Decru DataFort FC520v2, LKM 2.5.1 Common Criteria Security Target

Version 3.3

October 31, 2008

Decru DataFort FC 520v2	Hardware	P/N 60-000337 Rev: B
	Firmware	SAN_V2225_external_secure
Lifetime Key Management 2.5.1	Software	LKM2.5.1

TABLE of CONTENTS

Table of Figures

Table of Tables

1 Security Target Introduction

This section contains document management and introductory material.

1.1 Security Target Identification

TOE Identification	DataFort Model	Decru DataFort FC 520v2
	DataFort Hardware P/N	60-000337Rev: B
	DataFort Firmware P/N	SAN_V2225_external_secure
	Lifetime Key Management Software	LKM 2.5.1-TOE
	Software version	LKM 2.5.1
ST Title	Decru DataFort FC520v2, LKM 2.5.1 Common Criteria Security Target	
ST Version	3.3	
ST Author	Network Appliance	
Assurance Level	EAL 4, augmented with ALC_FLR.1, Basic flaw remediation	
CC version	2.3	
PP Conformance	None	
Keywords	Storage Attached Networks, Fibre Channel Security, Fault Tolerance, Stored Data Encryption	

1.2 Security Target Overview

NetApp Inc.'s product "Decru DataFort FC520v2, LKM 2.5.1" is a fault-tolerant 2U security appliance that provides managed, encrypted network storage in a SAN (Storage Area Network). The appliance Decru DataFort FC520v2 will henceforth be referred to as DataFort. The appliance encrypts data in transit to storage, and decrypts data retrieved from storage. . The appliance also provides authentication, fine-grained access controls and secure logging in the process. DataFort supports the creation of secured storage targets called Cryptainer™ vaults or Cryptainers, in which encrypted data is stored. Data remains encrypted while stored in a Cryptainer vault, protected from unauthorized access. The TOE also includes the Lifetime Key Management™ Software that manages wrapped keys and configuration information for multiple DataForts within an organization.

1.3 Common Criteria Conformance Claims

The TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
- Part 2 extended, Part 3 conformant

- EAL 4 augmented with ALC_FLR.1, Basic flaw remediation

1.4 Terminology

Table 1-1 Terminology

ID	Definition
ACL	Access Control List
Admin Card	A smart card used to authenticate the DataFort Administrator along with the username/password for the user associated with that card.
Administrator	A user with specific privileges. In this document, the term "administrator" refers generically to all privileged users including DataFort Administrators, Physical Security Officers, LKM Operators, and Recovery officers
AES	Advanced Encryption Standard (cryptographic algorithm)
AKEP2	Authentication and Key Exchange Protocol 2
AKS	Authentication Key Set. A key derivation key, together with an Authentication key. The authentication key is used in an AKEP2 protocol, and on success, the key derivation key is used to derive a session key set.
ANSI	American National Standards Institute
Block device	Target device supporting random accesses (e.g. disk)
BSD	Berkeley Software Distribution (UNIX)
CBC	Cipher Block Chaining (cryptographic mode of operation)
CC	Common Criteria
Chassis	The physical encasement of a device. DataFort is designed to resist and detect any attempt to open the chassis.
Cluster	A cluster is a set of interconnected devices. If one fails, the other can continue providing the service. By clustering DataFort devices, total system redundancy is increased, decreasing the probability of any downtime.
Ciphertext	Encrypted data
Cleartext	Data before encryption
CLI	Command line interface
Client	The portion of the Target Of Evaluation corresponding to the DataFort FC520v2 appliance. In a client-server protocol, the client refers to the party that initiates communications. In the context of this security target, a client requests for data from a server.
Client data	Data that a client stores remotely on the storage target. In the context of this Security Target, this corresponds to data stored in Fibre Channel targets, within Cryptainers, either disks or tapes, to which the client has access.

ID	Definition
Cryptainer™	A Cryptainer is a specially designated directory or LUN. The TOE encrypts data within a Cryptainer with a Cryptainer Key, using AES-256. Note that Cryptainers are logical abstractions for data stored within Fibre Channel targets, and not for data stored within the TOE. Cryptainers represent a unit of encryption and access control as implemented within the SCSI data protection policy.
DataFort	The portion of the Target Of Evaluation corresponding to the DataFort FC520v2 appliance.
DataFort Administrator	The DataFort Administrator configures and manages the DataFort appliance portion of the TOE.
DH	Diffie-Hellman (cryptographic key agreement algorithm)
Decru Host Authentication (DHA)	Decru DHA software runs on Hosts (SCSI initiators) and performs authentication with the DataFort.
DN	Distinguished Name
EAL	Evaluation Assurance Level (CC term)
ECC	Elliptic Curve Cryptography
ECCDH	Elliptic Curve Cryptography Diffie-Hellman (key agreement algorithm)
ESP	Encapsulating Security Payload
Fabric	A group of interconnections between ports of Fibre Channel devices. A Fibre Channel fabric usually employs a Fibre Channel switch to provide direct connections between node pairs.
Failover	The ability to withstand the failure of one or several system components by transferring access to data from a failed path to a healthy one. To provide redundancy in case of failure, the TOE can be deployed in a cluster.
Fibre Channel	A high–speed interconnect used in a SAN to connect servers to shared storage. Fibre Channel components include HBAs, hubs, switches, and cabling. The term Fibre Channel (FC) simultaneously refers to the physical layer protocols, the protocols to create and maintain a collection of switches and devices in a network (called a fabric), and the serialization and transport of SCSI commands across the FC fabric from one device to another. Hosts have access across the FC fabric to storage devices through the FC fabric.
Fibre Channel Switch	Provides frame switched connectivity within a Fibre Channel fabric. The Fibre Channel equivalent of an Ethernet switch.
FIPS	Federal Information Processing Standard
FTP	File transfer protocol
HBA	Host Bus Adapter – provides the interface between the Fibre Channel connection (fabric) and the TOE.
HMAC	Keyed-Hash Message Authentication Code (crypto algorithm)
Host	Computer equipped with a Host Bus Adapter that acts as an initiator in the SCSI protocol, reading data from and storing data to targets.

ID	Definition
Host Name	Name of server in a domain
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
Initiator	The initiating end of a SCSI transaction, usually a controlling device such as a computer.
I&A	Identification and authentication
IKE	Internet Key Exchange. Used with IPsec standard.
IPsec	Internet Protocol Security. A standard for secure network communication. Communication between clustered DataForts occurs over IPsec.
IT entity	IT entity is another device on the network, such as a NetApp appliance.
Key Agreement	A key establishment procedure where the resultant secret keying material is a function of information contributed by two participants, so that no one party can predetermine the value of the secret keying material independent from the contributions of the other parties.
LCD	Liquid Crystal Display
LKM	Lifetime Key Management. NetApp's proprietary software used to manage encryption keys and Cryptainer information.
LKM Operator	The LKM Operator configures and manages the LKM software portion of the TOE that runs on the LKM Server. Compare with the DataFort Administrator who configures and manages the DataFort.
LKM Server	Host platform hosting LKM software
LKM-TOE or LKM Software	The portion of the Lifetime Key Management server that is certified (forms part of the TOE) as opposed to third party code that forms part of the operating environment (such as the operating system or an MSSQL/MySQL database).
LKM UI	LKM user interface
LUN	Logical Unit Number – the number that identifies a sub-element within a SCSI target device.
Management Station	A Windows PC equipped with a smart card reader, from which a DataFort Administrator can manage the TOE via the WebUI.
Master Key	Generated by the DataFort at initialization time. Unique to each DataFort. Required in order to decrypt other keys in the configuration database.
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
Physical Security Officer	The Physical Security Officer is the individual responsible for maintaining and checking the physical security of the DataFort prior to insertion of the System Card into the chassis.
PRNG	Pseudo Random Number Generator

ID	Definition
Quorum	Minimum of recovery officers required to complete sensitive management operations
Recovery Card	Recovery Cards are used to store and recover encryption keys, to reconstruct the configuration database, and to recover or replace smart cards. They are given to the Recovery Officers, who will have to assemble in order for sensitive procedures to take place.
Recovery Officers	The presence of the quorum of Recovery Officers is required to securely initialize the DataFort TOE and authorize sensitive operations. Each Recovery Officer is authenticated by a password, as well as physical possession of a Recovery Card.
RNG	Random Number Generator
RSA	Rivest, Shamir, Adelman (cryptographic algorithm)
SAN	A Storage Area Network (SAN) is a high-performance network dedicated to the transmission of storage data. It is often (but not necessarily) implemented with a Fibre Channel.
SAR	Security Assurance Requirement (CC term)
SCSI	Small Computer System Interface, is a set of standards for physically connecting and transferring data between high performance devices.
Security Domain	The Security Domain is a portion of the enterprise network that is protected by one or more DataFort appliances sharing user access and administrative oversight. Each Security Domain is associated with a set of Recovery Officers and Recovery Cards. A Security Domain defines a distinct group of Recovery Cards,
SEP	See Storage Encryption Processor
Server	Computer or program that accepts connections from clients in order to service requests
SF	Security Function (CC term)
SFR	Security Functional Requirement (CC term)
Sequential access	Access mode in which data must be read in a specific order (as opposed to block access.) A tape is a typical sequential target.
SHA	Secure Hash Algorithm
SOF	Strength of Function (CC term)
ST	Security Target (CC term)
Storage Encryption Processor (SEP)	A FIPS 140-2 certified hardware cryptographic module within the DataFort.
Switch	See Fibre Channel switch
System Card	A smart card provided by NetApp that is inserted inside the front panel of the DataFort chassis. The System Card must be inserted into the unit during boot by the physical security officer, and may be removed thereafter. The System Card may be removed (for instance when transporting the unit) to protect against unauthorized use.
Tape block	A unit of data on a tape, roughly equivalent to a file.

ID	Definition
Target	The receiving end of a SCSI conversation, typically devices such as a disk drive or tape drive. The DataFort acts as both SCSI target and initiator.
TLS	Transport Layer Security
TOE	Target of Evaluation (CC term)
TSF	TOE Security Functions (CC term)
Trustee	A DataFort with which Cryptainer keys may be shared after a trustee relationship has been established. The trustee feature is intended to be used to share a subset of keys with a DataFort in another cluster.
VIP	Virtual IP Address
Virtual server	Server interface that the DataFort presents to clients so that the DataFort can mediate access to clients, encrypt data before it is stored in a Cryptainer, and decrypt data when responding to a client request.
VRID	Virtual Route Identifier
WebUI	A graphical user interface used to manage the DataFort device via a web browser. Commands are entered by selecting from drop down menus and filling out web forms.
WWN	A 64 bit identifier that uniquely identifies a Fibre Channel port. A device will typically have a single, unique, node WWN and one port WWN for each port on each HBA.
3DES	Triple Data Encryption Standard

2 TOE Description

2.1 TOE Overview

NetApp Inc.'s product "Decru DataFort FC520v2, LKM 2.5.1" is a fault-tolerant 2U security appliance that provides managed, encrypted network storage in a Storage Area Network (SAN). The appliance encrypts network data in transit to storage, and decrypts data retrieved from storage; providing authentication, fine grain access controls and secure logging in the process. As data flows through the DataFort, an encryption algorithm is applied, which transforms cleartext (unencrypted) data into ciphertext (encrypted) data. DataFort supports the creation of secured storage targets called Cryptainer™ vaults, in which encrypted data is stored. Data remains encrypted while stored in a Cryptainer vault, protected from unauthorized access. When an authorized host requests data, DataFort checks that the initiator is authorized for the data, decrypts it, and then forwards it to the appropriate network destination. The TOE also includes the Lifetime Key Management™ Software and the Decru Host Authentication (DHA) client. The Lifetime Key Management Software is used to manage wrapped keys and configuration information for multiple DataForts within an organization. DHA client side application software offers an additional level of protection that can be used to ensure that the Windows host issuing an I/O request is the authorized host.

2.1.1 Product Type

The Decru DataFort™ is a fault-tolerant 2U security appliance that provides managed, encrypted network storage in a Storage Area Network (SAN). The appliance provides an access control mechanism and is able to apply information flow control rules based on subject identity and the storage location and type of data. Flow control in this context refers to whether or not data access is allowed and not any kind of traffic management, traffic shaping, or quality of service mechanism. It provides managed, encrypted network storage in a Storage Area Network (SAN). The corresponding 1U system, the Decru DataFort FC525v2 appliance, is not part of the Common Criteria evaluation and will not be discussed further.

2.1.2 Product Description

The base system of the product consists of the following:

The **2U Decru DataFort™ FC520v2 storage security appliance** mediates access to both block level (e.g. disks) and sequential (tape) targets. The DataFort functions as both an encryption appliance and an information flow control device, protecting centralized storage data.

DataForts may be clustered together to provide fault-tolerance. Members of a cluster are able to synchronize security attributes. If a member of the cluster goes offline, and if

a minimum number of cluster members, called a cluster quorum are still functioning, the cluster remains formed. If a cluster quorum is not available, then some operations are disabled to ensure data integrity. Offline cluster members can be recovered or removed to restore full cluster operation.

In case of hardware or Fibre Channel (FC) link failure, proprietary software on the Fibre Channel initiators must detect the link failure and route traffic to the other cluster members. (Note that the proprietary software on the Fibre Channel initiators is not in the TOE and outside the scope of this evaluation.)

The DataFort appliance has a smart card reader embedded into the front panel. This reader is for the System Card, which must be inserted into the unit during boot by the Physical Security Officer, and may be removed thereafter.

Should the chassis lid be opened, an intrusion detector will detect the opening and place the DataFort into a mode in which data encryption and decryption are halted, and data encryption keys are cleared from SEP volatile memory. In order to resume service, the Physical Security Officer must re-insert the System Card into the appliance, after inspecting the appliance for signs of tampering. In addition, the DataFort supports a configuration setting where it destroys all key material upon detection of tampering and the Recovery Officers have to re-initialize it.

There is also a key zeroization button on the front of the chassis that can be used to zeroize all the data encryption keys in an emergency. Zeroization removes keys in both persistent and volatile memory as well as destroying the configuration database.

The appliance contains an LCD/touch screen that shows status information (such as throughput). The LCD/touch screen on the FC520v2 can also be used to configure the IP setting prior to initialization.

DataFort Administrators manage DataFort appliances from a Management Station using the Decru Management Console (DMC), DataFort WebUI and DataFort CLI. SecureView™ licenses enable administration of multiple appliances at once via the DMC.

The management station must be equipped with a Smart Card reader. DataFort Administrators must insert their Admin Card into the Smart Card reader at the management station in order to authenticate themselves.

Additionally, a serial port may be used to configure the appliance IP address and to zeroize the appliance. Serial port access requires that a customer provide a monitor and keyboard that is physically connected to the serial console port on the DataFort's rear panel. DataFort Administrators may access this interface by providing their username and password, but a smart card is not required.

The DataFort has a Command Line Interface (CLI) that is accessed using either the WebUI or via an SSH Server. The SSH Server is disabled in the evaluated configuration, but CLI commands can be entered through the WebUI.

Basic installation places DataFort in the SAN environment so that data passes through

DataFort as it is written to storage. In the process DataFort applies an encryption algorithm to the data. When data is read, the process occurs in reverse, with DataFort decrypting the data before it reaches the host.

A network configuration that separates storage from hosts, using separate Fibre Channel (FC) switches or FC switches capable of zoning, is necessary. It is recommended that a cluster be set up across separate fabrics to avoid compromising the availability of the cluster due to common fabric events.

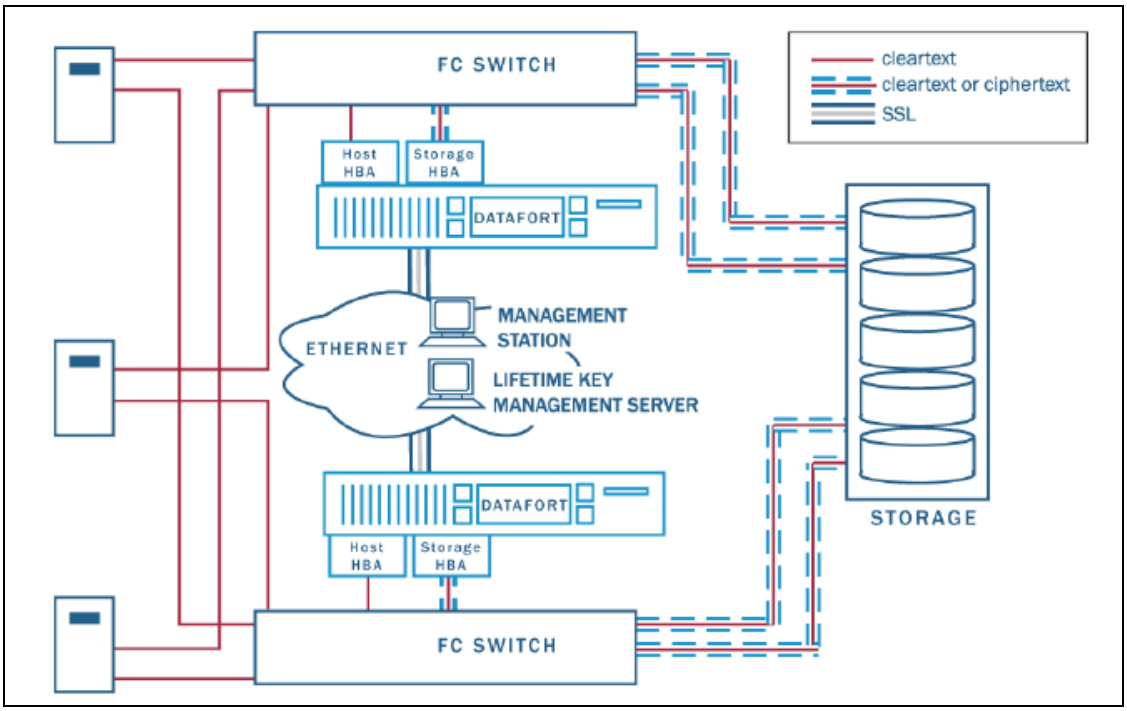

Figure 2-1 DataFort cluster with two FC switches showing redundancy

The **LKM Software** provides a mechanism to track encrypted keys and configuration information for multiple DataFort appliances within an organization. If a DataFort needs to be replaced, the configuration information and wrapped keys belonging to that appliance may be restored to a new appliance via a secure installation operation. Additionally, the LKM Software is able to send and receive wrapped keys from a DataFort appliance. For example, a DataFort that generates a large number of keys may regularly send backup copies of wrapped keys to a designated LKM Server, and then purge it from its internal key store. Since the LKM Software only receives wrapped keys, it does not have access to plaintext key material. The LKM Software includes a user interface, LKM UI.

2.1.3 Relationship between Product and TOE

The TOE consists of the base system product (the DataFort appliance), the LKM Software and DHA software.

2.2 TOE Boundary and IT Security Environment

2.2.1 Physical Boundaries

The Target of Evaluation consists of three components, the DataFort, the LKM Software and DHA client software.

- The DataFort is the Decru DataFort™ FC520v2, a storage security appliance.
- The LKM Software refers to a user interface and business logic that interacts with a third party database (MySQL and MSSQL are currently supported) and stores encrypted keys, which may be sent to the DataFort on demand.
- DHA client side application software offers an additional level of protection that can be used to ensure that the Windows host issuing an I/O request is the authorized host.

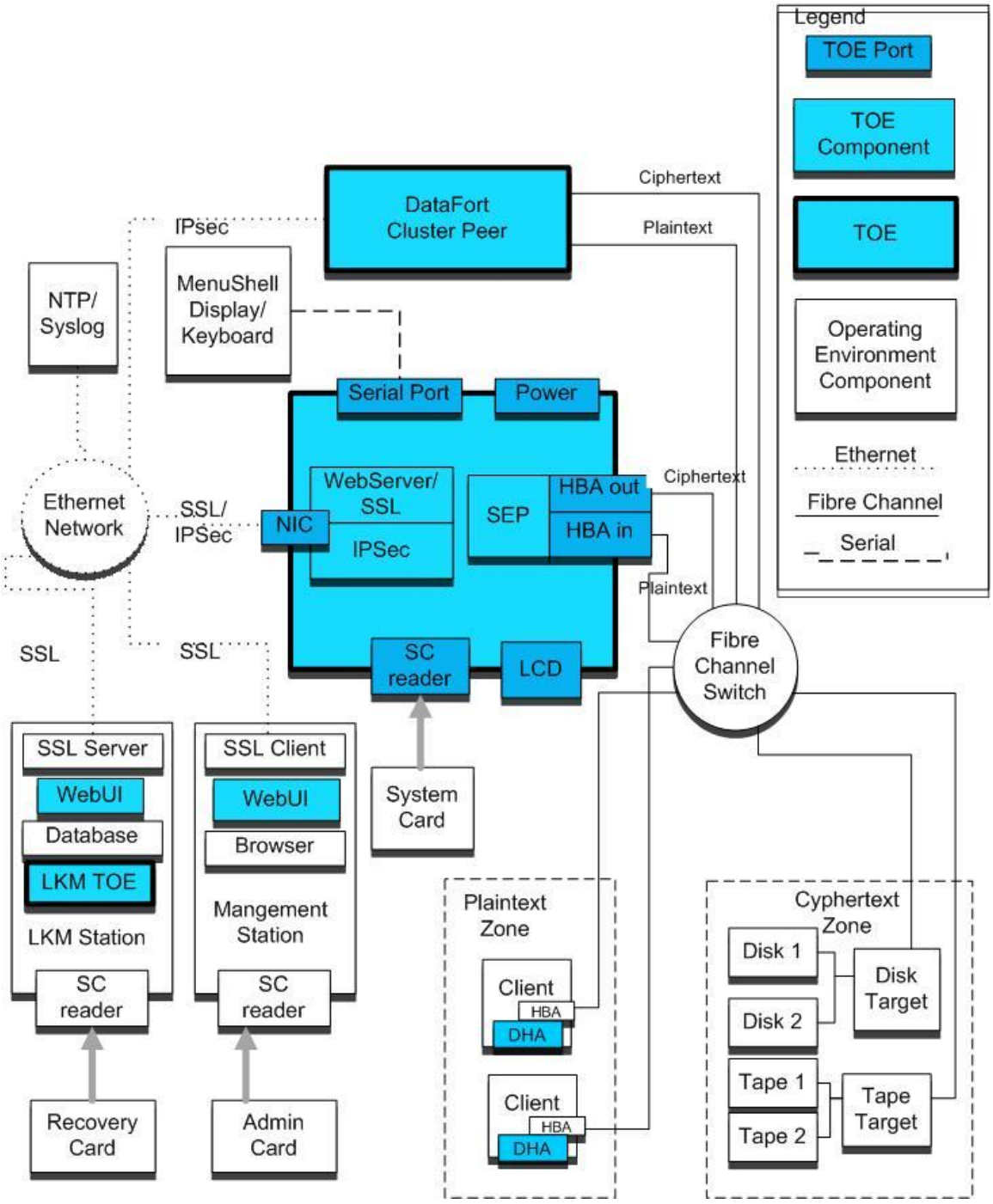

Figure 2-2: Target of Evaluation Deployment

Figure 2-1 depicts the TOE (DataFort, LKM Software and DHA) in the evaluated configuration. The evaluated configuration consists of the following:

- The entire DataFort appliance is part of the target of evaluation. The DataFort appliance is connected to the Ethernet network via a NIC, and to the Fibre Channel network via a HBA. The figure depicts a dual port HBA with the ports labeled as HBA in and HBA out. Additionally, on the Ethernet network, the appliance communicates to cluster peers via IPsec. Communication between the LKM Server (in which the LKM Software is installed) and the DataFort appliance is via TLSv1. Communication to the Management Station, from which the appliance is remotely managed, is also via TLSv1). The DataFort appliance contains a TLSv1 enabled web server that loads the WebUI into the Management Station (see below). The WebUI is part of the TOE, and consists of HTML pages with embedded Java applets.
- LKM Software consists of the user interface (LKM UI), business logic, and high-level communication logic between the LKM Server and the DataFort. Figure 2-2 depicts the LKM Software installed on the LKM Station, also known as the LKM Server.
- DHA client application initiates the connection to the DataFort and provides optional authentication for Windows based storage initiators. It implements the client side of the DHA protocol.

The TOE user interfaces (WebUI and LKM UI) also contain a facility to report the product versions of each TOE Firmware component as listed above. Base system hardware consisting of the chassis, motherboard, intrusion detector, and SEP is managed by NetApp and corresponds to the part number 60-000337 Rev: B.

Note: Decru Client Software (DCS), a deprecated software offering, is no longer supported by the Decru DataFort software and is not in the scope of evaluation.

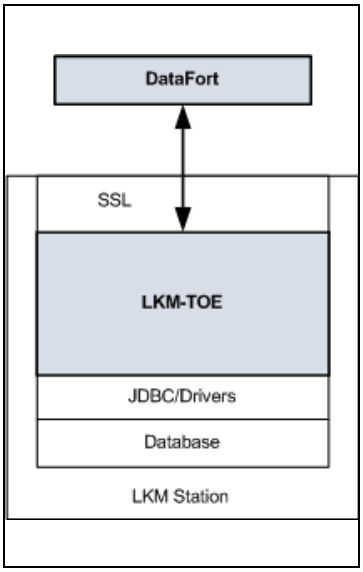

Figure 2-3: LKM Server

2.2.2 Logical Boundaries

The TOE provides the following security functions that are in the scope of the evaluation:

Security Audit

Audit records are generated within the TOE for the specified security relevant events. The DataFort may be configured to store audit log messages in temporary storage in the RAM, in the DataFort internal database and/or on a remote syslog server. In the Common Criteria configuration, the DataFort must be configured to store log messages both in its internal database and to a remote syslog server. The LKM server software will store audit records locally on the LKM server. Audit records on the LKM server may be viewed with a standard text editor. Audit records from the Windows based DHA client system are stored locally on the DHA client system. In addition, the DHA client software may be configured to send audit records to a remote syslog server or to the DHA system's local Windows event logger.

Cryptographic Support

The TOE provides cryptographic services to implement TSF security functionality such as user data protection, identification and authentication, protection of TSF data, and trusted channels.

The TOE contains a separate, physically secure, FIPS 140-2 Level 3 certified

(Certificate No. 833) cryptographic module - the Storage Encryption Processor (SEP). The SEP performs cryptographic operations in support of zeroization and self-protection.

The primary security function of the TOE is to encrypt data stored in Fibre Channel storage devices. This ensures that personnel who manage storage targets or backup tapes do not have access to plaintext data. Because the TOE is able to manage a large number of keys, further refinements of the ciphertext zone are possible. The TOE encrypts the contents of each Cryptainer with a unique key, providing for cryptographic separation of multiple data types (for example, data of differing sensitivities) stored on the same target. All Fibre Channel data encryption/decryption operations, as well as management of data encryption keys, are performed in the SEP.

The LKM Software can receive wrapped (encrypted and signed) keys from one DataFort appliance, and forward the key to another appliance, assuming both appliances were initialized to allow such key sharing by a quorum of recovery officers. The LKM Software can also zeroize keys from its internal datastore. Data is permanently unretrievable when keys used to encrypt it are destroyed in the LKM as well from the DataFort's keystore. When encrypting tapes, destruction supports a "data retention policy", if the data retention policy has rules about permanently deleting data.

Cryptographic services are also used in support of other TOE security functions such as identification and authentication using cryptographic protocols, protection of the TSF data including wrapping of keys, and trusted channels between distributed components of the TOE, other DataForts, and the Management Station. Some of the cryptographic services use cryptographic algorithms, HMAC-SHA, SHA, and AES that are implemented in the SEP and were tested as part of the FIPS certification. Other cryptographic algorithms, ECCDH and AKEP2, are implemented in the SEP and therefore were included in the scope of the FIPS 140-2 certification. However, ECCDH and AKEP2 are non-approved algorithms under FIPS 140-2, so they were not tested as part of the FIPS 140 certification effort.Certain SEP operations (ECDSA, SecretShare, RecoverSecret and ANSI X9.63 based KDFs) are outside the scope of evaluation as they are used during installation or upgrade.

Other cryptographic functionality (used for secure management/operation of the appliance clusters), specifically the TLS channels between the DataFort and the LKM Software and between the DataFort and the Management Station and the IPsec channels between DataForts within a cluster, are implemented in the platform software and were not included in the scope of the FIPS 140-2 certification. Testing for any algorithms not tested as part of the FIPS 140-2 certification is vendor affirmed. More details on where the algorithms are implemented and which implementations are included in the scope of FIPS 140-2 testing are included in Section 6.1.2 Cryptographic Support Functions.

User Data Protection

The TOE enforces a crypto-based information flow control policy to ensure that only authorized subjects are able to access plain text user data.

DataFort Administrators can compartmentalize aggregated data in shared storage using Cryptainer™ storage vaults. Cryptainer vaults, or "Cryptainers", cryptographically partition stored data at the level of Logical Unit Number (LUNs) and hence provide an additional layer of threat containment. Administrators may specify information flow control rules that specify which Fibre Channel Initiators (HBAs) may access which LUNs.

Identification and Authentication

The TOE is capable of authenticating administrators, users, and IT entities. Users are authenticated by passwords and possession of a Smart Card, depending upon their role. A DataFort administrator must prove ownership of their associated admin card and be authorized by another DataFort Administrator with the Authorizer role in order to access the WebUI interface. IT entities are authenticated using cryptographic authentication protocols and password-based authenticated protocols. There are some authentication protocols that involve cryptography (example: admin authentication which requires an administrator to prove that they are the holder of the private portion of an RSA key-pair) and some that use cryptography to protect the credentials (username/password) when the credentials are being sent from one system to another (i.e., the credentials are "in-flight"). The former would be classified as "cryptographic authentication protocols" and the latter as "password-based protocols".

Access to security functions and data is prohibited until a user is identified, with the exception of Fibre Channel Initiators that may send non-data status commands prior to identification and authentication.

Security Management

The TOE supports multiple administrative roles to support separation of security management functions. DataFort Administrators include the Full Administrator who can perform all DataFort administrative functions through the WebUI interface and "specialty" administrators who can each perform a subset of the DataFort administrative functions and can be used to enforce separation of duty. DataFort Administrators may also execute a limited set of security management commands through the serial port of the DataFort appliance.

The Physical Security Officer is responsible for maintaining and checking the physical security of the DataFort appliance prior to inserting the System Card into DataFort chassis. This ensures that the DataFort cannot be booted unless the Physical Security Officer is convinced that the DataFort has not been tampered with.

The LKM operator manages the LKM Software locally at the LKM Server.

Recovery Officers are required to perform secure installation and/or recovery operations. Recovery Officers do not perform runtime TOE administration. Recovery Officers are authenticated by a password and the possession of a smart card, the Recovery Card, and may only perform operations when acting in a quorum. During installation/recovery operations, key material is backed up and/or shared with other DataFort appliances.

Protection of the TSF

The TOE supports fault-tolerant configurations in which DataFort appliances are clustered together to provide failover in case of link failure. The fault-tolerance feature requires installation of an additional TOE in the evaluated configuration and the use of failover-capable software running on the initiator.

The TOE contains two security zones that perform self-protection functions.

The first zone consists of TOE platform software. Multiple software protection mechanisms such as a non-executable stack and heap, the segregation of network-based interface processes to chroot areas, BSD security levels, and immutable/no unlink bits on executables, protect the platform software from modification. The BSD security level is a variable used to set the restrictiveness of the operating system.

The second security zone consists of the Storage Encryption Processor (SEP), which is a FIPS 140-2 level 3 certified cryptographic module with its own physical security. The SEP maintains a potentially adversarial relationship with the first zone and protects itself against compromise by the first zone, in the sense that compromise of the TOE platform zone will neither reduce the entropy of Cryptainer Keys or of SEP CSPs nor disclose them in plaintext form.

The DataFort appliance supports reliable time stamps in conjunction with an NTP Server in the IT environment.

Trusted Channel

The TOE in conjunction with the IT environment protects TSF data from unauthorized disclosure or modification when it is being transmitted between distributed components of the TOE and copies of the TOE. The TOE supports the following trusted channels between:

- The DataFort and the LKM Software running on the LKM Server using TLSv1,
- The DataFort and the Management Station running the WebUI using TLSv1,
- Two DataForts within a cluster using IPsec, and
- A DataFort and a DataFort trustee using ECCDH and AES.

Note that all Cryptainer keys transmitted across these channels have already been wrapped (encrypted using AES and signed using HMAC-SHA-256 or 512), so the TSF does not rely upon TLS or IPsec for the protection of Cryptainer keys.

Table 5-13 - Trusted Channel Protocols and Algorithms specifies the cryptographic algorithms used within TLS, and the IPsec protocols. Section 6.1.2 Cryptographic Support Functions provides more information on how the specific cryptographic algorithms were tested (FIPS 140 versus vendor affirmed.)

2.2.3 Security Functionality in the IT Environment

The TOE depends on the IT Environment for the following security functions:

- Protection of the Audit data while it is in long term storage
- Support for the multiple methods of user and IT entity authentication
- Partial protection of the TSF files and data
- Generation of reliable timestamps
- Support for trusted channels between distributed components of the TOE and TOE copies.

2.2.4 TOE Operational Environment

The following components are connected to the DataFort appliance via the Ethernet port and are part of the operating environment:

- The Management Station is a dedicated PC that supports the functionality of the WebUI from which the DataFort may be remotely managed. The Management Station must be equipped with a smart card reader, necessary drivers and Java Runtime, and an Internet Explorer web browser with a TLS client, configured to support the TLS protocol. Administrators, equipped with Admin Cards, may log into the DataFort by loading code from the DataFort's web server into their browser. Both HTML code and Java applets are loaded from the DataFort. The web pages and embedded applets as served from the DataFort constitute the WebUI, which is part of the TOE. The Management Station is the TLS initiator.
- The LKM Server must be a dedicated PC in which the LKM Software is installed, together with a supported configuration of third party software. The LKM Server provides authentication of the LKM operator, a TLS server, the Java Runtime Environment, JDBC drivers, and a supported third party database. The LKM Server authenticates the LKM operator.
- The DHA software may be installed on a Windows based storage initiator in order to provide initiator authentication.
- Storage initiators may be equipped with optional multipath software. Mutipathing increases availability by providing multiple paths (path failover) from a server or a cluster to a storage subsystem.
- IT infrastructure services, such as an NTP server, a DNS server, and a syslog repository, are required to provide reliable clock, domain name services for hostname lookup, and long term log storage, respectively.
- The following smart cards are also part of the operating environment:
  - The *System Card* is used by the physical security officer to authenticate to the TOE, by insertion of the card into the front panel of the DataFort appliance.

- *Recovery Cards* are required during one of the three installation “wizards”: initializing a new DataFort, adding a new DataFort to an existing DataFort cluster, and re-installing a zeroized DataFort. Recovery Cards are not used during runtime.
- The *Admin Card* is used to provide two-factor authentication of DataFort Administrators when accessing the WebUI interface.

Note: each of the smart cards listed above run proprietary NetApp code and are not part of the TOE. All operations performed using the recovery cards prior to installation and during the recovery of a DataFort are also scoped out of this evaluation

Table 2-1: TOE Operating Environment Definition

TOE operating environment component		**Operating environment component definition**
Smart Cards (Admin Card, Recovery Card, System Card)		GemPlus firewall and JVM (CC certified by GemPlus)
		Decru Applet code
		GemPlus Gem Xpresso Pro 64K FIPS model smart cards
LKM operating environment	Windows Operating System (one of the following)	Windows XP SP3
		Windows 2000 Pro/Server Service Pack 4
		Windows Server 2003 Service Pack 1
	Database	MySQL or MSSQL
	Software support	Sun JVM v.1.4.2_08
		wrapper.dll v3.0.3 (makes a windows service out of java programs)
		PureTLS 0.9b4
	Minimum Hardware Specifications	2.8 Ghz Pentium
		1GB RAM
		2GB free hard drive space. LKM servers supporting multiple DataFort appliances may require more disk space. During installation you can opt to specify a different server to contain the database.
		A fixed IP address accessible via Ethernet to all DataFort appliances that will use LKM. DataFort appliances will send automated backups to this address.
		256kb connection for any remote LKM Server
		An available USB port for the smart card reader from NetApp
		A CD drive for installing software

TOE operating environment component		**Operating environment component definition**
		GemPlus smart card reader and driver
Management Station Operating environment[1]	Windows Operating System (one from list)	Windows XP Service Pack 3
		Windows 2000 Pro/Server Service Pack 4
		Windows 2003 Service Pack 1
	Browser for DataFort WebUI	Internet Explorer version 6.0 (Service Pack 1) or greater. TLS must be enabled.
		Microsoft JVM or Sun JRE 1.5.0 or greater. (DMC installs Sun JRE 1.5_06.)
	Minimum Hardware requirements (Pentium PC Server or Desktop)	1Ghz
		4GB free hard drive space
		An available USB port for the smart card reader from NetApp
		A CD drive for installing software
		GemPlus smart card reader and driver
DHA Operating Environment	Windows Operating System (one from list)	Windows XP Service Pack 3
		Windows 2000 Pro/Server Service Pack 4
		Windows 2003 Service Pack 1
		Windows NT 4.0 (SP6a or greater)

3 TOE Security Environment

This section identifies the following:

- Secure usage assumptions
- Organizational security policies
- Threats to Security

3.1 Secure Usage Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1: Assumptions

Item	Assumption	Description
1	A.Admin	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
2	A.Configure	The TOE is properly configured as described in the guidance documentation.
3	A.NoUntrusted	There are no untrusted users and no untrusted software on the Management station, LKM Server, and hosts on which DHA authentication software is installed.
4	A.PhysicalTamper	Opening the chassis sends a tamper notification signal to the SEP cryptographic module.
5	A.SmartCard	Each Smart Card is provided to the correct individual user. In addition, holders of Recovery Cards, System Cards, and Admin Cards ensure that the cards are kept in a secure location and used only in accordance with NetApp user guidance.
6	A.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote IT entities are via a secure channel.

3.2 Threats to Security

The TOE is designed to protect sensitive data and therefore to resist attackers with a moderate strength of capabilities, resources, and time. The TOE must counter the following threats to security:

Table 3-2: Threats

Item	Threat	Description

Item	Threat	Description
1	T.Disclosure	Data encrypted by the TOE may be disclosed to unauthorized persons. This includes disclosure from accessing data through software on the storage target or from physically accessing the disk or tape media.
2	T.Disruption	A malicious attacker may cause hardware or software TOE failure either by physically attacking the TOE, or by disrupting the Fibre Channel link between the TOE and the Fabric.
3	T.KeyLoss	Inadvertent or intentional loss or zeroization of encryption keys may prevent users from gaining access to their encrypted data.
4	T.Misconfiguration	Missing security management functionality may hinder effective management of the TSF and allow attackers to gain unauthorized access to resources protected by the TOE.
5	T.SelPro	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
6	T.Spoof	An unauthorized person or IT entity may attempt to access the TOE, and thereby disable security functionality, tamper with TSF code and data, or subvert security settings.
7	T.Transmission	An attacker may gain access to TSF data when it is transmitted between the DataFort and the Management Station, LKM Server, and other DataForts.
8	T.Undetectable	Administrators may make errors in the management of the TOE that are undetectable unless they are audited. A configuration error may leave the TOE vulnerable to attack by an unauthorized user.

3.3 Organizational Security Policies

No specific organizational security policies are specified for the TOE.

4 Security Objectives

The following sections describe the security objectives for the TOE and for the TOE environment.

4.1 Security Objectives for the TOE

The following table shows the security objectives for the TOE.

Table 4-1: TOE Security Objectives

Item	Objective	Description
1	O.Audit	The TSF must provide a means to accurately detect and record security-relevant events in audit records. Audit records stored on the TOE must be protected from unauthorized modification.
2	O.Crypto	The TSF must provide cryptographic operations to support user data protection, identification and authentication, and protection of TSF data and their associated key management functions.
3	O.CryptoShred	The TSF must provide mechanisms to efficiently destroy key material in accordance with an administrator-specified policy.
4	O.FaultTolerance	The TSF must provide fault tolerance of information flow control and data encryption/decryption services, ensuring continuation of service due to fibre channel link failure or failure of a cluster member.
5	O.IDAuth	The TSF must provide identification and authentication for users and IT entities.
6	O.IFC	The TSF must be able to control information flows between distributed clients and centralized storage devices.
7	O.LKM	The TSF must provide a centralized service that is able to send and receive keys and other security attributes from TOE appliances.
8	O.SecMan	The TSF must provide a means for an administrator to manage the TOE security functions.
9	O.SelPro	The TSF must maintain a domain for its own execution that protects itself and its resources from attempts by unauthorized users to bypass, deactivate, or tamper with its security functions through its own interfaces.
10	O.Time	The DataFort must provide a reliable clock to maintain the system time.
11	O.Transmission	The TSF must protect TSF data from disclosure or modification when it is transmitted between the DataFort and the Management Station, the LKM Server, and other DataForts.

4.2 Security Objectives for the Environment

The following table shows the security objectives for the IT Environment.

Table 4-2: Security Objective for the IT Environment

Item	Objective	Description
1E	OE.Audit	The IT environment must provide a long term audit store for the TOE.
2E	OE.IDAuth	The IT environment must support identification and authentication of users and IT entities.
3E	OE.SelPro	The IT environment must protect the TOE against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
4E	OE.Time	The IT environment must be configured with an NTP server that is able to provide reliable time to the TOE. The operating system platforms for the LKM Server and the management station in the IT environment must provide a reliable clock.
5E	OE.Transmission	The Management Station in the IT environment must initiate a TLSv1 session for communications with the TOE.

4.3 Security Objectives for the Non-IT Environment

Table 4-3: Security Objectives for the Non-IT Environment

Item	Objective	Description
1N	ON.Admin	Those responsible for the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
2N	ON.Configure	Those responsible for the TOE must ensure that the TOE is properly configured in accordance with administrator guidance. In addition, they must ensure that the Operating System of the LKM Server and the Management Station are properly configured to support the functioning of the LKM Software, and WebUI, respectively.
3N	ON.NoUntrusted	Those responsible for the TOE must ensure that there are no untrusted users and no untrusted software on the Management Station and LKM Server.
4N	ON.PhysicalTamper	The developer must ensure that the capabilities for the detection of physical tampering are appropriately tested.

Item	Objective	Description
5N	ON.SmartCard	Those responsible for the TOE must ensure that each Smart Card is provided to the correct individual user. In addition, holders of Recovery Cards, System Cards, and Admin Cards shall ensure that the cards are kept in a secure location and used only in accordance with DataFort administrator guidance.
6N	ON.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are via a secure channel.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations, and explicit functional components derived from the CC components.

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 and section 6.4.1.3.2 as:

- *Iteration*: allows a component to be used more than once with varying operations;
- *Assignment*: allows the specification of parameters;
- *Selection*: allows the specification of one or more items from a list; and
- *Refinement*: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the element ID. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash followed by a short textual ID such as "-AES". These follow the short family name and allow components to be used more than once with varying operations. The iteration ID is also appended to the name of the component with a colon ":". "*" refers to all iterations of a component.
- *Explicitly Stated Requirements in the TOE* will be noted with a "_EXP" added to the component ID. *Explicitly Stated Requirements in the IT Environment* will be noted with a "_ENV" added to the component ID.

Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.2 Security Functional Requirements for the TOE

Table 5-1 below summarizes the security functional requirements for the TOE. They consist of the components derived from Part 2 of the CC and explicitly stated requirements.

Table 5-1: Security Functional Requirements for the TOE

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_STG_EXP.1	Partial protected audit trail storage
3	FCS_CKM.1-AES	Cryptographic key generation: AES
4	FCS_CKM.1-RSA	Cryptographic key generation: RSA
5	FCS_CKM.1-3DES	Cryptographic key generation: 3DES
6	FCS_CKM.4	Cryptographic key destruction
7	FCS_CKM_EXP.5	Cryptographic key agreement: DH
8	FCS_CKM_EXP.6	Cryptographic key agreement: ECCDH
9	FCS_CKM_EXP.7	Cryptographic key export
10	FCS_CKM_EXP.8	Cryptographic key import
11	FCS_COP.1-AES	Cryptographic operation: AES
12	FCS_COP.1-RSA	Cryptographic operation: RSA
13	FCS_COP.1-3DES	Cryptographic operation: 3DES
14	FCS_COP_EXP.1	Cryptographic operation: HMAC-SHA
15	FCS_COP_EXP.2	Cryptographic operation: PRNG
16	FCS_COP_EXP.3	Cryptographic operation: SHA
17	FCS_COP_EXP.4	Cryptographic operation: AKEP2
18	FCS_COP_EXP.5	Cryptographic operation: Audit Log Signing
19	FDP_IFC.1	Subset information flow control
20	FDP_IFF.1	Simple security attributes
21	FIA_EAU_EXP.5	IT entity authentication mechanisms
22	FIA_EID_EXP.1	Partial IT entity timing of identification
23	FIA_UAU_EXP.5	Multiple authentication mechanisms
24	FIA_UID_EXP.2	Partial user identification before any action
25	FMT_MOF.1	Management of security functions behavior
26	FMT_MSA.1	Management of security attributes
27	FMT_MSA.2	Secure security attributes
28	FMT_MSA.3	Static attribute initialization
29	FMT_MTD.1	Management of TSF data
30	FMT_SMF.1	Specification of Management Functions
31	FMT_SMR.1	Security roles
32	FPT_FLS.1	Failure with preservation of secure state
33	FPT_RCV.4	Function recovery
34	FPT_RVM_EXP.1	Partial non-bypassability of the TSP
35	FPT_SEP_EXP.1	Partial TSF domain separation
36	FPT_STM_EXP.1	Partial reliable time stamps
37	FTP_ITC_EXP.1	Partial trusted channels

5.2.1 Class FAU: Security Audit

5.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[not specified]*** level of audit; and

c) [The events listed in column "Auditable Event" in Table 5-2: TOE Auditable Events].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST ***[information specified in last column of Table 5-3 - Audit Information].***

Table 5-2: TOE Auditable Events

Event Type	SFR	Auditable Event	Level
IFC			
	FDP_IFC.1, FDP_IFF.1	A host made a request that either violated an access rule or would have resulted in illegal information flow.	WARNING
Audit			
	FAU_GEN.1	DataFort audit function started	INFO
	FAU_GEN.1	DataFort audit function stopped	INFO
	FAU_GEN.1	Log message is repeated with no intermediary log message	Varies depending on repeated message
Authentication			
	FIA_UAU_EXP.5	User authentication failed.	WARNING
	FIA_UAU_EXP.5	User authentication succeeded.	INFO
	FIA_EAU_EXP.5	Host failed the DHA protocol.	WARNING
	FIA_EAU_EXP.5	Host successfully ran the DHA protocol.	INFO
Security Management			
	FMT_MTD.1 FMT_SMF.1	New user created.	INFO
	FMT_MTD.1 FMT_SMF.1	User deleted.	INFO

	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	DHA password of a host changed.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	DHA requirement for a host disabled.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	RAID administrator access to a host granted or revoked.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Port locking requirement turned ON for a host.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Cryptainer added.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flow added to a Cryptainer.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flow removed from a Cryptainer.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	All authorized information flows removed from a Cryptainer.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authentication requirements for a Cryptainer changed to off or DHA.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flows for a group of Cryptainers granted.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Information flows from a group of Cryptainers removed.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authentication requirements for a Cryptainer group changed to off or DHA.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	New tape pool created.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flow for the tape pool and the host added.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flow for the tape pool and the host removed	INFO

	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Modify Pool key policy attribute for the tape pool	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	ACL learning mode property for the tape pool changed, enabled or disabled	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	Authorized information flow for the tape pool and all hosts in the host group added.	INFO
	FMT_MSA.1 FMT_MTD.1 FMT_SMF.1	All authorized information flows for the tape pool and the hosts in host group removed.	INFO
Integrity			
	FPT_STM_EXP.1	DataFort clock changed.	INFO
	FCS_CKM.4	If chassis is opened or penetrated, then an intrusion event is generated..	WARNING
	FCS_CKM.4	Intrusion event triggered the zeroization function.	WARNING
	FMT_MTD.1 FMT_SMF.1	CryptoShred defense setting configured.	WARNING
	FMT_MTD.1 FMT_SMF.1	DataFort administrator issued a command to zeroize the SEP.	WARNING
	FMT_MTD.1 FMT_SMF.1	DataFort administrator issued a command to zeroize the DataFort System Card.	WARNING
	FPT_RCV.4	DataFort failover cluster aborted due to failure to reach a cluster member.	WARNING
	FPT_RCV.4	DataFort cluster transitioned to an aborted state.	WARNING
	FPT_RCV.4	DataFort cluster transitioned to an online state.	INFO
	FPT_STM_EXP.1	DataFort clock was changed by the NTP daemon	INFO
	FPT_STM_EXP.1	NTP daemon failed to change the DataFort clock.	WARNING

Table 5-3 - Audit Information

Event Type	Additional Audit **Information** for Event Type
IFC	Sequence number, priority, hostname, client, cryptainer, reason, serial number
Audit	Sequence number, priority, hostname, serial number, user, domain name of user, configuration property
Authentication	Sequence number, priority, hostname, user type, user, interface, client, reason, wwn
Security Management	Sequence number, priority, hostname, user type, user, user domain, user target, target user domain, admin, cryptainer, cryptainer group, host, host group, pool, pool group

Event Type	Additional Audit **Information** for Event Type
Integrity	Sequence number, priority, hostname, action taken (disable or zeroize SEP)

Table 5-4 Auditable Events for LKM Server

Event Type	**SFR**	**Auditable Event**	**Level**
LKM (In the LKM Software log LKM.log)			
		LKM Logger initialized	INFO
		Initiate a configuration database save to the LKM host.	INFO
		Zeroize the LKM database	INFO/ WARNING
		Single key deletion	N/A
		Delete the DataFort appliance	N/A
		Configuration database removal when Deleting a DataFort from the LKM host	INFO/ WARNING
LKM (In the LKM Software log lkmservice.log)			
		The new key creation	INFO
		The key update	INFO
		Configuration database save	INFO
		Key import to DataFort	INFO
		Echo is received and sent to IP address of DataFort	INFO
		Logged request received by LKM server.	INFO
		Logged response to DataFort query.	INFO

Table 5-5 – Auditable Events for the DHA Host

No.	**Event Type**	**SFR**	**Auditable Event**	**Level**
Audit				
1		FAU_GEN.1	Logging to syslog server turned off and on.	Information
2			Change syslog server host server setting	Information
Authentication				
3		FIA_EAU_EXP.5	Successful add of a new DataFort by DataFort name	Information
4			Successful add of a new DataFort by DataFort wwn	Information
5			Failed add of a DataFort name when the DataFort name already exists	Information
6			Failed add of a DataFort WWN when the DataFort WWN already exists	Information
7			DHA host password is successfully changed for a DataFort WWN	Warning
8			DHA host password is successfully changed for a DataFort Name	Warning

No.	Event Type	SFR	Auditable Event	Level
9			DHA host password change for a DataFort WWN failed due to old passwords mismatch	Warning
10			DHA host password change for a DataFort Name failed due to old passwords mismatch	Warning
11			Successful removal of DataFort name from DHA host	Information
12			Successful removal of DataFort wwn from DHA host.	Information
13			Rescan successful	Information
14			Rescan failed	Information
15			DHA service enabled on the DHA host	Information
16			DHA service disabled on the DHA host	Warning
17			DHA service is shutdown	Warning
18			DHA service is started	Information
19			DHA Daemon changes to “accepting input” state	Information
20			DHA service receives a command	Information
21			DHA service fails to receive a command	Information
22			DHA daemon verification of checksum of configuration file (dha.ini) file failed	Error
23			DHA daemon verification of checksum of configuration file (dha.ini) file successful	Information
24			DHA Daemon could not find configuration file (dha.ini)	Warning
25			DHA host received a challenge during DHA authentication protocol.	Warning
26			Authentication of DHA host is skipped	Information
27			Authentication of DHA host succeeded	Information
28			Authentication of DHA host failed	Warning
29			Challenge Message could not be read from the drive	Information

Dependency: FPT_STM.1 Reliable time stamps

5.2.1.2 FAU_STG_EXP.1 Partial protected audit trail storage

FAU_STG_EXP.1.1 The TSF with the support of a remote syslog server in the IT environment shall prevent any unauthorized deletions of the stored audit records.

FAU_STG_EXP.1.2 The TSF with the support of a remote syslog server in the IT environment shall prevent any unauthorized modifications to the stored audit records in the audit trail.

Dependency: FAU_GEN.1 Audit data generation

5.2.2 Class FCS: Cryptographic Support

5.2.2.1 FCS_CKM.1-AES Cryptographic key generation: AES

FCS_CKM_EXP.1-AES.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[AES]*** and specified cryptographic key sizes ***[128 and 256 bits]*** that meet the following: ***[FIPS 197]***

Dependencies:

FCS_COP.1-AES Cryptographic operation: AES

FCS_CKM.4 Cryptographic key destruction

FCS_COP_EXP.2 Cryptographic operation: PRNG

FMT_MSA.2 Secure security attributes

5.2.2.2 FCS_CKM.1-RSA Cryptographic key generation: RSA

FCS_CKM.1-RSA.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[RSA]*** and specified cryptographic key sizes ***[1024 and 2048 bits]*** that meet the following: ***[FIPS 186-2].***

Dependencies:

FCS_COP.1-RSA Cryptographic operation: RSA

FCS_CKM.4 Cryptographic key destruction

FCS_COP_EXP.2 Cryptographic operation: PRNG

FMT_MSA.2 Secure security attributes

5.2.2.3 FCS_CKM.1-3DES Cryptographic key generation: 3DES

FCS_CKM.1-3DES.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[3DES]*** and specified cryptographic key sizes ***[168 bits]*** that meet the following: ***[FIPS 46-3].***

Dependencies:

FCS_COP.1-3DES Cryptographic operation: 3DES

FCS_CKM.4 Cryptographic key destruction

FCS_COP_EXP.2 Cryptographic operation: PRNG

FMT_MSA.2 Secure security attributes

5.2.2.4 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified

cryptographic key destruction method ***[zeroization]*** that meets the following ***[DoD 5220.22-M].***

Dependencies:

[FCS_CKM.1 Cryptographic key generation or

FCS_CKM_EXP.8 Cryptographic key import]

FMT_MSA.2 Secure security attributes

5.2.2.5 FCS_CKM_EXP.5 Cryptographic key agreement: DH

FCS_CKM_EXP.5.1 The TSF shall establish keys using the Diffie-Hellman (DH) key agreement algorithm whose implementation conforms to the following standards: ANSI X9.42 and NIST SP 800-56A

Dependencies:

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1-AES Cryptographic operation: AES

5.2.2.6 FCS_CKM_EXP.6 Cryptographic key agreement: ECCDH

FCS_CKM_EXP.6.1 The TSF shall establish keys using the Elliptic Curve Cryptography Diffie-Hellman (DH) key agreement algorithm whose implementation conforms to the following standards: ANSI X9.63 and NIST SP 800-56A.

Dependencies:

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1-AES Cryptographic operation: AES

FCS_COP_EXP.1 Cryptographic operation: HMAC-SHA

5.2.2.7 FCS_CKM_EXP.7 Cryptographic key export

FCS_CKM_EXP.7.1 The TSF shall export cryptographic keys with a key size of 256 bits for use in the AES cryptographic algorithm that meets the following standards FIPS 197 and FIPS 140-2.

FCS_CKM_EXP.7.2 The TSF shall wrap the exported keys using AES encryption and the HMAC-SHA-256 for integrity.

Dependencies:

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1-AES Cryptographic operation: AES

FCS_COP_EXP.1 Cryptographic operation: HMAC-SHA

5.2.2.8 FCS_CKM_EXP.8 Cryptographic key import

FCS_CKM_EXP.8.1 The TSF shall import cryptographic keys with a key size of 256 bits for use in the AES cryptographic algorithm that meets the following standards FIPS 197 and FIPS 140-2.

FCS_CKM_EXP.8.2 The TSF shall unwrap cryptographic keys upon import using AES for decryption and the HMAC-SHA-256 for integrity.

Dependencies:

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1-AES Cryptographic operation: AES

FCS_COP_EXP.1 Cryptographic operation: HMAC-SHA

5.2.2.9 FCS_COP.1-AES Cryptographic operation: AES

FCS_COP.1-AES.1 The TSF shall perform ***[encryption, decryption]*** in accordance with a specified cryptographic algorithm ***[AES]*** and cryptographic key sizes ***[128 and 256 bits]*** that meet the following: ***[FIPS 197].***

Dependencies:

[FCS_CKM.1-AES Cryptographic key generation: AES or

FCS_CKM_EXP.7 Cryptographic key export or

FCS_CKM_EXP.8 Cryptographic key import]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.2.2.10 FCS_COP.1-RSA Cryptographic operation: RSA

FCS_COP.1-RSA.1 The TSF shall perform ***[encryption, and decryption]*** in accordance with a specified cryptographic algorithm ***[RSA]*** and cryptographic key sizes ***[1024 and 2048 bits]*** that meet the following: ***[FIPS 186-2].***

Dependencies:

FCS_CKM.1-RSA Cryptographic key generation: RSA

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.2.2.11 FCS_COP.1-3DES Cryptographic operation: 3DES

FCS_COP.1-3DES.1 The TSF shall perform ***[encryption, decryption]*** in accordance with a specified cryptographic algorithm ***[3DES]*** and cryptographic key sizes ***[168 bits]*** that meet the following: ***[FIPS 46-3].***

Dependencies

FCS_CKM.1-3DES Cryptographic key generation: 3DES

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.2.2.12 FCS_COP_EXP.1 Cryptographic operation: HMAC-SHA

FCS_COP_EXP.1.1 The TSF shall perform message authentication in accordance with a specified cryptographic algorithm HMAC-SHA and cryptographic key sizes as specified in the HMAC Key Size column of Table 5-6 that meet the following standards: FIPS 198*.*

Table 5-6: HMAC Algorithm Properties

HMAC-SHA Algorithm	SHA Algorithm	Size of output of SHA function (bits)	HMAC Key Size (bits)
HMAC-SHA-1	SHA-1	160	160
HMAC-SHA-256	SHA-256	256	256
HMAC-SHA-512	SHA-512	512	256

Dependency: FCS_COP_EXP.3 Cryptographic operation: SHA

5.2.2.13 FCS_COP_EXP.2 Cryptographic operation: PRNG

FCS_COP_EXP.2.1 The TSF shall generate pseudo random numbers in support of cryptographic key generation for the algorithms for AES, RSA, and 3DES, point multiplication for ECCDH, and nonce generation of AKEP2.

Dependencies:

FCS_CKM.1-AES Cryptographic key generation: AES

FCS_CKM.1-RSA Cryptographic key generation: RSA

FCS_CKM.1-3DES Cryptographic key generation: 3DES

FCS_CKM_EXP.6 Cryptographic key agreement: ECCDH

FCS_COP_EXP.4 Cryptographic operation: AKEP2

5.2.2.14 FCS_COP_EXP.3 Cryptographic operation: SHA

FCS_COP_EXP.3.1 The TSF shall perform secure hash in accordance with the

specified cryptographic algorithms: SHA-1, SHA-256, and SHA-512 and message digest sizes: 160 bits, 256 bits, and 512 bits, respectively that meet the following standards: FIPS 180-2.

Dependencies: None

5.2.2.15 FCS_COP_EXP.4 Cryptographic operation: AKEP2

FCS_COP_EXP.4.1 The TSF shall use the AKEP2 cryptographic protocol for mutual authentication and key exchange as specified in the Bellare and Rogaway paper (Bellare, Mihir and Phillip Rogaway, Entity Authentication and Key Distribution, August 1993).

FCS_COP_EXP.4.2 The AKEP2 cryptographic protocol shall use an ANSI X9.63 Pseudo Random Function to generate the shared secret.

Dependencies: None

5.2.2.16 FCS_COP_EXP.5 Cryptographic operation: Audit Log Signing

FCS_COP_EXP.5.1 The TSF shall digitally sign audit log records.

Dependencies: None

5.2.3 Class FDP: User Data Protection

5.2.3.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***[SCSI Data Protection Policy]*** on ***[***

- ***Controlled subjects: Fibre Channel initiators and targets (may be of block or sequential type)***
- ***Controlled information: Cryptainer Data***
  where a Cryptainer corresponds to a unit of storage (one or more LUNs or a set of tape blocks)
- ***Operations: read, write***
  In read operations, information flows from a target subject, is decrypted by the TOE using the appropriate Cryptainer Key, and is written to an initiator subject.
  In write operations, information flows from an initiator subject, is encrypted with the appropriate Cryptainer Key, and is written to the target subject.]

Dependency: FDP_IFF.1 Simple security attributes

5.2.3.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the ***[SCSI Data Protection Policy]*** based on the

following types of subject and information security attributes: ***[subject attributes defined in the column labeled "Attribute Name" of Table 5-7, information attributes defined in the column labeled "Attribute Name" of Table 5-8, and operation attributes defined in the column labeled "Attribute Name" of Table 5-9.]***

Table 5-7: Subject Attributes

Attribute Name	Meaning
WWN	Identifies the user that invoked the subject in the Fibre Channel Fabric (sufficient for HBAs, block target devices, and tape devices)
Port	Identifies the physical port (reported by the Fabric) through which the user interacts with the Fibre Channel Fabric.
Subject type	A Fibre Channel initiator, a sequential target, or a block target
Password	A reusable password (may be NULL)
Authenticated State	The authentication state of each subject is also tracked by the TSF

Table 5-8: Information Attributes

Attribute Name	Meaning
Media type	Cryptainers are classified as containing data of sequential or block media type.
Cryptainer ID	ID assigned by the TOE to controlled information.
Tape Pool ID	Identifies tape pool (only present in media of sequential type)

Table 5-9: Operation Attributes

Attribute Name	Meaning
Command	SCSI command, interpreted by the TSF as either a read command which retrieves data from the storage device, a write command which sends data to the storage device, or a no-data command which controls or tests the status of the device.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***[***

Port Locking rule

If a port number has been assigned to a subject, then the subject's reported port number, as reported by the Fabric, must match the assigned port number.

Application note: *Though port locking is expected to work with all FC switches, it is only certified with Brocade and McData FC switches.*

Authentication Rule

If an initiator subject is required to authenticate, then the subject's authentication state, as determined by the DHA rule in FDP_IFF.3, must equal "authenticated."

Authorized Flow Rule

If the Cryptainer is of block media type, then a controlled subject of initiator type with a reported WWN may issue a SCSI command to data within the Cryptainer if there is a matching allowed information flow of the form (Cryptainer ID, subject WWN, operation), where the operation is read, write, or both. (The TOE interprets a SCSI command as being of read or write type).

If the Cryptainer is of sequential media type, then a controlled subject of initiator type with a reported WWN may issue a SCSI command to data within the Cryptainer if there is a matching allowed information flow of the form (Cryptainer ID, Pool ID, subject WWN, pool operation), where operation is read, write, or both. (The TOE interprets a SCSI command as being of type read or write).]

FDP_IFF.1.3 The TSF shall enforce the ***[following additional information flow control rules:***

Decru Host Authentication rule

If the subject successfully performs a password-based authentication protocol, then the subject is considered authenticated for the next 5 minutes by the Information Flow Control functional requirement FDP_IFF.1.2. The authentication protocol satisfies the FIA_UAU_EXP.5 SFR.

Clear-text Rule

If the Assign Key Attribute is off when a Cryptainer is created on a disk, the data on the disk is not automatically encrypted and remains on the disk unprotected in cleartext format.

Application Note: The Administrator Guidance instructs trusted administrators to use this attribute only to import existing data. Once the data has been imported, it should be immediately be encrypted.

RAID Admin Rule

If RAID Admin is enabled, DataFort passes through all commands from that host to the devices it has permission to access. If RAID Admin is disabled, DataFort will block commands that it does not recognize such as unspecified commands and vendor-unique commands.

Tape Pool Rules

DataFort allows access control for tapes to be set by pool. The default Pool Policy determines whether keys are generated per tape or per pool by default. DataFort supports auto-detected pools, host default pools, and a Global Default Pool. Auto-detected pools are found during backups. Auto-detected pool labels match the application pool label. Host Default Pools are used when DataFort cannot parse pool information from the tape block 0 data. The tape is labeled with the Default Pool label. The Global Default Pool allows a single pool to be set across all hosts for applications that do not support pools.

Learning Mode Rule

Information flows between a controlled initiator subject and a controlled target subject are allowed in the absence of a matching authorized pool information flow if the TOE is in "Learning mode", in which case the attempted flow rules will be determined by the TOE based on the attempted flows.]

FDP_IFF.1.4 The TSF shall provide the following ***[additional capabilities:***

- ***To support the Decru Host Authentication rule, the TOE shall regularly attempt to authenticate initiators designated as requiring authentication.***
- ***The TOE shall forward SCSI commands which do not contain data payloads from specially designated initiators to storage devices.]***

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***[none].***

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***[The TSF shall not permit information flows from controlled target subjects to controlled target subjects, or from controlled initiator subjects to controlled initiator subjects]***

Dependencies:

FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

5.2.4 Class FIA: Identification and Authentication

5.2.4.1 FIA_EAU_EXP.5 IT Entity Authentication Mechanisms

FIA_EAU_EXP.5.1 The TSF shall provide the following authentication mechanisms:

- ***Cryptographic algorithms***
- ***Password-based authentication protocols***

to provide IT entity authentication.

FIA_EAU_EXP.5.2 The TSF shall authenticate IT entities using the mechanisms specified in Table 5-10.

Table 5-10 - IT Entity Authentication Mechanisms

IT Entity	Authentication Mechanism
Fibre Channel Initiator	Password-based authentication protocol in accordance with the rules specified in FDP_IFF.1
Admin Card	RSA public key
System Card	Negotiated Authentication Key Set and AKEP2 protocol
LKM to DataFort	AKEP2 protocol within TLSv1.
DataFort cluster peer	Diffie-Hellman public key within IKEv1

Dependencies: None

Application Notes:

This SFR covers authentication of IT entities using password-based protocols and cryptographic algorithms.

Recovery cards are authenticated in the IT environment.

5.2.4.2 FIA_EID_EXP.1 Partial IT entity timing of identification

FIA_EID_EXP.1.1 The TSF shall allow Fibre Channel initiators to send non-data status commands on behalf of the IT entity to be performed before the IT entity is identified.

FIA_EID_EXP.1.2 The TSF in conjunction with the IT environment shall require IT each entity to be successfully identified before allowing any other TSF-mediated actions on behalf of that entity.

Dependencies: None

5.2.4.3 FIA_UAU_EXP.5 Multiple authentication mechanisms

FIA_UAU_EXP.5.1 The TSF shall provide the following authentication mechanisms:

- ***Smart cards***
  - ***Admin Card***
  - ***System Card***
- ***Password***

to support user authentication.

FIA_UAU_EXP.5.2 The TSF shall authenticate any user's claimed identity according to

the following rules:

- ***DataFort Administrator***

  - ***The DataFort Administrator is authenticated to the WebUI interface by entering a password and inserting an Admin Card into the Smart Card Reader at the Management Station.***
  - ***A DataFort administrator must be authorized by another DataFort Administrator with the Authorizer role in order to access the WebUI interface.***
  - ***A DataFort Administrator is authenticated at the menushell (serial port) interface by a password.***

- ***Physical Security Officer: A Physical Security Officer is authenticated by inserting a System Card into the Smart Card Reader at the DataFort appliance.]***

Dependencies: None

Application Notes:

This SFR covers authentication of human users.

User Authentication is performed partly by the TOE and partly by the IT environment. The LKM Operator is authenticated by the IT environment host operating system on the LKM Server.

The Recovery Officer is authenticated by a password stored on the Recovery Card in the IT environment during initialization. The only Smart Card that stores a password is the Recovery Card.
User Authentication for the DataFort Administrator is a combination of Admin Card and Password. The password is not stored on the Admin Card, The Admin Card and password are associated with the DataFort Administrator at the time that the user is created and the password is stored on the DataFort.

The System Card is used to authenticate the Physical Security Officer role. No passwords are associated with the System Card.

5.2.4.4 FIA_UID_EXP.2 Partial user identification before any action

FIA_UID_EXP.2.1 The TSF in conjunction with the LKM operating system in the IT environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: None

5.2.5 Class FMT: Security Management

5.2.5.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***[determine the behavior of, disable, enable, modify the behavior of (see column 1 of Table below)]*** the functions ***[see column 2 of Table below]*** to ***[see column 3 of Table below].***

Table 5-11: Management of TOE Security Functions

#	Ability	Function	Role
1	Enable	LKM function – automated uploading of configuration databases and encrypted keys from a TOE appliance.	Full Administrator or Backup Administrator
2	Disable	LKM function – automated uploading of configuration databases and encrypted keys from a TOE appliance.	Full Administrator or Backup Administrator
3	Enable	All functions during DataFort initialization.	Recovery Officer AND Full Administrator
4	Modify the Behavior of	Allow Crypto-SEP (authorizes the Establish Trustee Link service)	Recovery Officer AND Full Administrator or Key Administrator
5	Modify the Behavior of	Allow Crypto-SEP (authorizes encryption services after boot or after opening of the chassis)	Physical Security Officer AND Full Administrator or Security Administrator

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

5.2.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***[SCSI Data Protection policy]*** to restrict the ability to ***[modify],*** the security attributes ***[subject WWN, Cryptainer ID, Tape Pool ID, initiator password, DHA authentication required, learning mode enabled or disabled, port locking required],*** to ***[the Full Administrator, or Storage Administrator].***

Dependencies:

FDP_IFC.1 Subset information flow control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

5.2.5.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FDP_IFC.1 Subset information flow control

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.2.5.4 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the ***[SCSI Data Protection policy]*** to provide ***[other]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***[no one]*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.2.5.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 **Refinement**: ***For each role,*** the TSF shall restrict the ability to ***[perform the operations listed in column 1 of Table 5-12]*** the ***[TSF data defined in column 2 of Table 5-12]*** to ***[the roles defined in column 3 of Table 5-12].***

Table 5-12: Management of TSF data

#	Operation	TSF Data	Role
1.	Execute	Set up wizard	Full Administrator
2.	Initialize	DataFort	Full Administrator
3.	Maintain	Cluster Quorum	Full Administrator or Machine Administrator
4.	Add/Remove	Cluster Members	Full Administrator or Machine Administrator
5.	Replace	DataFort appliance in a Cluster	Full Administrator
6.	Recover	Cluster	Full Administrator
7.	Resolve	Cluster Conflict	Full Administrator or Machine Administrator
8.	Add and delete	Administrators	Accounts Administrator or Full Administrator
9.	Create	Specialty administrators	Accounts Administrator or Full Administrator

#	Operation	TSF Data	Role
10.	Change	Administrator roles	Accounts Administrator or Full Administrator
11.	Associate	Administrators with smart cards	Accounts Administrator or Full Administrator
12.	Require	Login authorization for an administrator	Accounts Administrator or Full Administrator
13.	Authorize	DataFort Administrator login	Authorizer
14.	Manage	Licenses	Security Administrator or Full Administrator
15.	Manage	Trustees	Key Administrator or Full Administrator
16.	Import	Keys	Key Administrator or Full Administrator
17.	Export	Exportable keys	Key Administrator. Backup Administrator, or Full Administrator
18.	Purge	Keys upon backup to LKM	Key Administrator or Full Administrator
19.	Require	Admin Card for DataFort administrator authentication	Full Administrator or Accounts Administrator
20.	Set	Security Certificates	Full Administrator or Machine Administrator
21.	Manage	Recovery Officers and Recovery Cards	Key Administrator or Full Administrator
22.	Create and manage	Cryptainers	Storage Administrator or Key Administrator or Full Administrator
23.	Manage	Hosts	Storage Administrator or Full Administrator
24.	Manage	Storage devices	Storage Administrator or Full Administrator
25.	Modify	Subject attributes of the SCSI data protection policy (WWN, port number, , tape pool ID, password of an initiator, learning mode policy)	Storage Administrator or Full Administrator
26.	Modify	Information control rule attribute (port locking requirements, authorized flow rule, authentication requirements)	Storage Administrator or Full Administrator
27.	Manage	Tape pools and tapes	Storage Administrator or Full Administrator
28.	Enable/disable	ACL learning mode	Storage Administrator or Full Administrator
29.	Set	Virtualization on or off	Storage Administrator or Full Administrator

#	Operation	TSF Data	Role
30.	Set	Single or Multi ID mode	Storage Administrator or Full Administrator
31.	Set	DataFort Defense Level to Basic, Medium, or High	Key Administrator or Full Administrator
32.	Clear	Defense alert	Security Administrator or Full Administrator
33.	Configure and view	Log storage	Security Administrator or Full Administrator
34.	Zeroize	DataFort appliance	Security Administrator or Full Administrator
35.	Save	Configurations to Lifetime Key Management Software	Backup Administrator or Full Administrator
36.	Download	Configurations to a Remote Location	Backup Administrator or Full Administrator
37.	Configure	NTP server	Full Administrator
38.	Configure	Network settings	Machine Administrator or Full Administrator
39.	Modify	LKM ID attributes: server IP, port, secondary server IP	Key administrator, Full Administrator, or Backup Administrator
40.	Export to LKM	Encrypted Cryptainer Key	Full Administrator or Backup Administrator
41.	Import from LKM	Encrypted Cryptainer Key	Key administrator or Full Administrator
42.	View	TOE identification attributes: TOE label, TOE IP settings.	LKM Operator
43.	Transfer from one appliance to another	Keys	LKM Operator
44.	View	Cryptainer attributes: Subject attributes, Cryptainer name, Cryptainer ID, Key version (for Encrypted Cryptainer Keys sent to LKM)	LKM Operator
45.	Delete from LKM	Cryptainer Key	LKM Operator
46.	Authorize	Establishment of a Trustee	Recovery Officer and Full Administrator or Key administrator

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

5.2.5.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[***

- ***Configuring the information flow control policy parameters, including adding users, adding Cryptainers, setting authentication parameters for users, setting learning mode settings, and setting allowed information flow rules.***
- ***Configuring the number and type of administrators, and their authentication data.***
- ***Authorization of DataFort Administrator Login***
- ***Configuring the type and number of trustees***
- ***Configuring the clock to accept updates from a remote NTP server***
- ***Configuring the location of a remote log repository***
- ***Configuring the definition and number of cluster members for fault tolerance***
- ***Configuring the data retention policy, including which parameters are zeroized on intrusion, manual deletion of Cryptainer Keys in LKM, and setting time based key expiration parameters***
- ***Security management functions listed under FMT_MOF.1***
- ***Security management functions listed under FMT_MSA.1***
- ***Security management functions listed under FMT_MTD.1].***

Dependencies: None

5.2.5.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

- ***DataFort Administrator: may be one of the following types:***
  - ***Full Administrator***
  - ***Accounts Administrator***
  - ***Storage Administrator***
  - ***Key Administrator***
  - ***Security Administrator***
  - ***Backup Administrator***
  - ***Machine Administrator***
  - ***Read-Only Administrator***

- ***Authorizer***

- ***Physical Security Officer***
- ***LKM Operator***
- ***Recovery Officer***
- ***Fibre Channel Initiator]***

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependency: FIA_UID.1 Timing of identification

5.2.6 Class FPT: Protection of the TSF

5.2.6.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: ***[***

- ***Power failure to the TOE***
- ***Corruption of key or data within the SEP***
- ***Zeroization].***

Dependency: ADV_SPM.1 Informal TOE security policy model

5.2.6.2 FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that ***[***

- ***HA – Loss of service from a cluster member***
- ***SELFPRO – Zeroization]***

have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Dependency: ADV_SPM.1 Informal TOE security policy model

5.2.6.3 FPT_RVM_EXP.1 Partial Non-bypassability of the TSP

FPT_RVM_EXP.1.1 The DataFort appliance portion of the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the DataFort appliance's scope of control is allowed to proceed further.

FPT_RVM_EXP.1.2 The webUI running on the Management Station portion of the TSF, when invoked by the underlying OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the webUI's scope of control is allowed to proceed.

FPT_RVM_EXP.1.3 The LKM Software portion of the TSF, when invoked by the underlying OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the LKM Software's scope of control is allowed to proceed.

Dependencies: None

5.2.6.4 FPT_SEP_EXP.1 Partial TSF domain separation

FPT_SEP_EXP.1.1 The DataFort appliance portion of the TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects.

FPT_SEP_EXP.1.2 The WebUI running on the Management Station portion of the TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.3 The LKM Software portion of the TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.4 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

Dependencies: None

5.2.6.5 FPT_STM_EXP.1 Partial reliable time stamps

FPT_STM_EXP.1.1 The TSF with the support of an NTP Server in the IT environment shall be able to provide reliable time stamps for its own use.

Dependencies: None

5.2.7 Class FTP: Trusted path/channels

5.2.7.1 FTP_ITC_EXP.1 Partial trusted channels

FTP_ITC_EXP.1.1 The TSF with the support of TLS running on the Management Station in the IT environment shall provide trusted communication channels between distributed TOE components and the TOE and remote IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the cryptographic operations and communications protocols as shown in Table 5-13 below.

Table 5-13 - Trusted Channel Protocols and Algorithms

Trusted Channel (Initiator to Target)	Type of Channel	Comm Protocol, if applicable	Protocol RFC, if applicable	Algorithm used to establish Key	Standard	Symmetric Encryption Algorithm	Symmetric Encryption Standard	Auth type

Trusted Channel (Initiator to Target)	Type of Channel	Comm Protocol, if applicable	Protocol RFC, if applicable	Algorithm used to establish Key	Standard	Symmetric Encryption Algorithm	Symmetric Encryption Standard	Auth type
DataFort to DataFort within cluster	TOE to TOE copy	IPsec	RFC 2407, RFC 2408, RFC 2409	DH within IKEv1	X9.42 SP 800-56A	AES	FIPS 197	Shared secret
DataFort to LKM Software	Distributed TOE components	TLSv1	RFC 2246	RSA	FIPS 186-2	3DES	FIPS 46-3	Shared Secret
Mgmt Station to DataFort	TOE to IT environment	TLSv1	RFC 2246 RFC 4346	RSA	FIPS 186-2	3DES	FIPS 46-3	X509v3 certificate
DataFort to DataFort Trustee	TOE to TOE copy	NA	NA	ECCDH	X9.63 SP 800-56A	AES	FIPS 197 FIPS 140-2	SHA-256 hash value verified by offline means

FTP_ITC_EXP.1.2 The TSF shall permit the TSF or the remote trusted IT product to initiate communication via the trusted channel as indicated in the *"Trusted Channel (Initiator to Target)"* column in Table 5-13 above.

FTP_ITC_EXP.1.3 The TSF shall initiate communication via the trusted channel for user data protection, identification and authentication, and protection of TSF data.

Dependencies: None

5.2.8 TOE Strength of Function Claims

The TOE claims a minimum strength of function level of SOF-medium for all of the TOE security functional requirements with the exception of the FCS requirements, which pertain to cryptography, the strength of which is not part of the evaluation. The only permutational non-cryptographic functions in the TOE are password based authentication protocols as described in FIA_UAU_EXP.5 and FIA_EAU_EXP.5.

5.3 Security Requirements for the IT Environment

Table 5-14 lists the Security Functional Requirements provided by the IT Environment. They are all specified as explicitly stated requirements.

Table 5-14: Security Functional Requirements for the IT Environment

Item	Component	Component Name
1E	FAU_STG_ENV.1	Partial protected audit trail storage
2E	FIA_EAU_ENV.2	IT entity authentication before any action
3E	FIA_EID_ENV.2	IT entity identification before any action
4E	FIA_UAU_ENV.5	Multiple authentication mechanisms
5E	FIA_UID_ENV.2	User identification before any action
6E	FPT_RVM_ENV.1	Partial non-bypassability of the TSP
7E	FPT_SEP_ENV.1	Partial TSF domain separation
8E	FPT_STM_ENV.1	Partial reliable time stamps
9E	FTP_ITC_ENV.1	Trusted channel - management station

5.3.1 Class FAU: Security Audit

5.3.1.1 FAU_STG_ENV.1 Partial protected audit trail storage

FAU_STG_ENV.1.1 The remote syslog server in the IT Environment shall protect the DataFort stored audit records from unauthorized deletion.

FAU_STG_ENV.1.2 The remote syslog server in the IT Environment shall be able to prevent unauthorized modifications to DataFort stored audit records.

FAU_STG_ENV.1.3 The LKM server OS in the IT Environment shall protect the LKM stored audit records from unauthorized deletion.

FAU_STG_ENV.1.4 The LKM server OS in the IT Environment shall be able to prevent unauthorized modifications to LKM stored audit records.

FAU_STG_ENV.1.5 The DHA client host OS IT Environment shall protect the DHA client stored audit records from unauthorized deletion.

FAU_STG_ENV.1.6 The DHA client host OS in the IT Environment shall be able to prevent unauthorized modifications to DHA stored audit records.

Dependency: FAU_GEN.1

5.3.2 Class FIA: Identification and Authentication

5.3.2.1 FIA_EAU_ENV.2 IT entity authentication before any action

FIA_EAU_ENV.2.1 The System Card in the IT environment shall authenticate the Recovery Card using the AKEP2 protocol and notify the TSF of the success or failure of the authentication operation.

Dependencies: None

5.3.2.2 FIA_EID_ENV.2 IT entity identification before any action

FIA_EID_ENV.2.1 The Smart Card under the control of the Physical Security Officer in the IT environment shall identify the Recovery Card before authenticating it.

FIA_EID_ENV.2.2 The Recovery Card shall authenticate the Recovery Officer as the valid holder of the Recovery Card using a password.
Dependencies: None

5.3.2.3 FIA_UAU_ENV.5 Multiple authentication mechanisms

FIA_UAU_ENV.5.1 The IT environment shall provide password mechanisms to support user authentication.

FIA_UAU_ENV.5.2 The IT environment shall authenticate users according to the following rules:

- ***The operating system on the LKM Server shall authenticate the LKM operator's claimed identity using a password before allowing the LKM Operator to access the LKM software***

Dependencies: None

5.3.2.4 FIA_UID_ENV.2 User identification before any action

FIA_UID_ENV.2.1 The operating system on the LKM Server in the IT environment shall require that the LKM Operator identify him/herself before authenticating the user.

Dependencies: None

5.3.3 Class FPT: Protection of the TSF

5.3.3.1 FPT_RVM_ENV.1 Partial non-bypassability of the TSP

FPT_RVM_ENV.1.1 The security functions of the LKM Server and Management Station platforms in the IT Environment shall ensure that the IT Environment security policy enforcement functions are invoked and succeed before each function within the scope of control of the IT Environment is allowed to proceed.

Dependencies: None

5.3.3.2 FPT_SEP_ENV.1 Partial TSF domain separation

FPT_SEP_ENV.1.1 The LKM Server and management station platforms in the IT Environment shall provide shall maintain a security domain for the TOE that protects the

TOE from interference and tampering by untrusted subjects initiating actions through the platform's TSFI.

Dependencies: None

5.3.3.3 FPT_STM_ENV.1 Partial reliable time stamps

FPT_STM_ENV.1.1 The NTP server in the IT Environment in conjunction with the TOE shall be able to provide reliable time stamps for the TOE's use.

Dependencies: None

5.3.4 Class FTP: Trusted path/channels

5.3.4.1 FTP_ITC_ENV.1 Trusted channel - Management Station

FTP_ITC_ENV.1.1 The Management Station shall provide a communication channel between itself and the TOE that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure using the TLSv1 cryptographic protocol.

FTP_ITC_ENV.1.2 The Management Station shall initiate communication via the trusted channel for the protection of TSF data.

Dependencies: None

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) taken from Part 3 of the Common Criteria. The TOE shall meet the EAL 4 assurance requirements augmented by ALC_FLR.1, as listed below:

Table 5-15: Security Assurance Requirements

Assurance Class	Component	Component Title
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design

Assurance Class	Component	Component Title
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis
Flaw Remediation	ALC_FLR.1	Basic flaw remediation (augmentation)

6 TOE Summary Specification

This section provides a high-level description of the security functions and assurance measures provided by the TOE to meet the requirements specified in Section 5.

6.1 TOE Security Functions

The following table identifies the TOE Security Functions and the Security Functional Requirements to which they must conform.

Table 6-1: TSF Description

TSF	Sub-function	Sub-function description	SFR	SFR name
Security Audit	AU-1	Audit Data Generation	FAU_GEN.1	Audit data generation
	AU-2	Audit Data Storage & Protection	FAU_STG_EXP.1	Partial protected audit trail storage
Cryptographic Support	CS-1	Cryptographic Key Generation	FCS_CKM.1-AES	Cryptographic key generation: AES
			FCS_CKM.1-RSA	Cryptographic key generation: RSA
			FCS_CKM.1-3DES	Cryptographic key generation: 3DES
	CS-2	Cryptographic Key Destruction	FCS_CKM.4	Cryptographic key destruction
	CS-3	Cryptographic key Agreement	FCS_CKM_EXP.5	Cryptographic key agreement: DH
			FCS_CKM_EXP.6	Cryptographic key agreement: ECCDH
	CS-4	Cryptographic Key Export	FCS_CKM_EXP.7	Cryptographic key export
	CS-5	Cryptographic Key Import	FCS_CKM_EXP.8	Cryptographic key import
	CS-6	Advance Encryption Standard (AES)	FCS_COP.1-AES	Cryptographic operation: AES
	CS-7	Rivest Shamir Adelman (RSA)	FCS_COP.1-RSA	Cryptographic operation: RSA

TSF	Sub-function	Sub-function description	SFR	SFR name
	CS-8	Triple Data Encryption Standard (3DES)	FCS_COP.1-3DES	Cryptographic operation: 3DES
	CS-9	Keyed Hash Message Authentication Code (HMAC-SHA)	FCS_COP_EXP.1	Cryptographic operation: HMAC-SHA
	CS-10	Pseudo Random Number Generator (PRNG)	FCS_COP_EXP.2	Cryptographic operation: PRNG
	CS-11	Secure Hash (SHA)	FCS_COP_EXP.3	Cryptographic operation: SHA
	CS-12	Authentication and Key Exchange Protocol (AKEP2)	FCS_COP_EXP.4	Cryptographic operation: AKEP2
	CS-13	Audit Log Signing	FCS_COP_EXP.5	Cryptographic operation: Audit Log Signing
User Data Protection	IFC-1	Information Flow Control Enforcement	FDP_IFC.1	Subset information flow control
			FDP_IFF.1	Simple security attributes
Identification and Authentication	IA-1	User Identification and Authentication	FIA_UAU_EXP.5	Multiple authentication mechanisms
			FIA_UID_EXP.2	Partial user identification before any action
	IA-2	IT Entity Identification and Authentication	FIA_EAU_EXP.5	IT entity authentication mechanisms
			FIA_EID_EXP.1	Partial IT entity timing of identification
Security Management	SM-1	Management Functions	FMT_MOF.1	Management of security functions behaviour
			FMT_SMF.1	Specification of Management Functions

TSF	Sub-function	Sub-function description	SFR	SFR name
	SM-2	Administrative Roles	FMT_SMR.1	Security roles
	SM-3	Information Flow Control Management	FMT_MSA.1	Management of security attributes
			FMT_MSA.2	Secure security attributes
			FMT_MSA.3	Static attribute initialization
	SM-4	TSF Data Management	FMT_MTD.1	Management of TSF data
Protection of the TSF	SP-1	Self-Protection	FPT_RVM_EXP.1	Partial non-bypassability of the TSP
			FPT_SEP_EXP.1	Partial TSF domain separation
	SP-2	Fault tolerance	FPT_FLS.1	Failure with preservation of secure state
			FPT_RCV.4	Function recovery
	SP-3	Time	FPT_STM_EXP.1	Partial reliable time stamps
Trusted channel	TC-1	Trusted channel	FTP_ITC_EXP.1	Partial trusted channels

6.1.1 Security Audit Functions

6.1.1.1 AU-1: Audit Data Generation

FAU_GEN.1

Audit records are generated within the TOE by the TSF for the events listed in Table 5-2: TOE Auditable Events. Audit records contain a timestamp, the ID of the entity triggering the event (e.g. username, IP address of DataFort), and a summary of the event as well as the additional information listed in Table 5-3 - Audit Information.

6.1.1.2 AU-2: Audit Data Storage & Protection

FAU_STG_EXP.1

The TOE is able to generate three types of logs: security logs, operations logs, and performance logs, which are stored separately. All the security relevant events listed under FAU_GEN.1 are stored in security logs; only security logs are relevant for the

Common Criteria evaluation. There are two types of security logs: high priority security log and low priority security log. Events with a priority level of “WARNING” are stored in the high priority security log. Events with a priority level of “INFO” are stored in the low priority security log.

The TOE is able to store audit logs in three locations: temporary storage, database storage, and remote storage. Temporary Storage Logs stored are written to RAM within the DataFort appliance. Database storage logs are written to the DataFort appliance configuration database. For remote storage, the DataFort appliance forwards log messages to a remote syslog host.

The administrative interface allows all, some, or none of these options for storage locations to be configured. At least two of the storage options including remote storage must be selected in the evaluated configuration. The DataFort audit function is configured using the WebUI in the evaluated configuration.

DataFort purges stored log messages depending on the storage location. The purging operation is independent for the same message stored in multiple locations.

For remotely stored logs, the administrator may also optionally specify log message signing, in which case the DataFort appliance appends a signature to the exported log message. (FAU_STG_ENV.1) Audit logs are signed using HMAC-SHA-256 before they are exported from the TOE. See Section 6.1.2.13 CS-13 Audit Log Signing for more details. Audit log signing provides an integrity check that protects against unauthorized modification. There is no TOE interface to delete audit records.

The entire remote audit log is not signed over. Rather, each individual audit record within the remote audit log is signed. An administrator can then verify the signature on an individual audit record by executing a DataFort log verification command on that single record. Consequently, any unauthorized modifications or deletions within a single audit record can be detected.

6.1.2 Cryptographic Support Functions

Please consult the public Security Policy for the SEP for additional information regarding the primitives that support the cryptogrqaphic functions described below.

6.1.2.1 CS-1: Cryptographic Key Generation

FCS_CKM.1 - The TSF generates cryptographic keys for the following cryptographic algorithms implemented by the TOE:

- AES with specified key sizes 128 and 256 bits
- RSA with specified key sizes 1024 and 2048 bits
- Triple DES with specified key sizes 168 bits

. Keys are generated using pseudo random number generators in the module where the key is generated.

Keys inside the SEP are generated using a FIPS 186-2 Appendix 3 PRNG engine. This engine is continually seeded using the output of a TRNG engine.

6.1.2.2 CS-2: Cryptographic Key Destruction

FCS_CKM.4

Key destruction refers to the procedure of deleting key material in such a way that plaintext data corresponding to ciphertext may no longer be accessed. It allows for deletion of either a specific key, or deletion of all keys within the TOE.

CryptoShred™ refers specifically to the service for deleting Cryptainer keys. There are three CryptoShred mechanisms. One is a mechanism for destroying key material in the event of intrusion detection. The second is a mechanism in which key material is destroyed by pressing the key zeroization button on the front of the chassis. The third is a key retention policy, in which (wrapped) keys are deleted by the TOE platform and by the LKM Server software.

If an organization keeps all keys within the TOE and LKM database, then deleting the wrapped Cryptainer Keys from both the LKM database as well as the TOE's internal database effectively destroys the data. Keys are deleted (zeroized) in accordance with the DoD 5220.22-M standard. [Informative.]

Other cryptographic keys are destroyed within the engine where they are created. Only zeroization performed in the SEP cryptographic module is FIPS 140-2 tested. Testing of other implementations is vendor affirmed.

6.1.2.3 CS-3 Cryptographic Key Agreement

FCS_CKM_EXP.5
FCS_CKM_EXP.6

The TOE implements two algorithms for cryptographic key establishment: Diffie-Hellman, and Elliptic Curve Cryptography Diffie-Hellman (ECCDH).

The TSF implements the Diffie-Hellmann (DH) algorithm in accordance with ANSI X9.42 and NIST SP 800-56A. Diffie Hellman is used within the IKEv1 key exchange protocol to establish a symmetric AES key for use within the IPsec protocol. IPsec is used to establish a trusted channel between DataFort appliances within a cluster. The Diffie-Hellman mode of operation is dhEphem.

The TSF implements the Elliptic Curve Diffie-Hellmann (ECCDH) algorithm in accordance with ANSI X9.63 and NIST SP 800-56A. The key size is 521 bits based on the P-521 curve domain parameters as specified in FIPS 186-2. ECCDH is used for key agreement to support the trusted channel between the DataFort TOE and a DataFort trustee. The ECCDH mode of operation is (Cofactor) Ephemeral Unified Model C(2, 0, ECCDH). The cofactor is 1.

6.1.2.4 CS-4 Cryptographic Key Export

FCS_CKM_EXP.7

The TSF can export wrapped AES -256 keys to either the LKM Software, to another DataFort within a cluster, or to a trustee partner. Cryptainer keys are signed using HMAC-SHA-512 and the rest of the keys in the system are signed using HMAC-SHA-256. All keys are encrypted using AES-256.

6.1.2.5 CS-5 Cryptographic Key Import

FCS_CKM_EXP.8

The TSF can import wrapped AES keys from either the LKM Software, from another DataFort within a cluster, or from a trustee partner. Keys are unwrapped on import. Signatures are verified as part of the unwrap operation.

6.1.2.6 CS-6 Advance Encryption Standard (AES)

FCS_COP.1-AES

The TOE implements the Advanced Encryption Standard (AES) with 128 and 256 bit keys in accordance with FIPS 197.

There are three implementations of AES within the TOE. Two are within the SEP cryptographic module and have been FIPS 140-2 tested. The other one is within the IPsec engine and testing is vendor affirmed.

The primary use of AES in the DataFort is for the encryption of user data stored within Cryptainers. Data within a Cryptainer (either a designated LUN or tape block) is encrypted in a tweak encryption mode using an AES engine with a Cryptainer Key as it is written to the media, and decrypted on retrieval by authorized initiators. The encryption algorithm is AES-256 (FCS_COP.1-AES). Cryptainer Keys are generated internally using a PRNG within the SEP (FCS_CKM.1), or alternately they may be imported (in wrapped form) into the appliance from either the LKM Software, from another DataFort within a cluster, or from a trustee partner. This algorithm was tested under FIPS 140-2, and its certificate number is cert #445.

AES is also used for the wrapping of Cryptainer keys when they are transmitted internal to the TOE or when they are exported to a remote trusted IT product. In all cases in which keys are exported or imported, Recovery Officers must approve of the operation; either by initializing the TOE into the same trust domain as a clustered DataFort peer, or by authorizing a trustee link establishment operation. When keys are wrapped for transmission to the LKM or for a clustered DataFort peer, they are encrypted using the AES-256 engine described in the previous paragraph and signed using an HMAC-SHA-512 engine.

When keys are wrapped for transmission to DataFort trustee, the AES algorithm used is AES-256-CBC. This algorithm was tested under FIPS 140-2, and its certificate number is cert #446.

AES is also used within IPsec protocol, when communicating with other DataFort peers within a cluster. The AES algorithm used is AES-128-CBC. This implementation of the AES algorithm was not FIPS 140-2 tested and testing is vendor affirmed. Note that any Cryptainer keys sent over this channel are already wrapped, i.e., encrypted using AES-256 and signed using HMAC-SHA-512.

6.1.2.7 CS-7 Rivest Shamir Adelman (RSA)

FCS_COP.1-RSA

The TSF implements the RSA asymmetric algorithm with a cryptographic key size of 1024 bits that meets the FIPS 186-2 standard. RSA is used for authentication by the Admin Card and within the TLS communications protocol.

RSA is implemented within the TLS engines on the DataFort and the LKM software. Testing is vendor affirmed.

6.1.2.8 CS-8 Triple Data Encryption Standard (3DES)

FCS_COP.1-3DES

The TSF implements the Triple DES algorithm for the encryption and description of data using a key size of 168 bits accordance with the FIPS 46-3 standard.

Triple DES is used by the TLS protocol to encrypt data sent between the DataFort and an LKM Server and between DataFort and the Management Station. The operating mode for 3DES is 3DES-CBC-EDE.

6.1.2.9 CS-9 Keyed Hash Message Authentication Code (HMAC-SHA)

FCS_COP_EXP.1

The DataFort SEP implements the HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 Keyed Hash Message Authentication algorithms in accordance with FIPS 198 and FIPS 140-2. All three of these algorithms were tested as part of the FIPS 140-2 certification of the Decru DataFort SEP cryptographic module. In the DataFort SEP, HMAC is used for to provide an integrity check on wrapped keys.

HMAC is also implemented within TLS and IPsec on the DataFort and within TLS in the LKM software. These implementations of HMAC were not FIPS 140-2 tested and testing is vendor affirmed.

HMAC is used for authentication in the AKEP2 authentication and key exchange protocol.

HMAC-SHA-256 is also used for signing audit logs. This implementation is vendor affirmed.

FIPS 198 requires that HMAC be used with a FIPS approved cryptographic hash function (e.g., SHA) and that the size of the Key shall be equal to or greater than half the size of the hash function output. See Table 5-6 for how the SHA message digest

and the selected HMAC key sizes relate to each other.

6.1.2.10 CS-10 Pseudo Random Number Generation (PRNG)

FCS_COP_EXP.2

The TSF implements a pseudo random number generator algorithm. Pseudo random number generators are required to support key generation for other cryptographic algorithms.

The PRNG algorithm in the SEP cryptographic module was tested as part of the FIPS 140-2 certification as being in compliance with FIPS 186-2 Appendix 3. Its FIPS 140-2 number is Cert #232.

The TOE also has implemented PRNGs within TLS, IPsec, and BSD on the DataFort and within TLS in the LKM software. PRNGs are also implemented with AKEP2 protocol for generation of nonces as well as for ECCDH point multipliers, together with generation of additional paramaters such as Key IDs. Testing of these PRNG implementations is vendor affirmed.

6.1.2.11 CS-11 Secure Hash (SHA)

FCS_COP_EXP.3

The SEP implements the SHA-1, SHA-256, and SHA-512 secure hash algorithms in accordance with FIPS 180-2 and FIPS 140-2. These three secure hash algorithms were tested as part of the FIPS 140-2 certification of the Decru DataFort SEP cryptographic module. The certificate numbers for SHA-1, SHA-256, and SHA-512 respectively are Cert #192, Cert #223, and Cert #511.

SHA-1 and SHA-256 algorithms are also implemented by TLS, IPsec, and BSD on the DataFort and within by TLS in the LKM software. Testing of these SHA-1 and SHA-256 implementations is vendor affirmed.

Secure hash algorithms support other cryptographic functions. They are used for computing a random hash of a longer string. For example, the secure hash algorithms provide a message digest for input into the keyed hash message authentication code (HMAC) algorithm.

6.1.2.12 CS-12 Authentication and Key Exchange Protocol (AKEP2)

FCS_COP_EXP.4

The TOE implements the AKEP2 protocol for authentication with the algorithm defined in the Bellare and Rogaway paper. AKEP2 uses an ANSI X9.63 random number function to generate the shared secret.

The AKEP2 protocol provides authentication between the System Card and the SEP, as well as between the DataFort and the LKM Software. It is also used in the Decru Host Authentication protocol between the Host Initiators and the DataFort.

Testing of AKEP2 is vendor affirmed, as this is not a FIPS-approved algorithm.

6.1.2.13 CS-13 Audit Log Signing

FCS_COP_EXP.5

The TOE implements audit log signing using HMAC-SHA-256 to provide an integrity check on audit records when they are exported from the TSF. The BSD PRNG and HMAC-SHA-256 algorithms are used.

6.1.3 Information Flow Control Functions

6.1.3.1 IFC-1: Information Flow Control Enforcement

FDP_IFC.1, FDP_IFF.1

The TOE enforces information flow control in a Fibre Channel environment. In this environment, initiators (hosts) send ‘read’, ‘write’, and control commands to storage devices (targets) through the FC switches comprising an FC network (fabric). A single SCSI command request from a host can be either a read or a write request, but not both. There is no SCSI command for simultaneous reading and writing. For disk, reads and writes may happen at the "same time" but with different commands, usually to different blocks. For tape, reads and writes cannot be interleaved on a given tape without rewinds or seek to end of data (for append) first. Tape is generally serialized, so even the append operation would not have a read and write simultaneously. A device (host or storage device) is connected to one of the fabric’s switches via a cable. The host is typically a server or workstation containing one or more HBAs serving as FC ports attached to the fabric switch. The storage device is typically a disc drive, disc array, or tape drive attached through one or more embedded FC ports to a fabric switch. Storage devices expose their individual functions (for example a disc partition, a tape robot, or an individual tape drive unit) as logical units (each referred to as a LUN). The LUNs of a storage device are accessed through block level SCSI commands and are presented as block level devices. The switches in the fabric are responsible for forwarding frames from one device to another across the switches and inter-switch links (ISLs) of the fabric. The fabric as a whole contains a set of services responsible for maintaining the state of the fabric and its attached devices. These services include initialization, path selection, naming, device discovery (both by the fabric and by individual devices), and change notification. Devices within a fabric are identified by their FC WWN (World Wide Name). Each device has a unique WWNN (World Wide Node Name) identifying the device itself and a unique WWPN (World Wide Port Name) identifying each of its ports. In addition when a device is attached to a fabric, it is also assigned FC_ID values for each of its ports. The FC_ID is the current address of the device within the FC fabric and is used to route frames to that device. [Informative]

In this context, the TOE contains an IFC security function that handles traffic received on its Fibre Channel interfaces (ports) and implements the FDP_IFC.1 and FDP_IFF.1 requirements. The IFC function is capable of handling the SCSI commands appropriate to all supported SCSI device classes as defined by ANSI standards. The TOE maintains separate FC ports dedicated to targets and initiators, respectively, and virtualizes initiators to targets and targets to initiators, respectively. In other words, when an initiator wishes to send a command to a target, the command must be sent by the initiator to the TOE, and then the TOE applies the Information flow control function, and sends a modified command to the target on behalf of the initiator. This virtualization may occur either by port or LUN. When the TOE exposes virtual ports (internally associated to the actual storage target ports) to the initiators, those initiators accessing the storage devices must be configured to send data to the appropriate virtual ports. When the TOE exposes virtual LUNs to the initiators, those initiators accessing the storage devices must similarly be configured to access the virtual port and LUN combination. In both cases the TOE must be configured to access the correct actual storage devices according to its internal mappings such that traffic received on the virtualized target port can be forwarded to the actual storage device from the TOE. In this case the TOE acts as a virtualized initiator when communicating to the actual storage device. [Informative]

Upon first receiving a SCSI command from a unique WWPN, the security function creates a controlled subject and associates with this subject the security attributes listed in requirement FDP_IFF.1.1. Of these attributes, all but Cryptainer ID, authenticated state, and password are provided directly by the SCSI protocol.

A Cryptainer is assigned by the Full Administrator or Storage Administrator to an ordered pair (LUN, WWN) for direct access targets, and to a set of triplets {(Tape Block ID, LUN, WWN)} for sequential access targets. All of this information is provided either directly or indirectly by the Fibre Channel protocols. The IFC function is able to identify the Cryptainer ID from this information by performing a lookup.

The IFC function also contains a lookup table that classifies all supported SCSI commands into ‘read’, ‘write’, or ‘management’. Management commands do not contain data payloads, are forwarded directly to targets, and only initiators corresponding to Administrator-designated WWNs may issue these commands.

From these security attributes, the IFC function enforces the SCSI Data Protection policy by enforcing the port locking, authentication, and authorized flow rules specified in FDP_IFF.1.1 and FDP_IFF.1.2. The authentication rule, port locking settings, and authorized flows are listed in lookup tables accessible to the IFC function.

Information flow control (IFC) is enforced using the underlying cryptographic module. The IFC function forwards data payloads to the Crypto security function for encryption (and possibly signing) with the Cryptainer Key determined by a lookup table on the Cryptainer ID. The Cryptainer Key is encrypted and stored outside of the Storage Encryption Processor. The IFC function loads both the encrypted key and the data payload into the SEP, which returns the encrypted data.

For target responses to authorized requests (e.g. requests which meet the IFC rules),

the SEP decrypts data and forwards the result to authorized initiators.

The TSF enforces the following additional information flow control rules: Decru Host Authentication (DHA) Rule, Clear-Text Rule, RAID Admin Rule, Tape Pool Rules, and Learning Mode Rule. (FDP_IFF.3)

In accordance with the DHA rule, The TOE shall regularly attempt to authenticate initiators designated as requiring authentication. The authenticated state and password is reported by the supporting Identification and Authentication security function.

Cryptainers may be designated as clear-text Cryptainers using a clear text tag. A clear-text cryptainer is one that does not protect data. This feature is designed for use primarily during installation. It allows the DataFort to be 'dropped into' an existing storage environment and then rekeyed to be encrypted. Once the rekey (or encryption) is completed, the administrator removes the clear text tag and the cryptainer becomes a regular cryptainer. The Administrator Guidance states that in order to stay in the evaluated configuration clear-text Cryptainers should be used only under such scenarios.

If RAID Admin is enabled, DataFort passes through all commands from that host to the devices that the host has permission to access. If RAID Admin is disabled, DataFort will block commands that it does not recognize such as unspecified commands and vendor-unique commands. These are the commands that are allowed to pass through the TOE before identification and authentication.

DataFort allows access control for tapes to be set at the level of a pool rather than for an individual tape. The default Pool Policy determines whether keys are generated per tape or per pool by default. DataFort supports auto-detected pools, host default pools, and a Global Default Pool. Auto-detected pools are found during backups. Auto-detected pool labels match the application pool label. Host Default Pools are used when DataFort cannot parse pool information from the tape block 0 data. The tape is labeled with the Default Pool label. The Global Default Pool allows a single pool to be set across all hosts for applications that do not support pools.

If the TOE is in “Learning Mode”, information flows between a controlled initiator subject and a controlled target subject are allowed in the absence of a matching authorized pool information flow. Based on the attempted flows, the TOE will determine the attempted flow rules.

6.1.4 Identification and Authentication Functions

6.1.4.1 IA-1: User Identification and Authentication

FIA_UAU_EXP.5

FIA_UID_EXP.2

No administrative action may occur prior to user identification and authentication after

system initialization.

The TSF provides multiple mechanisms to authenticate users of the TOE:

- *Smart Card* authentication mechanism
- *Password* authentication mechanism

These methods may be used in combination as set forth in the authentication rules specified in FIA_UAU_EXP.5

The Physical Security Officer is identified by possession of the System Card.

DataFort Administrators, when accessing the TOE management interface, are authenticated with a username and reusable password, together with possession of an Admin Card. The password must be at least 8 characters in length, and may contain alphanumeric, upper and lower case characters. The TOE is configured to require that administrators be authenticated in pairs, to enforce a two-man rule requirement. Requiring that another administrator with the "authorizer" role authorize an administrator's login enforces this notion.

Administrators may also authenticate via their username and password to access the menushell (serial port) interface, which allows for changing the IP settings of the TOE, as well as zeroizing the TOE.

User Authentication is performed partly by the TOE and partly by the IT environment. The LKM Operator is authenticated by the host operating system on the LKM Server. The Recovery Officer is authenticated by a password stored on the Recovery Card during initialization of the TOE.

6.1.4.2 IA-2: IT Entity Identification and Authentication

FIA_EAU_EXP.5

FIA_EID_EXP.1

The only actions allowed before IT entity identification and authentication are that some Fibre Channel initiators may send non-data status commands through the TOE to targets.

The TSF uses a combination of cryptographic algorithms and password based protocols to authenticate IT entities.

The TSF identifies and authenticates the following IT entities:

- ***Fibre Channel Initiators***
- ***Admin Cards***
- ***System Cards***
- ***LKM Server***
- ***DataFort with Cluster***

Fibre Channel Initiators

Fibre Channel block targets (e.g. disk storage) are identified according to WWN. Fibre Channel sequential targets consist of both a tape drive and media. The tape drive is identified by its WWN. The Media is identified according to the Media ID, which can correspond to a Tape ID or a Tape Pool ID. The Media ID attributes are read from specially designated blocks on the tape, as implemented by each tape vendor and backup application

Fibre Channel Initiators are authenticated using password-based DHA authentication protocol in accordance with the rules specified in FDP_IFF.1

Admin Cards

Admin cards authenticate to the DataFort utilizing the RSA key pairs.

System Cards

The system card authenticates itself to the SEP using the AKEP2 protocol. The Decru Applet code running on the Smart Cards implements cryptographic algorithms in support of identification and authentication.

DataFort to LKM Software

The DataFort and the LKM software communicate using a channel that is secured by TLSv1 and AKEP2. Upon successful completion of the TLS handshake, the two parties mutually authenticate each other with AKEP2 using a combination of a pre-shared secret and the pre-master secret that was used to establish the TLS channel. To support, AKEP2, the DataFort Administrator and LKM operator must enter the shared secret.

DataFort Peers within a Cluster

DataFort peers within a cluster are authenticated using Diffie-Hellman ephemeral public keys within IKEv1.

Management Stations

Authentication of Management Stations is not required, since DataFort Administrators authenticate themselves directly to the DataFort appliance through the WebUI interface. The DataFort is the TLS Server.

Recovery Cards

Recovery cards initialized for a particular DataFort during TOE initialization. When inserted, the System Card in the IT environment using the AKEP2 protocol authenticates them.

Trustees

Trustee Link Establishment is performed using the ECCDH cryptographic algorithm.

6.1.5 Security Management Functions

6.1.5.1 SM-1: Management Functions

FMT_MOF.1, FMT_SMF.1

The TOE's primary security management interface is the WebUI, which is a java web application loaded from the TOE onto the Management Station via a TLS channel. DataFort Administrators interact with the applet, sending commands to the TSF.

The following security management functions are provided by the TSF:

- Configuration of the information flow control policy parameters, including adding users, adding Cryptainers, setting authentication parameters for users, setting learning mode settings, and setting allowed information flow rules
- Configuration of the number and type of administrators, and their authentication data.
- Configuration of the type and number of trustees
- Configuration of the clock to accept updates from a remote NTP server
- Configuration of the location of a remote log repository
- Configuration of the definition and number of cluster members for fault tolerance
- Configuration of the data retention policy, including which parameters are zeroized on intrusion, manual deletion of Cryptainer Keys in LKM, and setting time based key expiration parameters
- ***Security management functions listed under FMT_MOF.1***
- ***Security management functions listed under FMT_MSA.1***
- ***Security management functions listed under FMT_MTD.1***

The security management functions that can be modified are specified in Table 5-11: Management of TOE Security Functions.

Additionally, those with physical access to the TOE may use a menushell (serial port) interface that allows for specifying the IP parameters of the DataFort appliance, as well as for zeroization of the appliance. Connecting a workstation to the serial console port on the DataFort’s rear panel and opening a serial console, such as HyperTerminal, on the workstation, enable an administrator to logon to this interface.

6.1.5.2 SM-2: Administrative Roles

FMT_SMR.1

The TOE supports the following types of administrator roles:

- DataFort supports the creation of specialized DataFort administrators. The DataFort administrative roles are as follows:
  - ***Full Administrator***
  - ***Accounts Administrator***
  - ***Storage Administrator***
  - ***Key Administrator***
  - ***Security Administrator***
  - ***Backup Administrator***
  - ***Machine Administrator***
  - ***Read-Only Administrator***
  - ***Authorizer***
  - ***Physical Security Officer***
  - ***LKM Operator***
  - ***Recovery Officer***
  - ***Fibre Channel Initiator***

In addition, any DataFort Administrator may also be granted the Authorizer role.

- The *Physical Security Officer* is charged with maintaining the physical security of the DataFort appliance. The physical security officer is the holder of the System Card, which must be inserted into the DataFort chassis prior to booting the appliance, and may be removed thereafter. The Physical Security Officer performs no services other than inspection of the DataFort chassis, and ensuring that the appliance is physically secure while the system card is inserted into the chassis.
- *Recovery Officers* are allowed to perform secure installation and/or recovery operations. Recovery Officers do not perform runtime TOE administration. Recovery Officers are authenticated by a password and the possession of a smart card, the "Recovery Card", and may only perform operations when acting in a quorum. During installation/recovery operations, key material is backed up and/or shared with other DataFort appliances.
- The *LKM Operator* is responsible for configuring the LKM Software, and is authenticated by the LKM Server operating system.

6.1.5.3 SM-3: Information Flow Control Management

FMT_MSA.1, FMT_MSA.2, FMT_MSA.3

This TSF specifies the SCSI Data Protection policy that is used to manage the security attributes used for Information Flow Control (see IFC-1)

Lookup tables within the TOE manage all information flow control attributes. The Full

Administrator, Key Administrator or the Storage Administrator may specify port locking requirements, authentication requirements, Decru Host Authentication (DHA) requirements, and authorized flows.

To specify port locking requirements, the Full Administrator, Key Administrator or Storage Administrator first ensures that the ports used by the current initiator is correct, and then imports this value from the switch. (FMT_MSA.1)

A Full Administrator, Key Administrator or a Storage Administrator by specifying a storage location can create a Cryptainer. The default settings are such that there are no authorized information flows, port locking is not required, and authentication is not required. These settings are secure as no initiator may access the Cryptainer until an authorized flow rule is established.

The default values are as follows:

- WWN: 0
- type of flow: All
- DHA status: not enabled
- Authorization status: client not currently authenticated
- RAID admin mode: disabled
- port lock mode: disabled

The “other” default values in FMT_MSA.3.1 refer to the following:

- WWN
- type of flow
- DHA status
- Authorization status
- RAID Admin mode
- Port lock mode

(FMT_MSA.2, FMT_MSA.3)

Default settings cannot be modified. There is no external interface for changing the default values. The appliance is configured to deny access on default. Note that for sequential devices (e.g. tape storage) the module supports a learning mode, in which it allows all accesses to data, as the IFC rules are not yet enforced. The appliance records the subject attributes and flow policies, which are then enforced when learning mode is disabled. The Full Administrator, Key Administrator or the Storage Administrator must explicitly enable “Learning Mode” as it is disabled by default (see FMT_MOF.1).

FMT_MSA.2 also applies to wizards run at the WebUI as part of the appliance installation and initial configuration process. Recovery Officers are able to specify

cluster membership, and trustee exports. This involves establishing or loading shared key material into the appliance, so that FMT_MSA.2 acts in support of the FCS_COP.1 requirements.

6.1.5.4 SM-4: TSF Data Management

FMT_MTD.1

The Management of TSF Data provided by the TOE is summarized in Table 5-12: Management of TSF data.

DataFort supports the creation of specialized DataFort administrators. Only the Full Administrator can perform all DataFort Administrative functions including DataFort Initialization and Cluster management. The DataFort administrator functions listed in the paragraphs below map directly to the corresponding sections of the DataFort Administrator Guide, where they are described in more detail.

In addition, a Full Administrator can perform all of the following administrative functions:

- Account Administration
- Storage Administration
- Key Administration
- Security Administration
- Backup Administration
- Physical Security Administration
- Machine Administration

An Accounts Administrator is responsible for managing DataFort administrators. Only an Accounts Administrator or a Full Administrator can perform the following Account Administrative functions:

- Add and delete administrators
- Create specialty administrators
- Change administrator roles
- Associate administrators with smart cards
- Specify that an administrator requires login authorization

A Key Administrator is responsible for applying security-related settings to DataFort appliances. Only a Key Administrator or a Full Administrator can perform the following Account Administrative functions:

- Manage Trustees as well as importing and exporting exportable keys
- Purge keys upon backup to LKM as described in Key Purging

- Configure Management Security Settings
- Set Security Certificates
- Manage Recovery Officers and Recovery Cards

A Storage Administrator specializes in adding and deleting hosts and targets which are required in order to create Cryptainers. Only a Storage Administrator, a Full Administrator, or a Key Administrator can perform the following Storage Administration functions:

- Create Cryptainer
- Manage hosts
- Manage Cryptainer
- Manage storage
- Manage tape settings
- Manage SAN Storage Settings
- Restore a Cryptainer

A Security Administrator is responsible for applying physical security-related settings to DataFort appliances. Only a Security Administrator or a Full Administrator can perform the following Security Administration functions:

-
- Configure and Viewing Logs
- Zeroize the DataFort appliance
- Add or delete licenses

A Backup Administrator is responsible for managing backups of the configuration database, including those to LKM. Only a Backup Administrator and a Full Administrator can perform the following Backup Administration functions:

- Save configurations to Lifetime Key Management Software
- Download configurations to a Remote Location

A Machine Administrator is responsible for managing system properties and non-security sensitive cluster operations. This administrator can change local network settings. Only a Machine Administrator or a Full Administrator can perform the following Machine Administrative functions:

- Set IP addresses
- Configure the Network Time Protocol (NTP) client

Any Administrator including the Read-Only Administrator can view all DataFort settings, logs, and status. However, the Read-Only Administrator cannot modify settings. The DataFort WebUI can be used to view the following:

- DataFort Logs
- DataFort Throughput and CPU Usage
- Storage Diagnostics
- DataFort Date and Time Setting
- DataFort System Users
- DataFort Network Settings
- Crypto Status of DataFort
- Information About DataFort
- DataFort Sensors
- DataFort LCD in WebUI

Administrators who have been granted the Authorizer role may authorize another Administrator's login.

The Physical Security Officer is able to load the System Card into the TOE appliance chassis, thereby authorizing cryptographic functions to start (in case the appliance is turned off) or resume (in case the appliance is in a tamper mode).

This paragraph briefly describes the functionality provided by the Lifetime Key Management (LKM) Server software. The LKM Server software collects wrapped Cryptainer Keys from each appliance that it oversees, and can display their attributes to the LKM Operator. The LKM Operator may then transfer keys from one appliance to another, assuming that the SEPs of both appliances already share sufficient key material to decrypt the wrapped key packages. Configuration Databases of TOE appliances may also be stored within the LKM Server. In order to upload an old database copy into an existing TOE; the TOE must undergo a zeroization and re-installation procedure. In this case, a quorum of Recovery Cards are used to transfer secret shares of key material to the zeroized SEP (see "secret recovery" operations within the SEP Security Policy.) The LKM Server can be used to store wrapped Cryptainer Keys in case the internal database of a TOE is full. For example, when making tape backups that are seldom read, the Cryptainer Keys may be purged from a DataFort and exported to the LKM database. Keys needed to unwrap the Cryptainer Keys remain in the SEP and are not transferred to LKM. Additionally, the LKM Server can display the TOE name and configuration information of each unit, as well as which smart cards are assigned to that appliance. This aids an organization that manages a large number of appliances and smart cards. [Informative]

A DataFort Full Administrator (or Key Administrator) can:

- Set the LKM ID attributes of server IP, port, and secondary server IP.
- Initiate a connection to an LKM server. Once this is done, the TOE is able to upload its configuration information to the server, and to upload and download encrypted keys and databases from the LKM Server.
- Authorize data transfers to occur automatically or as a result of a DataFort Administrator issued command, once a connection is established

Once the LKM/DataFort connection is established, the LKM Operator can:

- Transfer keys from one appliance to another, assuming that the SEPs of both appliances already share sufficient key material to decrypt the wrapped key packages
- View TOE identification attributes: TOE label, TOE IP settings.
- View Cryptainer attributes: Subject attributes, Cryptainer name, Cryptainer ID, Key version (for Encrypted Cryptainer Keys sent to LKM)
- Modify the DataFort label in its internal database.
- Delete Cryptainer Keys from the LKM Server

The Recovery Officer can authorize establishment of a Trustee.

An initiator responds to the DataFort appliance with information required to enforce the SCSI Data Protection policy when a target is of sequential media type.

6.1.6 Protection of the TSF Functions

6.1.6.1 SP-1: Self-Protection

FPT_RVM_EXP.1, FPT_SEP_EXP.1

The DataFort appliance portion of the TSF enforces non-bypassability and domain separation without additional support from the IT environment. The interfaces to the DataFort appliance are designed and implemented to ensure that TSF policies are invoked before allowing access to resources protected by the TSF and to enforce of domain separation.

The LKM Software and WebUI are software only TOE components. They rely upon the protection mechanisms of the underlying operating system platforms to protect them against untrusted subjects bypassing their security mechanisms or tampering with TSF code or data through OS interfaces. The LKM Software and WebUI software are designed to ensure that TSF policies are enforced when accessed through their own interfaces.

The TSF software also protects itself from unauthorized tampering by validating user input, having a non-executable stack, separating code from data, and using authorization lists limiting the commands that users may input.

In addition to the TSF as a whole protecting itself, the SEP module protects itself by not trusting the platform software with key material or state information. From the point of view of the SEP, the TOE platform functions as a user and cannot access the SEP's internal key and state registers. In addition, interaction between the SEP and the TOE CPU occurs through a limited, well-defined register interface that defends the SEP's underlying processes against unauthorized tampering.

6.1.6.2 SP-2: Fault Tolerance

FPT_FLS.1, FPT_RCV.4

Clustering two or more DataFort-TOE copies together, with the Security Management attributes replicated among all cluster members provides fault-tolerance. This provides fault tolerance for the TOE. In particular, any cluster member can enforce the SCSI data protection policy.

It is assumed that proprietary software running on the Fibre Channel initiators will detect failure of the data path to a particular cluster member, and will reroute read and write requests to an alternate cluster member; the DataFort-TOE does not route data, but is responsible for:

- Replicating SCSI data protection policy and related attributes among cluster members
- Ensuring that the attributes are kept in synch in case a cluster member goes off-line. This is accomplished by joint monitoring system, in which DataFort TOE cluster members query each other's state to determine the health of the overall cluster

Should one DataFort TOE in a cluster experience one of the trigger events listed below, a failover will occur, where failover is defined as a transition to the following state:

- DataFort Administrators attempting to access either cluster member will not be able to modify the SCSI data protection policy attributes (either because one of the DataFort-TOEs is offline, or because the unit is online and has placed itself into a read-only state). The non-modification ensures that the failure occurs with a secure state.
- Fibre Channel initiators, which have been configured to access both cluster members will be able to continue reading and writing data from and to Cryptainers.
- Power failure to the TOE => DataFort is not operational.
- Corruption of key or data within the SEP => If a key is corrupted, then that key is not loaded and the box continues its steady state of operation.

- Zeroization => The DataFort does not have key material to perform any encrypt/decrypt operations.

The following trigger will cause a failover to occur:

- In the event of interface failure or power failure of a TOE, the active TOE will take over the load of the failed TOE.
- In case of key corruption or opening of the chassis, the TOE will place itself into an error state, prompting the failover.

The TOE also performs self-tests (the SEP module performs power on and conditional self-tests as required by FIPS 140-2, and a watchdog process also performs periodic encryption and decryption self-tests). In the event that self-tests fail, a failover will occur.

Note that there are multiple ways to recover from a failover event, determined by the nature of the error that caused the failover to occur:

- For those trigger events corresponding to the opening of the chassis, it is possible to resume service by inserting the System Card into the unit, after inspection by the Physical Security Officer. Then a Full Administrator is able to log into the WebUI and clear tamper mode.
- For trigger events corresponding to link failure, normal functioning might resume after a reboot or repair of the network connections between the cluster members, including the Fibre Channel switch, Ethernet routers, and IP or Fibre channel interconnects.
- For any non-link failure issue, one of the units can be replaced, in which case a new unit may need to be installed as a replacement cluster unit.
- A corrupt database or permissions issue may be resolved by performing a recovery operation with a backup configuration database (essentially reinstalling the unit)
- A firmware upgrade or other service may need to be performed to address failure of self-tests or entrance into an error state, as well as most key corruption issues.
- Reboot of the affected appliance will resolve internal Cryptainer Key corruption, assuming that the internal database contains a correct copy of the encrypted key.

Once a quorum of cluster members is healthy, normal functioning will resume.

6.1.6.3 SP-3 Time

FPT_STM_EXP.1

The TSF supports reliable time stamps for the use of the TSF. The DataFort acquires the time from an NTP server and maintains it for the use of TSF functions executing on the DataFort.

6.1.7 Trusted Channel

6.1.7.1 TC-1 Trusted channel

FTP_ITC_EXP.1

The TSF supports trusted channels between the TOE and other remote trusted IT products. DataFort implements trusted channels for communications between itself and the following:

- ***DataFort cluster peers***
- ***DataFort to LKM Software***
- ***Management Station to DataFort***
- ***DataFort trustees***

DataFort Cluster Peers

The TSF implements the IPsec protocol in conformance with RFC 4306. The TOE IPsec protocol uses IKEv1 for key establishment and AES for encryption. IPsec supports the trusted channel between DataFort appliance in the TOE and another DataFort appliance in the same cluster. The TOE uses transport mode and the Encapsulating Security Payload (ESP) Packet Format

DataFort to LKM

The TSF uses the TLSv1 protocol to build a trusted channel when communicating between the DataFort appliance and LKM Server. The TLS mode is TLS-RSA-WITH-3DES-EDE-CBC-SHA.

The DataFort appliance initiates the TLS Connection to the LKM TOE software.

The LKM Software generates a 1024 bit RSA key pair at initialization time. To provide mutual authentication, the DataFort platform software includes the TLS ‘master secret’ while computing the HMAC in the AKEP2 protocol.

TLS uses the 3DES symmetric algorithm for data encryption. Note that all Cryptainer Keys transmitted between the DataFort and the LKM Server are wrapped by the SEP.

Management Station to DataFort

The TSF uses the TLSv1 protocol to build a trusted channel when communicating between the DataFort appliance and Management Station. The DataFort appliance initiates the TLS connection to the Management Station platform in the IT environment. A 1024-bit RSA private key is generated at DataFort initialization time. The encryption algorithm is 3DES (EDE) in CBC mode with SHA1 being used as the underlying hash

structure. TLS-RSA-WITH-3DES-EDE-CBC-SHA is the actual TLS string for this mode.

Trustee Link Establishment

Trustee link establishment is performed using the ECCDH cryptographic algorithm. The two ends in the trustee are the importer (which initiates the trustee establishment process) and the exporter SEP that is sharing the key with the importer. The ECCDH keys are generated using the P-521 curve for point multiplication. The ECCDH mode of operation is (Cofactor) Ephemeral Unified Model C (2, 0, ECCDH) as specified in NIST SP 800-56A. The cofactor is 1. Recovery Officers use their Recovery Cards to approve trustee link establishment.

6.1.8 Strength of Function Mechanisms

The SOF claim of SOF-medium applies to the password-based authentication mechanisms as described in 6.1.4.1 IA-1: User Identification and Authentication and 6.1.4.2 IA-2: IT Entity Identification and Authentication.

6.2 Assurance Measures

The security assurance requirements are EAL4 augmented with ALC_FLR.1, Basic flaw remediation. The EAL4 assurance classes are as follows:

- Configuration Management (ACM)
- Delivery and Operation (ADO)
- Development (ADV)
- Guidance Documents (AGD)
- Life Cycle Support (ALC)
- Tests (ATE)
- Vulnerability Assessment (AVA)

The sections below show how the assurance requirements are satisfied for each class.

6.2.1.1 Configuration Management (ACM)

The following table describes how Configuration Management assurance requirements are satisfied.

Table 6-2: ACM Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
ACM_AUT.1	Partial CM automation	BID 21446: Decru DataFort FC520v2: Configuration Management Addendum (ACM_AUT.1, NetApp Acceptance Plan); v1.2

Assurance Component ID	Assurance Component Name	How Satisfied
ACM_CAP.4	Generation support and acceptance procedures	BID 21446: Release Engineering Plan; v1.1 BID 21446: CC: Decru Configuration Management Policies; 267-0019 A0 v1.1
ACM_SCP.2	Problem tracking CM coverage	DecruBugzDefectLifecycle; r5 BID 21446: Configuration List; r25

6.2.1.2 Delivery and Operation (ADO)

The following table describes how Delivery and Operation (ADO) assurance requirements are satisfied.

Table 6-3: ADO Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
ADO_DEL.2	Detection of modification	FC520v2 Packing List NetApp website Administration Guide: DataFort FC-Series Version 2.2.2; 210-03944 A0 (090208_FC222) BID 38951: CC ADO-Delivery and Operations; 267-00112_A1
ADO_IGS.1	Installation, generation, and start-up procedures	Administration Guide: DataFort FC-Series Version 2.2.2; 210-03944 A0 (090208_FC222) FC-Series Release Note 2.2.2; 210-03947 A0

6.2.1.3 Development (ADV)

The following table describes how Development (ADV) assurance requirements are satisfied.

Table 6-4: ADV Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
ADV_FSP.2	Fully defined external interfaces	BID 18761: Decru DataFort FC520v2, LKM 2.5.1 Functional Specification; v1.33
ADV_HLD.2	Security enforcing high-level design	BID 29341: DataFort Overview; v1.3
ADV_IMP.1	Subset of the implementation of the TSF	Source code needed for evaluation was provided.

Assurance Component ID	Assurance Component Name	How Satisfied
ADV_LLD.1	Descriptive low-level design	BID 39423: Decru DataFort FC520v2, LKM 2.5.1 Common Criteria EAL4: Low Level Design Documentation Roadmap and Addendum; v1.1
ADV_RCR.1	Informal correspondence demonstration	BID 27950: SAN ST to FSP Mapping; v1.11
ADV_SPM.1	Informal TOE security policy model	BID 11337: DataFort FC520v2 Security Policy Model; v1.9

6.2.1.4 Guidance Documents (AGD)

The following table describes how Guidance Documents (AGD) assurance requirements are satisfied.

Table 6-5: AGD Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
AGD_ADM.1	Administrator guidance	Administration Guide: DataFort FC-Series Version 2.2.2; 210-03944 A0 (090208_FC222) Administration Guide: Lifetime Key Management Server Software 2.5.1; 210-04034 A0 v 2.5.1 012308 Operation Guide: Decru Host Authentication; 30-000318 A0 (101608_08_DHA20) Operation Guide: Operating the DataFort Appliance in Common Criteria Mode; 30-000348 A0 (103108) Appendix IV Common Criteria Mode
AGD_USR.1	User guidance	Administration Guide: DataFort FC-Series Version 2.2.2; 210-03944 A0 (090208_FC222) Administration Guide: Lifetime Key Management Server Software 2.5.1; 210-04034 A0 v 2.5.1 012308 Operation Guide: Decru Host Authentication; 30-000318 A0 (101608_08_DHA20) Operation Guide: Operating the DataFort Appliance in Common Criteria Mode; 30-000348 A0 (103108)

6.2.1.5 Life Cycle Support (ALC)

The following table describes how Life Cycle Support (ALC) assurance requirements are satisfied.

Table 6-6: ALC Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
ALC_DVS.1	Identification of security measures	BID 38340: Decru DataFort FC520v2: Life Cycle Suport Documentation (ALC_LCD.1, ALC_TAT.1, ALC_DVS.1 and ALC_FLR.1); version 2.0
ALC_FLR.1	Basic flaw remediation	BID 38340: Decru DataFort FC520v2: Life Cycle Suport Documentation (ALC_LCD.1, ALC_TAT.1, ALC_DVS.1 and ALC_FLR.1); version 2.0
ALC_LCD.1	Developer defined life-cycle model	BID 38340: Decru DataFort FC520v2: Life Cycle Suport Documentation (ALC_LCD.1, ALC_TAT.1, ALC_DVS.1 and ALC_FLR.1); version 2.0
ALC_TAT.1	Well-defined development tools	BID 38340: Decru DataFort FC520v2: Life Cycle Suport Documentation (ALC_LCD.1, ALC_TAT.1, ALC_DVS.1 and ALC_FLR.1); version 2.0

6.2.1.6 Tests (ATE)

The following table describes how Tests (ATE) assurance requirements are satisfied.

Table 6-7: ATE Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
ATE_COV.2	Analysis of coverage	SAN2AuditTestCriteria; r50 SAN2CryptoTestCriteria; r21 SAN2IFCTestCriteria; r36 SAN2AuthenticaionTestCriteria; r29 SAN2SecureManagementTestCriteria; r62 SAN2HATestCriteria; r22 SAN2TrustedChannelsTestCriteria; r15
ATE_DPT.1	Testing: high-level design	SAN2DPT
ATE_FUN.1	Functional testing	DataFort FC520v2 Test Plan For Common Criteria (EAL4) Testing; version 1.9.0
ATE_IND.2	Independent testing – sample	TOE provided for testing

6.2.1.7 Vulnerability Assessment (AVA)

The following table describes how Vulnerability Assessment (AVA) assurance requirements are satisfied.

Table 6-8: AVA Requirements Satisfied

Assurance Component ID	Assurance Component Name	How Satisfied
AVA_MSU.2	Validation of analysis	BID 33866: Decru SAN: Evidence for AVA_MSU.2: The Misuse Analysis of the Guidance; v1.4
AVA_SOF.1	Strength of TOE security function analysis	BID 33631: Strength of Function Analysis; v1.3
AVA_VLA.2	Independent vulnerability analysis	BID 36367: DataFort Vulnerability Analysis Plan; v1.1 BID 36404: Decru DataFort FC520v2, LKM 2.5.1 Vulnerability Analysis; v1.3

7 Protection Profile Claims

This Security Target was not written to address any existing Protection Profile.

8 Rationale

This section provides the rationale for the completeness and consistency of the security target.

8.1 Security Objectives Rationale

8.1.1 Threats

The table below shows that all the identified threats to security are countered by Security Objectives for the TOE. Rationale is provided for each threat in the table.

Table 8-1: All Threats to Security Countered

Item	Threat	Security Objectives Addressing Threat	Rationale
1	T.Disclosure Data encrypted by the TOE may be disclosed to unauthorized persons. This includes disclosure from accessing data through software on the storage target or from physically accessing the disk or tape media.	O.Crypto O.CryptoShred O.IFC	This threat is mitigated by O.Crypto, which provides for confidentiality of data accessed outside of the TOE. Also, O.CryptoShred defends against disclosure of data by preventing access to data past its allowed lifetime. O.IFC requires that the system enforce an information flow policy that cannot be bypassed.
2	T.Disruption A malicious attacker may cause hardware or software TOE failure either by physically attacking the TOE, or by disrupting the Fibre Channel link between the TOE and the Fabric.	O.FaultTolerance	This threat mitigated by O.FaultTolerance, which requires that access still be provided to encryption and decryption services, in case either the TOE is damaged or a communications link between the TOE and a Fibre Channel initiator is disrupted.
3	T.KeyLoss Inadvertent or intentional loss or zeroization of encryption keys may prevent users from gaining access to their encrypted data.	O.LKM	This threat is mitigated by O.LKM, which requires that the TSF must provide a centralized service that is able to send and receive keys and other security attributes from TOE appliances.

4	T.Misconfiguration Missing security management functionality may hinder effective management of the TSF and allow attackers to gain unauthorized access to resources protected by the TOE.	O.Audit OE.Audit O.SecMan O.Time OE.Time	This threat is mitigated by the ability of the TOE to provide adequate management interfaces for the DataFort appliance (O.SecMan). Additionally, changes to critical configuration settings are audited allowing for detection of administrative errors (O.Audit and OE.Audit). O.Time and OE.Time support the audit function by providing reliable time stamps.
5	T.SelPro An unauthorized person may read, modify, or destroy security critical TOE configuration data.	O.SelPro OE.SelPro O.Crypto O.CryptoShred	This threat is mitigated by preventing bypass or deactivation of TOE security functions through the protection mechanisms of both the TOE and the IT Environment (O.SelPro and OE.SelPro.) Cryptographic algorithms (O.Crypto) provide support for the protection of TSF data. O.CryptoShred provides for the zeroization of cryptographic keys.
6	T. Spoof An unauthorized person or IT entity may attempt to access the TOE, and thereby disable security functionality, tamper with TSF code and data, or subvert security settings.	O.IDAuth OE.IDAuth O.Crypto	This threat is mitigated by requiring the authentication of users and IT entities. (O.IDAuth and OE.IDAuth). Cryptographic algorithms (O.Crypto) support the authentication of IT entities.
7	T.Transmission An attacker may gain access to TSF data when it is transmitted between the DataFort and the Management Station, LKM Server, and other DataForts.	O.Transmission OE.Transmission O.Crypto	This threat is mitigated by protecting communications channels (O.Transmission and OE.Transmission). Cryptographic algorithms (O.Crypto) provide support for the protection of communications channels.
8	T.Undetectable Administrators may make errors in the management of the TOE that are undetectable unless they are audited. A configuration error may leave the TOE vulnerable to attack by an unauthorized user.	O.Audit OE.Audit O.Time OE.Time O.Crypto	This threat is mitigated by auditing security relevant events (O.Audit and OE.Audit.) Reliable time stamps are applied to audit records and allow the reconstruction of a sequence of events at a later date (O.Time and OE.Time). Cryptographic algorithms (O.Crypto) provide support for user authentication and protection of audit logs in the IT environment.

8.1.2 Organizational Security Policies

There are no Organizational Security Policies that must be met by the TOE.

8.1.3 Assumptions

The Table below shows that each identified assumption is countered by a least one Non-IT Environment objective.

Table 8-2: All Assumptions Countered

Item	Assumption ID	Non-IT Objective Addressing Assumption	Rationale
1	A.Admin Administrators are non-hostile, appropriately trained and follow all administrator guidance.	ON.Admin	The assumption is addressed by the ON.Admin objective which requires that those responsible for the TOE must ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
2	A.Configure The TOE is properly configured as described in the guidance documentation.	ON.Configure	This assumption is addressed by the ON.Configure objective, which requires that those responsible for the TOE must ensure that the TOE is properly configured in accordance with the administrator guidance.
3	A.NoUntrusted There are no untrusted users and no untrusted software on the Management station and LKM Server	ON.NoUntrusted	This assumption is addressed by the ON.NoUntrusted objective, which requires that those responsible for the TOE must ensure that there are no untrusted users and no untrusted software on the Management station, LKM Server, and hosts on which DHA authentication software is installed.
4	A.PhysicalTamper Opening the chassis sends a tamper notification signal to the SEP cryptographic module.	ON.PhysicalTamper	This assumption is addressed by the ON.PhysicalTamper objective, which requires that the developer must ensure that the capabilities for the detection of physical tampering are adequately tested.

Item	Assumption ID	Non-IT Objective Addressing Assumption	Rationale
5	A.SmartCard Each Smart Card is provided to the correct individual user. In addition, holders of Recovery Cards, System Cards, and Admin Cards ensure that the cards are kept in a secure location and used only in accordance with NetApp user guidance.	ON.SmartCard	This assumption is addressed by the ON.SmartCard objective. ON.SmartCard requires that Administrators bring their cards to the Management Station in order to allow for authentication. ON.SmartCard also protects the cards against compromise, strengthening the integrity of the smart card authentication mechanism.
6	A.ProtectComm Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote IT entities are via a secure channel.	ON.ProtectComm	This assumption is addressed by the ON.ProtectComm objective. ON.ProtectComm requires that communications between the TOE components and between the TOE components and remote IT entities are secured.

8.1.4 All Objectives Necessary

The following two tables show that there are no unnecessary security objectives for the TOE or the IT Environment, since each objective addresses at least one threat, policy or secure usage assumption.

Table 8-3: Reverse Mapping TOE Security Objectives

Item	TOE Objective	Assumption/Threat/Policy
1	O.Audit	T.Misconfiguration T.Undetectable
2	O.Crypto	T.Disclosure T.SelPro T.Spoof T.Transmission T.Undetectable
3	O.CryptoShred	T.Disclosure T.SelPro
4	O.FaultTolerance	T.Disruption
5	O.IDAuth	T.Spoof

Item	TOE Objective	Assumption/Threat/Policy
6	O.IFC	T.Disclosure
7	O.LKM	T.KeyLoss
8	O.SecMan	T.Misconfiguration
9	O.SelPro	T.SelPro
10	O.Time	T.Misconfiguration T.Undetectable
11	O.Transmission	T.Transmission

Table 8-4: Reverse Mapping IT Environment Security Objectives

Item	Security Objective for Environment	Assumption/Threat/Policy
1E	OE.Audit	T.Misconfiguration T.Undetectable
2E	OE.IDAuth	T.Spoof
3E	OE.SelPro	T.SelPro
4E	OE.Time	T.Misconfiguration T.Undetectable
5E	OE.Transmission	T.Transmission
6E	ON.ProtectComm	A.ProtectComm
1N	ON.Admin	A.Admin
2N	ON.Configure	A.Configure
3N	ON.NoUntrusted	A.NoUntrusted
4N	ON.PhysicalTamper	A.PhysicalTamper
5N	ON.SmartCard	A.SmartCard

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements for the TOE

The table below shows that all of the security objectives for the TOE are satisfied by at least one security functional requirement (SFR).

Table 8-5: All Objectives for the TOE Met by Functional Requirements for the TOE

Item	Objective ID	SFR(s)	Rationale
1	O.Audit The TOE must provide a means to accurately detect and record security-relevant events in audit records. Audit records stored on the TOE must be protected from unauthorized modification.	FAU_GEN.1 FAU_STG_EXP.1 FCS_COP_EXP.5	An audit record can be generated for security-relevant events (FAU_GEN.1) The TOE is able to protect audit records stored internally (FAU_STG_EXP.1). FCS_COP_EXP.5 specifies the signing of audit records, so that modifications can be detected.

Item	Objective ID	SFR(s)	Rationale
2	O.Crypto The TSF must provide cryptographic operations to support user data protection, identification and authentication, and protection of TSF data and their associated key management functions.	FCS_CKM.1-AES FCS_CKM.1-RSA FCS_CKM.1-3DES FCS_CKM.4 FCS_CKM_EXP.5 FCS_CKM_EXP.6 FCS_CKM_EXP.7 FCS_CKM_EXP.8 FCS_COP.1-AES FCS_COP.1-RSA FCS_COP.1-3DES FCS_COP_EXP.1 FCS_COP_EXP.2 FCS_COP_EXP.3 FCS_COP_EXP.4 FCS_COP_EXP.5	This objective is met by the cryptographic support class (FCS) of SFR components. FCS_COP.1-AES, FCS_COP.1-RSA, FCS_COP.1-3DES specify encryption and decryption. FCS_CKM_EXP.5 (DH), FCS_CKM_EXP.6 (ECCDH), FCS_COP.1-RSA and FCS_COP_EXP.4 (AKEP2) specify authentication. FCS_COP_EXP.5 specifies audit log signing. Supporting cryptographic functions are provided by FCS_COP_EXP.1 (HMAC_SHA), FCS_COP_EXP.2 (PRNG), and FCS_COP_EXP.3 (SHA). FCS_CKM.1-AES, FCS_CKM.1-RSA, FCS_CKM.1-3DES specify key generation. Individual keys may be zeroized within either the LKM or DataFort appliance, or the entire appliance may be zeroized (FCS_CKM.4). Key agreement is specified by FCS_CKM_EXP.5 (DH) and FCS_CKM_EXP.6 (ECCDH). FCS_CKM_EXP.7 and FCS_CKM_EXP.8 specifying wrapping of keys on export and key import respectively.
3	O.CryptoShred The TOE must provide mechanisms to efficiently destroy key material in accordance with an administrator-specified policy.	FCS_CKM.4	This objective is satisfied using cryptographic destruction of cryptographic keys (FCS_CKM.4). Note that destruction may occur by deleting a specific key, or by zeroization of the entire TOE appliance.

Item	Objective ID	SFR(s)	Rationale
4	O.FaultTolerance The TOE must provide fault tolerance of information flow control and data encryption/decryption services, ensuring continuation of service due to fibre channel link failure, or failure of a cluster member.	FPT_RCV.4 FPT_FLS.1	This objective is met by utilizing the TOE in a redundant configuration. In the case of failure of one TOE appliance, the redundant TOE appliance(s) will ensure that information flow control policies continue to be met, and data encryption/decryption services are maintained (FPT_RCV.4, FPT_FLS.1).
5	O.IDAuth The TSF must provide identification and authentication for users and IT entities.	FIA_EAU_EXP.5 FIA_EID_EXP.1 FIA_UAU_EXP.5 FIA_UID_EXP.2 FCS_COP_EXP.5 FCS_COP.1-RSA FCS_COP_EXP.4	This objective is met with the inclusion of multiple authentication mechanisms within the TOE, as well as the prevention of information flows and services before successful authentication occurs (FIA_EAU_EXP.5, FIA_EID_EXP.1, FIA_UAU_EXP.5, FIA_UID_EXP.2). FCS_COP_EXP.5 (DH), FCS_COP.1-RSA, and FCS_COP_EXP.4 (AKEP2) provide cryptographic support for the identification and authentication of IT entities.
6	O.IFC The TOE must be able to control information flows between distributed clients and centralized storage devices.	FDP_IFC.1 FDP_IFF.1 FCS_COP.1-AES	The objective is met by the Information flow control SFRs (FDP_IFC.1, FDP_IFF.1), describing the SCSI data protection policy. The information flow policy is implementing using AES for encryption/decryption (FCS_COP.1-AES)

Item	Objective ID	SFR(s)	Rationale
7	O.LKM The TOE must provide a centralized service that is able to send and receive keys and other security attributes from TOE appliances.	FMT_MTD.1 FMT_MOF.1 FMT_SMF.1 FCS_CKM_EXP.7	This requirement is met by the management of functions capabilities assigned to the LKM Operator (FMT_MOF.1, FMT_SMF.1), as well as the LKM Operator's ability to manage TSF data by the importing and export of Cryptainer keys and database backups between the LKM and DataFort as described in FMT_MTD.1. Note that in most cases, both the LKM Operator and the DataFort Administrator are required to approve TSF data sharing between the LKM and the TOE. FCS_CKM_EXP.7 requires that keys must be wrapped using AES when they are transmitted between distributed components of the TOE or to other DataForts.

Item	Objective ID	SFR(s)	Rationale
8	O.SecMan The TOE must provide a means for an administrator to manage the TOE security functions.	FMT_MTD.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FMT_MOF.1	This objective is met by supporting multiple management roles (FMT_SMR.1), and ensuring that the TOE security attributes may only be modified by an appropriate administrator (FMT_MSA.1, FMT_SMF.1). In addition, the TOE ensures that only secure values are accepted for security attributes (FMT_MSA.2). The TOE initializes all security attributes enforcing the SFP to default values (FMT_MSA.3), and allows for the appropriate management of functions for each role (FMT_MOF.1), and TSF data within each function (FMT_MTD.1).

Item	Objective ID	SFR(s)	Rationale
9	O.SelPro The TSF must maintain a domain for its own execution that protects itself and its resources from attempts by unauthorized users to bypass, deactivate, or tamper with its security functions through its own interfaces.	FAU_STG_EXP.1 FCS_CKM_EXP.7 FCS_COP.1-AES FCS_COP.1-RSA FCS_COP.1-3DES FCS_COP_EXP.5 FPT_RVM_EXP.1 FPT_SEP_EXP.1 FTP_ITC_EXP.1	FPT_SEP_EXP.1 provides for protection of the TSF against external users by maintaining a security domain for its own execution that protects it from interference and tampering by untrusted subjects, as well as by differentiating between subjects in the TSC. This is achieved by means of kernel protection mechanisms, and the association of security attributes to subjects. This objective is also met by the FPT_RVM_EXP.1 requirement, which provides for non-bypassability of the TOE FTP_ITC_EXP.1 provides for the protection TSF data from unauthorized disclosure or modification when it is being transmitted between the TOE and a remote trusted IT entity. FCS_CKM_EXP.7 specifies that keys must be wrapped using AES when they are transmitted between distributed components of the TOE or to other DataForts. FCS_COP.1-AES, FCS_COP.1-RSA, and FCS_COP.1-3DES provide cryptographic support for the protection of TSF data. FAU_STG_EXP.1 specifies that audit records are protected while they are stored within the TSF. FCS_COP_EXP.5 specified the signing of audit logs.

Item	Objective ID	SFR(s)	Rationale
10	O.Time The DataFort must provide a reliable clock to maintain the system time.	FPT_STM_EXP.1	This objective is met by FPT_STM_EXP.1 which requires that the TSF acquire time from an NTP Server in the IT environment and maintain the time reliably for its own use.
11	O.Transmission The TSF must protect TSF data from disclosure or modification when it is transmitted between the DataFort and the Management Station, the LKM Server, and other DataForts.	FTP_ITC_EXP.1 FCS_CKM_EXP.5 FCS_CKM_EXP.6 FCS_CKM_EXP.7 FCS_CKM_EXP.8 FCS_COP.1-AES FCS_COP.1-RSA FCS_COP.1-3DES FCS_COP_EXP.4	FTP_ITC_EXP.1 requires cryptographic based communications protocols between distributed components of the TOE, other DataForts, and the Management station in the IT environment. FCS_CKM_EXP.7 and FCS_CKM_EXP.8 require that keys be wrapped using AES for encryption when they are transmitted between distributed components of the TOE or to other DataForts. DH (FCS_CKM_EXP.5), ECCDH (FCS_CKM_EXP.6), AES (FCS_COP.1-AES), RSA (FCS_COP.1-RSA) , 3DES (FCS_COP.1 3DES) , and AKEP2 (FCS_COP_EXP.4) are the underlying cryptographic algorithms that support the trusted channels.

Table 8-6: Reverse Mapping of TOE SFRs to Objectives

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1	O.Audit
2	FAU_STG_EXP.1	O.Audit
		O.SelPro
3	FCS_CKM.1-AES	O.Crypto
4	FCS_CKM.1-RSA	O.Crypto
5	FCS_CKM.1-3DES	O.Crypto

Item	SFR ID	TOE Security Objective
6	FCS_CKM.4	O.Crypto
		O.CryptoShred
7	FCS_CKM_EXP.5	O.Crypto
		O.IDAuth
		O.Transmission
8	FCS_CKM_EXP.6	O.Crypto
		O.Transmission
9	FCS_CKM_EXP.7	O.Crypto
		O.LKM
		O.SelPro
		O.Transmission
10	FCS_CKM_EXP.8	O.Crypto
		O.Transmission
11	FCS_COP.1-AES	O.Crypto
		O.IFC
		O.SelPro
		O.Transmission
12	FCS_COP.1-RSA	O.Crypto
		O.IDAuth
		O.SelPro
		O.Transmission
13	FCS_COP.1-3DES	O.Crypto
		O.SelPro
		O.Transmission
14	FCS_COP_EXP.1	O.Crypto
15	FCS_COP_EXP.2	O.Crypto
16	FCS_COP_EXP.3	O.Crypto
17	FCS_COP_EXP.4	O.Crypto
		O.IDAuth
		O.Transmission
18	FCS_COP_EXP.5	O.Audit
		O.Crypto
		O.SelPro
19	FDP_IFC.1	O.IFC
20	FDP_IFF.1	O.IFC
21	FIA_EAU_EXP.5	O.IDAuth
22	FIA_EID_EXP.1	O.IDAuth
23	FIA_UAU_EXP.5	O.IDAuth
24	FIA_UID_EXP.2	O.IDAuth
25	FMT_MOF.1	O.LKM
		O.SecMan

Item	SFR ID	TOE Security Objective
26	FMT_MSA.1	O.SecMan
27	FMT_MSA.2	O.SecMan
28	FMT_MSA.3	O.SecMan
29	FMT_MTD.1	O.LKM
		O.SecMan
30	FMT_SMF.1	O.LKM
		O.SecMan
31	FMT_SMR.1	O.SecMan
32	FPT_FLS.1	O.FaultTolerance
33	FPT_RCV.4	O.FaultTolerance
34	FPT_RVM_EXP.1	O.SelPro
35	FPT_SEP_EXP.1	O.SelPro
36	FPT_STM_EXP.1	O.Time
37	FTP_ITC_EXP.1	O.SelPro
		O.Transmission

Note: This table has been provided for completeness to show that all security functional requirements map to at least one TOE Security Objective.

8.2.2 Security Functional Requirements for the IT Environment

Table 8-7 below shows that all of the security objectives for the IT Environment are satisfied.

Table 8-7: All Objectives for the IT Environment Met by Functional Requirements

Item	Objective	Requirement for the IT Environment	Rationale
1E	OE.Audit The IT environment must provide a long term audit store for the TOE.	FAU_STG_ENV.1	This objective is met by FAU_STG_ENV.1, which specifies that the operating environment be provided with a log repository.

Item	Objective	Requirement for the IT Environment	Rationale
2E	OE.IDAuth The IT environment must support identification and authentication of users and IT entities.	FIA_EAU_ENV.2 FIA_EID_ENV.2 FIA_UAU_ENV.5 FIA_UID_ENV.2	This objective is met by FIA_EAU_ENV.2 and FIA_EID_ENV.2, which specify the requirements for entity identification and authentication and FIA_UAU_ENV.5 and FIA_UID_ENV.2, which specify the requirements for user identification and authentication in the IT environment.
3E	OE.SelPro The IT environment must protect the TOE against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	FAU_STG_ENV.1 FPT_RVM_ENV.1 FPT_SEP_ENV.1 FTP_ITC_ENV.1	This objective is met by FAU_STG_ENV.1, which specifies that the IT Environment will provide protection to the audit records from unauthorized modification and deletion, FPT_RVM_ENV.1 which provides for non-bypassability of security functions, FPT_SEP_ENV.1, which specifies protection of the TSF code and data, and by FTP_ITC_ ENV.1, which specifies that the Management Station in the IT environment will support TLSv1.
4E	OE.Time The IT environment must be configured with an NTP server that is able to provide a reliable clock to the TOE.	FPT_STM_ENV.1	This objective is met by FPT_STM_ENV.1, which requires that the IT environment to supply time stamps to the TOE.
5E	OE.Transmission The Management Station in the IT environment must initiate a TLSv1 session for communications with the TOE.	FTP_ITC_ENV.1	This objective is met by FTP_ITC_ENV.1, which requires the management station in the IT environment initiate a TLS session for communications with the TOE.

Table 8-8: Reverse Mapping of IT Environment SFRs to Objectives

Item	Environment SFR ID	Environment Security Objectives
1E	FAU_STG_ENV.1	OE.Audit OE.SelPro
2E	FIA_EAU_ENV.2	OE.IDAuth
3E	FIA_EID_ENV.2	OE.IDAuth
4E	FIA_UAU_ENV.5	OE.IDAuth
5E	FIA_UID_ENV.2	OE.IDAuth
6E	FPT_RVM_ENV.1	OE.SelPro
7E	FPT_SEP_ENV.1	OE.SelPro
8E	FPT_STM_ENV.1	OE.Time
9E	FTP_ITC_ENV.1	OE.SelPro OE.Transmission

Note: This table has been provided for completeness to show that all IT Environment Security Functional Requirements map to at least one IT Environment Security Objective.

8.2.3 Dependencies

Table 8-9 and

Table 8-10 below show the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by hierarchical components are denoted by an (H) following the dependency reference. An (E) following the dependency reference designates that the SFR is for the IT Environment. EAL4 in the Item Reference column means that the dependency is satisfied by an EAL4 assurance requirement. An (H) after the reference indicates that the SFR claimed in the ST is hierarchical to the dependency.

Table 8-9: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM_EXP.1 FPT_STM_ENV.1	36 8E
2	FAU_STG_EXP.1	Protected audit trail storage	FAU_GEN.1	1
3	FCS_CKM.1-AES	Cryptographic key generation: AES	FCS_CKM.4 FCS_COP.1-AES FCS_COP_EXP.2 FMT_MSA.2	6 11 15 27

Item	SFR ID	SFR Title	Dependencies	Item Reference
4	FCS_CKM.1-RSA	Cryptographic key generation: RSA	FCS_CKM.4 FCS_COP.1-RSA FCS_COP_EXP.2 FMT_MSA.2	6 12 15 27
5	FCS_CKM.1-3DES	Cryptographic key generation: 3DES	FCS_CKM.4 FCS_COP.1-3DES FCS_COP_EXP.2 FMT_MSA.2	6 13 15 27
6	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1-* FCS_CKM_EXP.8 FTM_MSA.2	3, 4, 5 10 27
7	FCS_CKM_EXP.5	Cryptographic key agreement: DH	FCS_CKM.4 FCS_COP.1-AES	6 11
8	FCS_CKM_EXP.6	Cryptographic key agreement: ECCDH	FCS_CKM.4 FCS_COP.1-AES FCS_COP_EXP.1	6 11 14
9	FCS_CKM_EXP.7	Cryptographic key export	FCS_CKM.4 FCS_COP.1-AES FCS_COP_EXP.1	6 11 14
10	FCS_CKM_EXP.8	Cryptographic key import	FCS_CKM.4 FCS_COP.1-AES FCS_COP_EXP.1	6 11 14
11	FCS_COP.1-AES	Cryptographic operation: AES	FCS_CKM.1-AES FCS_CKM_EXP.7 FCS_CKM_EXP.8 FCS_CKM.4 FMT_MSA.2	3 9 10 6 27
12	FCS_COP.1-RSA	Cryptographic operation: RSA	FCS_CKM.1-RSA FCS_CKM.4 FMT_MSA.2	4 6 27
13	FCS_COP.1-3DES	Cryptographic operation: 3DES	FCS_CKM.1-3DES FCS_CKM.4 FMT_MSA.2	5 6 27
14	FCS_COP_EXP.1	Cryptographic operation: HMAC-SHA	FCS_COP_EXP.3	16

Item	SFR ID	SFR Title	Dependencies	Item Reference
15	FCS_COP_EXP.2	Cryptographic operation: PRNG	FCS_CKM.1-AES FCS_CKM.1-RSA FCS_CKM.1-3DES FCS_CKM_EXP.6 FCS_COP_EXP.4	3 4 5 8 17
16	FCS_COP_EXP.3	Cryptographic operation: SHA	None	N/A
17	FCS_COP_EXP.4	Cryptographic operation: AKEP2	None	N/A
18	FCS_COP_EXP.5	Cryptographic operation: Audit Log Signing	None	N/A
19	FDP_IFC.1	Subset information flow control	FDP_IFF.1	20
20	FDP_IFF.1	Simple security attributes	FDP_IFC.1 FMT_MSA.3	19 28
21	FIA_EAU_EXP.5	IT entity authentication mechanisms	None	N/A
22	FIA_EID_EXP.1	Partial IT entity timing of identification	None	N/A
23	FIA_UAU_EXP.5	Multiple authentication mechanisms	None	N/A
24	FIA_UID_EXP.2	User identification before any action	None	N/A
25	FMT_MOF.1	Management of security functions behavior	FMT_SMF.1 FMT_SMR.1	30 31
26	FMT_MSA.1	Management of security attributes	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	18 30 31
27	FMT_MSA.2	Secure security attributes	ADV_SPM.1 FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	EAL4 19 26 31
28	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	26 31
29	FMT_MTD.1	Management of TSF data	FMT_SMF.1 FMT_SMR.1	30 31
30	FMT_SMF.1	Specification of Management Functions	None	N/A
31	FMT_SMR.1	Security roles	FIA_UID.1	24(H)
32	FPT_FLS.1	Failure with preservation of secure state	ADV_SPM.1	EAL4

Item	SFR ID	SFR Title	Dependencies	Item Reference
33	FPT_RCV.4	Function recovery	ADV_SPM.1	EAL4
34	FPT_RVM_EXP.1	Non-bypassability of the TSP	None	N/A
35	FPT_SEP_EXP.1	Partial TSF domain separation	None	N/A
36	FPT_STM_EXP.1	Partial reliable time stamps	None	N/A
37	FTP_ITC_EXP.1	Partial trusted channels	None	N/A

Table 8-10: IT Environment Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1E	FAU_STG_ENV.1	Protected audit trail storage	FAU_GEN.1	1
2E	FIA_EAU_ENV.2	IT entity authentication before any action	None	N/A
3E	FIA_EID_ENV.2	IT entity identification before any action	None	N/A
4E	FIA_UAU_ENV.5	Multiple authentication mechanisms	None	N/A
5E	FIA_UID_ENV.2	User identification before any action	None	N/A
6E	FPT_RVM_ENV.1	Partial non-bypassability of the TSP	None	N/A
7E	FPT_SEP_ENV.1	Partial TSF domain separation	None	N/A
8E	FPT_STM_ENV.1	Partial Reliable time stamps	None	N/A
9E	FTP_ITC_ENV.1	Trusted channel - management station	None	N/A

All dependencies for SFRs in both the TOE and IT environment have been met.

8.2.4 Mutual Support Rationale

The IT Security Requirements are mutually supportive. All dependencies of the IT security requirements are satisfied. In addition, FPT_RVM_EXP.1 and FPT_RVM_ENV.1 together prevent bypassing of other security functional requirements. FPT_SEP_EXP.1 and FPT_SEP_ENV.1 prevent tampering with other security

functional requirements. FMT_MOF.1 and FMT_MTD.1 ensure that only authorized administrators can perform TSF management functions and prevent de-activation of other security functional requirements. FAU_GEN.1, FAU_STG_EXP.1, and FAU_STG_ENV.1 enable detection of attacks aimed at defeating other security functional requirements.

8.2.5 Internal Consistency Rationale

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements.

8.2.6 Strength of Function Rationale

Strength of function claim of SOF-medium is required to withstand attackers with a moderate attack potential. The TOE is designed to withstand an attack potential of moderate. SOF-medium is consistent with a vulnerability analysis requirement of AVA_VLA.2.

The only probabilistic or permutational mechanisms within the TOE are passwords and password based authentication protocols. The SOF claim applies to the IA-1 and IA-2 security functions.

8.2.7 Assurance Requirements Rationale

The assurance level selected for the TOE is EAL4 augmented with ALC_FLR.1 because it provides appropriate assurance measures for the expected application of the product.

EAL 4 ensures a product that is methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It also requires a moderate to high level of independently assured security.

ALC_FLR.1 is an augmentation to the EAL4 requirements. ALC_FLR.1 is included to add assurance for flaw remediation that is a standard part of a product's life cycle.

8.2.8 Explicitly Stated Requirements Rationale

FAU_STG_EXP.1 and FAU_STG_ENV.1 are explicitly stated to account for the fact that the TOE maintains only a limited audit store internally, and relies on an external log repository for long term audit storage. Therefore protection of the audit records depends upon both the TOE's own protection mechanisms and those of the IT Environment.

FCS_CKM_EXP.5 and FCS_CKM_EXP.6 are explicitly stated to specify the DH and

ECCDH key agreement algorithms. CC Part 2 does not contain an SFR in the FCS_CKM key management family for key establishment, which is a distinctly different process than key generation.

FCS_CKM_EXP.7 is explicitly stated to specify key export. CC Part 2 does not contain an SFR in the FCS_CKM key management family for key export.

FCS_CKM_EXP.8 is explicitly stated to address importing cryptographic keys. Using FDP_ITC is not appropriate for this TOE, because all the keys are TSF data.

FCS_COP_EXP.1, FCS_COP_EXP.2, FCS_COP_EXP.3, and FCS_COP_EXP.4 are explicitly stated to specify HMAC-SHA, PRNG, SHA, and AKEP2 cryptographic algorithms, since these algorithms are specified by properties other than key size.

FCS_COP_EXP.5 is explicitly stated to specify signing of audit logs, since an equivalent SFR is not available in CC Part 2.

FIA_EAU_EXP.5, FIA_EID_EXP.1, FIA_EAU_ENV.2, and FIA_EID_ENV.2 are explicitly stated to address IT entity authentication as opposed to the FIA_UAU and FIA_UID families, which are for user authentication and use different mechanisms.

FIA_UAU_EXP.5, FIA_UID_EXP.2, FIA_UAU_ENV.5, and FIA_UID_ENV.2 are explicitly stated due to user identification and authentication being provided partially by the TOE and partially by the IT environment.

FPT_RVM_EXP.1, FPT_RVM_ENV.1, FPT_SEP_EXP.1 and FPT_SEP_ENV.1 are explicitly stated because the functionality is provided partially by the TOE and partially by the IT environment. The TOE components running on the LKM Server and the Management Station are software only and cannot protect themselves or enforce non-bypassability without the support of the underlying platform

FPT_STM_EXP.1 and FPT_STM_ENV.1 are explicitly stated because the functionality is provided partially by the TOE and partially by the IT environment. The TOE obtains the time from an NTP server in the IT environment. However, the DataFort platform must maintain the time for the use of other TSF functions. Similarly, the underlying platforms for the LKM Server and the Management Station in the IT environment maintain the time for the use of the LKM Software and the WebUI respectively.

FTP_ITC_EXP.1 and FTP_ITC_ENV.1 are explicitly stated because the functionality is provided partially by the TOE and partially by the IT environment. Also, sometimes the trusted channel is between distributed components of the TOE (DataFort appliance and LKM_TOE software, sometimes between TOE copies (Clustered DataForts, DataFort trustees), and sometimes between the TOE and the IT environment (Management Station).

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

The table below shows that the IT security functions in the TOE Summary Specification (TSS) implement all of the TOE Security Functional Requirements.

All security functions are defined in section 6, in which a mapping is provided from Security Functions to SFRs. This section contains a reverse mapping, indicating that all the security functional requirements are necessary for the TSF to meet the specified security requirements.

Table 8-11: SFR to Security Function Mapping and Rationale

#	SFR ID/Title	TSF ID/Title	Rationale
1	FAU_GEN.1 Audit data generation	AU-1 Audit Data Generation	Specifies how audit records are generated by the TOE wand what data fields are contained in each record.
2	FAU_STG_EXP.1 Partial protected audit trail storage	AU-2 Audit Data Storage & Protection	Specifies how audit records are stored and protected by the TOE.
3	FCS_CKM.1-AES Cryptographic key generation: AES	CS-1 Cryptographic Key Generation	Specifies how cryptographic keys are generated
4	FCS_CKM.1-RSA Cryptographic key generation: RSA	CS- 1 Cryptographic Key Generation	Specifies how cryptographic keys are generated
5	FCS_CKM.1-3DES Cryptographic key generation: 3DES	CS-1 Cryptographic Key Generation	Specifies how cryptographic keys are generated
6	FCS_CKM.4 Cryptographic key destruction	CS-2 Cryptographic Key Destruction	Specifies how the TOE zeroizes keys as requested by an administrator or as specified as a result of a time based zeroization policy.
7	FCS_CKM_EXP.5 Cryptographic key agreement: DH	CS-3 Cryptographic Key Agreement	Specifies the Diffie-Hellmann (DH) algorithm.
8	FCS_CKM_EXP.6 Cryptographic key agreement: ECCDH	CS-3 Cryptographic Key Agreement	Specifies the Elliptic Curve Diffie Hellman (ECCDH) algorithm.
9	FCS_CKM_EXP.7 Cryptographic key export	CS-4 Cryptographic Key Export	Specifies the wrapping of exported cryptographic keys

#	SFR ID/Title	TSF ID/Title	Rationale
10	FCS_CKM_EXP.8 Cryptographic key import	CS-5 Cryptographic Key Import	Specifies that AES-wrapped cryptographic keys are imported into the TSF.
11	FCS_COP.1-AES Cryptographic operation: AES	CS-6 Advance Encryption Standard (AES)	Specifies the Advance Encryption Standard (AES) algorithm.
12	FCS_COP.1-RSA Cryptographic operation: RSA	CS-7 Rivest Shamir Adelman (RSA)	Specifies the Rivest Shamir Adelman (RSA) algorithm.
13	FCS_COP.1-3DES Cryptographic operation: 3DES	CS-8 Triple Data Encryption Standard (3DES)	Specifies the Triple Data Encryption Standard (3DES) algorithm.
14	FCS_COP_EXP.1 Cryptographic operation: HMAC-SHA	CS-9 Keyed Hash Message Authentication Code (HMAC-SHA)	Specifies the Keyed Hash Message Authentication Code (HMAC-SHA) algorithm.
15	FCS_COP_EXP.2 Cryptographic operation: PRNG	CS-10 Pseudo Random Number Generator (PRNG)	Specifies the Pseudo Random Number Generator (PRNG)
16	FCS_COP_EXP.3 Cryptographic operation: SHA	CS-11 Secure Hash (SHA)	Specifies the Secure Hash (SHA) algorithm
17	FCS_COP_EXP.4 Cryptographic operation: AKEP2	CS-12 Authenticated Key Exchange Protocol (AKEP2)	Specifies the Authenticated Key Exchange Protocol (AKEP2)
18	FCS_COP_EXP.5 Cryptographic operation: Audit Log Signing	CS-13 Audit Log Signing	Specifies that audit logs are digitally signed.
19	FDP_IFC.1 Subset information flow control	IFC-1 Information Flow Control Enforcement	Specifies how the SCSI data protection policy is enforced. This security function acts as a proxy to SCSI traffic, applying information flow rules.
20	FDP_IFF.1 Simple security attributes	IFC-1 Information Flow Control Enforcement	Specifies the subject, information and operation attributes used by the SCSI data protection policy. Also specifies the rules used to enforce the policy.

#	SFR ID/Title	TSF ID/Title	Rationale
21	FIA_EAU_EXP.5 IT entity authentication mechanisms	IA-2 IT Entity Identification and Authentication	Specifies the multiple user authentication mechanisms provided by the TOE and when each is used.
22	FIA_EID_EXP.1 Partial IT entity timing of identification	IA-2 IT Entity Identification and Authentication	Specifies that IT entities must be identified before being allowed access to the TSF and TSF data.
23	FIA_UAU_EXP.5 Multiple authentication mechanisms	IA-1 User Identification and Authentication	Specifies the multiple user authentication mechanisms provided by the TOE and when each is used.
24	FIA_UID_EXP.2 Partial user identification before any action	IA-1 User Identification and Authentication	Specifies that users must be identified before being allowed access to the TSF and TSF data.
25	FMT_MOF.1 Management of security functions behavior	SM-1 Management Functions	Specifies how the management functions for DataFort key backup and learning modes can be modified.
26	FMT_MSA.1 Management of security attributes	SM-3 Information Flow Control Management	Specifies the security attributes used to enforce the SCSI Data Protection policy that can be modified.
27	FMT_MSA.2 Secure security attributes	SM-3 Information Flow Control Management	Specifies the secure values for the security attributes used to enforce the SCSI Data Protection policy.
28	FMT_MSA.3 Static attribute initialization	SM-3 Information Flow Control Management	Specifies the default values for the security attributes used to enforce the SCSI Data Protection policy.
29	FMT_MTD.1 Management of TSF data	SM-4 TSF Data Management	Specifies the operations allowed on TSF data and which roles may perform those operations.
30	FMT_SMF.1 Specification of Management Functions	SM-1 Management Functions	Specifies the management functions available to the administrative users of the TOE.
31	FMT_SMR.1 Security roles	SM-2 Administrative Roles	Specifies the administrative roles assigned to users of the TOE and how each is authenticated.

#	SFR ID/Title	TSF ID/Title	Rationale
32	FPT_FLS.1 Failure with preservation of secure state	SP-2 Fault tolerance	Specifies the types of failures for which the TOE preserves a secure state.
33	FPT_RCV.4 Function recovery	SP-2 Fault tolerance	Specifies the failure scenarios from which the TSF can recover.
34	FPT_RVM_EXP.1 Partial non-bypassability of the TSP	SP-1 Self-Protection	Specifies how reference mediation is achieved by the SCSI proxy, in that it intercepts SCSI commands and forwards them to targets.
35	FPT_SEP_EXP.1 Partial TSF domain separation	SP-1 Self-Protection	Specifies how domain separation is achieved by both the SEP, which contains its own security domain that allows it to handle keys in plaintext, and by the DataFort TOE code outside of the SEP, which protects against unauthorized tampering.
36	FPT_STM_EXP.1 Partial reliable time stamps	SP-3 Time	Specifies that DataFort's clock maintain the system time for the use of the TSF after it has been set from an NTP server.
37	FTP_ITC_EXP.1 Partial trusted channels	TC-1 Trusted channel	Specifies that TSF data will be protected from unauthorized disclosure or modification when it is transmitted between the TOE and another trusted remote IT product.

8.3.2 Assurance Measures Rationale

Section 6.2 lists the documents provided to address each of the assurance requirements. The tables in Section 6.2 show that all the assurance requirements are addressed.

8.4 PP Claims Rationale

This section is not applicable. There are no PP claims.

9 References

NetApp Documentation

NetApp, *Decru DataFort™ SAN SEP 2.0 Security Policy,* January 25, 2007.

NetApp, *Decru Security Administration Guide, DataFort FC-Series,* Version 2.1

NetApp, *Administration Guide, Lifetime Key Management Tool*, Version 2.1

Fibre Channel specifications available from http://www.t11.org

SCSI-3 Fibre Channel Protocol (SCSI-FCP), X3.269:1996

Fibre Channel Physical and Signaling Interface (FC-PH) X3.230:1994

Fibre Channel 2nd Generation (FC-PH-2), X3.297:1 997

Third Generation Fibre Channel Physical and Signaling Interface (FC-PH-3) X3.303:1998,

Fibre Channel—Arbitrated Loop (FC-AL-2), working draft, revision 6.4, August 28, 1998

Fibre Channel Fabric Loop Attachment Technical Report (FC-FLA) NCITS/TR-20:1998

Fibre Channel—Private Loop Direct Attach Technical Report (FC-PLDA), NCITS/TR-19:1998

Fibre Channel Tape (FC-TAPE) profile, T11/99-069v4, revision 1.17, May 14, 1999

SCSI Fibre Channel Protocol-2 (FCP-2) working draft, revision 3, October 1, 1999

ANSI Information Technology—SCSI 3 Architecture Model, revision 18, November 27 1995

SCSI specifications available from http://www.t10.org:

SCSI Architectural Model (SAM, SAM-2)

SCSI Primary Commands (SPC, SPC-2, SPC-3)

SCSI Block Commands (SBC, SBC-2)

SCSI Stream Commands (SSC, SSC-2, SSC-3)

SCSI Media Changer Commands (SMC, SMC-2, SMC-3)

FIPS Cryptographic Standards available from http://csrc.nist.gov/publications/fips/index.html

Federal Information Processing Standard Publication FIPS PUB 146-3,

Federal Information Processing Standard Publication FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

Federal Information Processing Standard Publication FIPS PUB 180-2, *Secure Hash Standard*, August 1, 2002.

Federal Information Processing Standard Publication FIPS PUB 186-2*, Digital Signature Standard*, June 27, 2000

Federal Information Processing Standard Publication FIPS PUB 197, *Advanced Encryption Standard*, November 26, 2001

Federal Information Processing Standard Publication FIPS PUB 198, *The Keyed Hash Message Authentication Code*, March 6, 2002

NIST Special Publications 800 Series available from http://csrc.nist.gov/publications/nistpubs/index.html

NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.* March 2006

NIST Special Publication 800-57, *Recommendation for Key Management -- Part 1: General (Revised).* May 2006

Requests for Comment Standards available from www.ietf.org

RFC 2104, *Keyed Hashing for Message Authentication*

RFC 2246, *The TLS protocol, version 1.0*, January 1999

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, November 1998.

RFC 2409, *The Internet Key Exchange (IKE)*. November 1998.

RFC 2411, *IP Security Document Roadmap*

RFC 2631, *Diffie-Hellman Key Agreement Method*, June 1999.

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*, September 2003

RFC 4109, *Algorithms for Internet Key Exchange version 1 (IKEv1)*, May 2005.

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4304, *IP Encapsulating Security Payload (ESP)*

RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH),* December 2005.

RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*, April 2006.

X9 Series ANSI Standards available from www.X9.org

American National Standards Institute. American National Standard X9.17:

Financial Institution Key Management (Wholesale), 1985.

American National Standards Institute. American National Standard X9.31: *Digital Signatures Using Reversible Key Cryptography for the Financial Services Industry (rDSA),* September 1998.

American National Standards Institute. American National Standard X9.42: *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography,* November 2003,

American National Standards Institute. American National Standard X9.63-2001: *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography,* November 20, 2001.

[1] DataFort FC-Series Version 2.2.2, p. 37