ch
RELEASE (6)	17h
RELEASE (10)	57h
REPORT LUNS	A0h
REQUEST SENSE	03h
RESERVE (6)	16h
RESERVE (10)	56h
SEND DIAGNOSTIC	1Dh
TEST UNIT READY	00h
WRITE BUFFER	3Bh
READ ATTRIBUTE	8Ch
WRITE ATTRIBUTE	8Dh
REPORT SUPPORTED OPERATION CODES	A3h
FORMAT UNIT	04h
PRE-FETCH (10) 1	34h
READ (6)	08h
READ (10)	28h
READ (16) 3	88h
READ CAPACITY (10)	25h
READ CAPACITY (16) 3	9Eh/10h
SEEK (10) 2	2Bh
START STOP UNIT	1Bh
SYNCHRONIZE CACHE (10)	35h
VERIFY (10)	2Fh
VERIFY (16) 3	8Fh
WRITE (6)	0Ah
WRITE (10)	2Ah
WRITE (16) 3	8Ah
WRITE AND VERIFY (10)	2Eh
WRITE AND VERIFY (16) 3	8Eh
GET EVENT STATUS NOTIFICATION	4Ah

10.2 Non-security Related ATA Commands

Command Name	Command Code
NOP	00h
DEVICE RESET	08h
READ SECTORS	20h
EXECUTE DEVICE DIAGNOSTIC	90h
IDENTIFY PACKET DEVICE	A1h
PACKET	A0h
IDENTIFY DEVICE	ECh
SET FEATURES	EFh
STANDBY IMMEDIATE	E0h
IDLE IMMEDIATE	E1h
CHECK POWER MODE	E5h
SLEEP	E6h

11 Multiple Approved Modes

Table 17 maps the algorithms, services and self-tests performed in each of the Approved Modes.

Table 17: Individual Approved Mode Access

Mode	Authorized Roles	Algorithms	Services	Self-Tests
No Cartridge Accessible (NCA)	• FW Load	• SHA • HMAC • RSA Signature Verification	**Unauthenticated Services:** • Show Status • Self-Tests • Non-Security Related SCSI/ATA Commands **Authenticated Services:** • FW Download	**Cryptographic Algorithm Tests:** • SHA KAT • HMAC KAT • RSA Signature Verification KAT **FW Integrity Test:** • 32-bit CRC **Conditional Tests:** • FW Load Test
Cartridge Accessible (CA)	• CO • User • FW Load	• DRBG • AES • SHA • HMAC • PBKDF • RSA Signature Verification • XTS-AES	**Unauthenticated Services:** • Initialize First Key Slot • Zeroize • Authenticate • Show Status • Read Encrypted Data • Read Data (unauthenticated) • Write Data (unauthenticated) • Self-Tests • Provide Authentication Parameters • Delete Key Slot (unauthenticated)	**Cryptographic Algorithm Tests:** • DRBG KAT • AES KAT • TRNG RCT & APT • SHA KAT • HMAC KAT • XTS-AES KAT • RSA Signature Verification KAT **Conditional Tests:** • CRNGT • RCT • APT • Periodic Generate Health Test • FW Load Test • XTS Check

			• Non Security Related SCSI/ ATA Commands **<u>Authenticated Services:</u>** • Configure Automatic Decryption • Create Additional or Modify Key Slot • Delete Key Slot (authenticated) • Read Data (authenticated) • Write Data (authenticated) • FW Download • Provide Encrypted DPK	