National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

NetApp

Decru DataFort FC520v2, LKM 2.5.1

Report Number: **CCEVS-VR-VID10035-2009**

Dated: February 20, 2009
Version 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Daniel P. Faigin

The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Swapna Katikaneni
Deepak Somseula
Elise Berger
Dragua Zenelaj

CygnaCom Solutions (an Entrust Company)
McLean, Virginia

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of Decru DataFort FC520v2, LKM 2.5.1 was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 31 October 2008. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.3, Part 2 and Part 3, Evaluation Assurance Level (EAL 4), and the Common Methodology for IT Security Evaluation (CEM), Version 2.3.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL4) augmented with ALC_FLR.1, Basic Flaw Remediation have been met. This Validation Report is not an endorsement of the NetApp, Inc. product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is a NetApp Inc.'s product "Decru DataFort FC520v2, LKM 2.5.1". NetApp Inc. develops the product with the brand name "Decru DataFort™". The Decru DataFort™ FC520v2 is a fault- tolerant 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.

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.

Decru DataFort FC520v2, LKM 2.5.1 provides:

- **Security Audit** - Audit records are generated within the TOE for the specified security relevant events.

- **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.

- **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.

- **Identification and Authentication** - The TOE is capable of authenticating administrators, users, and IT entities.

- **Security Management** - The TOE supports multiple administrative roles to support separation of security management functions.

- **Protection of the TSF**- The TOE supports fault tolerant configurations in which DataFort appliances are clustered to provide for failover in case of link failure.

- **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 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. 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, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Additionally, 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. The non-approved algorithms, as well as the cryptography not covered by the FIPS certification have only been asserted as tested by the vendor.

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 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 2.1-1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The organizations and individuals participating in the evaluation.

Table 2.1-1 – Evaluation Identifiers

Evaluation Identifiers for NetApp, Inc. product Decru DataFort FC520v2, LKM 2.5.1	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Decru DataFort FC520v2, LKM 2.5.1

Evaluation Identifiers for NetApp, Inc. product Decru DataFort FC520v2, LKM 2.5.1	
Protection Profile	N/A
Security Target	Decru DataFort FC520v2, LKM 2.5.1 version 3.3, Oct 31 2008
Evaluation Technical Report	Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, Decru DataFort FC520v2, LKM 2.5.1, version 2.0, October 31 2008 Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE – Decru DataFort FC520v2, LKM 2.5.1, version 2.0, October 31 2008
Conformance Result	Common Criteria Version 2.3, Part 2 extended and Part 3 conformant, at Evaluation Assurance Level (EAL) 4, augmented with ALC_FLR.1, Basic Flaw Remediation
Version of CC	*Common Criteria for Information Technology Security Evaluatio*n, Version 2.3, August 2005
Version of CEM	*Common Evaluation Methodology for Information Technology Securit*y, Version 2.3, August 2005
Sponsor	NetApp, Inc. 1260 Crossman Avenue, Bldg 10, Sunnyvale, CA 94089
Developer	NetApp, Inc. 1260 Crossman Avenue, Bldg 10, Sunnyvale, CA 94089
Evaluator(s)	**Cygnacom Solutions** Swapna Katikaneni Deepak Somesula Elise Berger Dragua Zenelaj
Validator(s)	**NIAP CCEVS** Daniel Faigin (Lead) *The Aerospace Corporation*

Evaluation Identifiers for NetApp, Inc. product Decru DataFort FC520v2, LKM 2.5.1	
Keywords	Access Control, Encrypted Network Storage, Information Flow Control, Security Target, and Security Management

2.1 APPLICABLE INTERPRETATIONS

The evaluation team performed an analysis of the international and national (NIAP) interpretations regarding the CC and the CEM and determined that none were applicable.

3 SECURITY POLICY

The Decru DataFort FC520v2, LKM 2.5.1 TOE provides the following security services:

- Security Audit
- Cryptographic Support
- Identification & Authentication (I&A)
- Security Management
- Protection of the TSF
- TOE Session Establishment

Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

3.1 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. The DataFort must be configured to store log messages both in its internal database and to a remote syslog server.

3.2 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 DataForts 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, although they were deemed to be acceptable commercially available algorithms. These non-approved algorithms have not been analyzed or tested to conform to cryptographic standards during this evaluation, and have only been asserted as tested by the vendor.

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. This other cryptographic functionality has not been analyzed or tested to conform to cryptographic standards during this evaluation, and has only been asserted as tested by the vendor. More details on where the algorithms are implemented and which implementations are included in the scope of FIPS 140-2 testing are included in ST Section 6.1.2 Cryptographic Support Functions.

3.3 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.

3.4 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 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.

3.5 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.

3.6 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. However, the proprietary software on the fiber channel initiators is outside of the scope of the evaluation

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 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 BSD security level is a variable used to set the restrictiveness of the operating system.

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

3.7 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 following:

- 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.
- 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.

4 ASSUMPTIONS, THREATS AND OBJECTIVES

4.1 USAGE ASSUMPTIONS

The following table contains the assumptions regarding the security environment and the intended usage of the TOE.

Table 4.1-1 Assumptions

It is assumed that the Administrators are non-hostile, appropriately trained and follow all administrator guidance.
It is assumed that the TOE is properly configured as described in the guidance documentation.
There are no untrusted users and no untrusted software on the Management station, LKM Server, and hosts on which DHA authentication software is installed.
It is assumed that opening the chassis sends a tamper notification signal to the SEP cryptographic module.
It is assumed that 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 Decru user guidance.

It is assumed that 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

4.2 POTENTIAL THREATS

The TOE must counter the threats to security described in the table below.

Table 4.2-1 Threats

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.
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.
Inadvertent or intentional loss or zeroization of encryption keys may prevent users from gaining access to their encrypted data.
Missing security management functionality may hinder effective management of the TSF and allow attackers to gain unauthorized access to resources protected by the TOE
An unauthorized person may read, modify, or destroy security critical TOE configuration data.
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.
An attacker may gain access to TSF data when it is transmitted between the DataFort and the Management Station, LKM Server, and other DataForts.
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.

4.3 SECURITY OBJECTIVES

The following table contains the TOE Security Objectives.

Table 4.3-1 TOE Security Objectives

The TSF must provide a means to accurately detect and record security-relevant events in audit records. Audit records must be protected from unauthorized modification or deletion.
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.
The TSF must provide mechanisms to efficiently destroy key material in accordance with an administrator-specified policy.
The TSF must provide fault tolerant information flow control and data encryption/decryption services, ensuring continuation of service due to fibre channel link failure or failure of a cluster member.
The TSF in conjunction with the IT environment must identify and authenticate users and IT entities
The TSF must be able to control information flows between distributed clients and centralized storage devices.
The TSF must provide a centralized service that is able to send and receive keys and other security attributes from TOE appliances.
The TSF must provide a means for an administrator to manage the TOE security functions.
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.
The DataFort must provide a reliable clock to maintain the system time.
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.

The following table contains the Security Objectives for the IT Environment.

Table 4.3-2 Security Objectives for the IT Environment

The IT environment must provide a long term audit store for the TOE.
The IT environment must support identification and authentication of users and IT entities.
The IT environment must protect the TOE against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
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.
The Management Station in the IT environment must initiate a TLSv1 session for communications with the TOE.

The following table contains the Security Objectives for the Non-IT Environment.

Table 4.3-3 Security Objectives for the Non-IT Environment

Those responsible for the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
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.
Those responsible for the TOE must ensure that there are no untrusted users and no untrusted software on the Management Station and LKM Server.
The developer must ensure that the capabilities for the detection of physical tampering are appropriately tested.
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 Decru administrator guidance.
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 CLARIFICATION OF SCOPE

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL4 in this case).

2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.

3. As with all EAL4 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or "vulnerabilities" to objectives not claimed in the ST.

4. Initiators require multipath software to detect the link failure and route traffic to the other cluster members. The proprietary software on the fiber channel initiators is outside of the scope of the evaluation.

5. The SSH Server is disabled in the evaluated configuration.

6. Operations using FTP are not supported in the evaluated configuration

7. 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

8. The 1U system, the Decru DataFort FC525v2 appliance, is not part of the Common Criteria evaluation.

9. 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.

10. System card, recovery card and admin card run proprietary NetApp code and are not part of the TOE.

11. All operations performed using the recovery cards prior to installation and during the recovery of a DataFort are also scoped out of this evaluation

Decru DataFort FC520v2, LKM 2.5.1 depends on the IT environment to provide support for multiple methods of user and IT entity authentication and reliable time stamps.

The ST provides additional information on the assumptions made and the threats countered.

6 ARCHITECTURAL INFORMATION

6.1 TOE COMPONENTS

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

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 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.

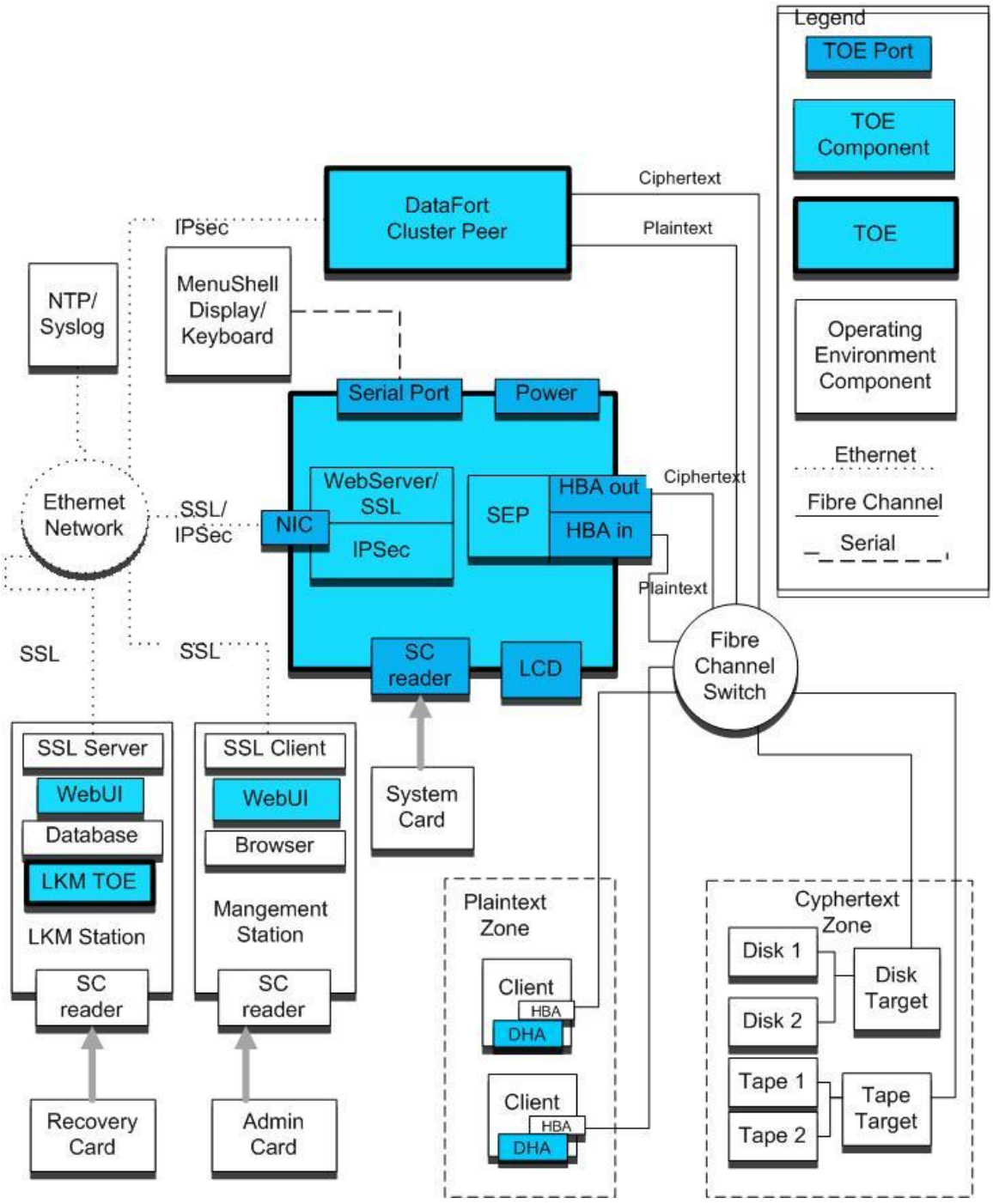

Figure 1: TOE Deployment

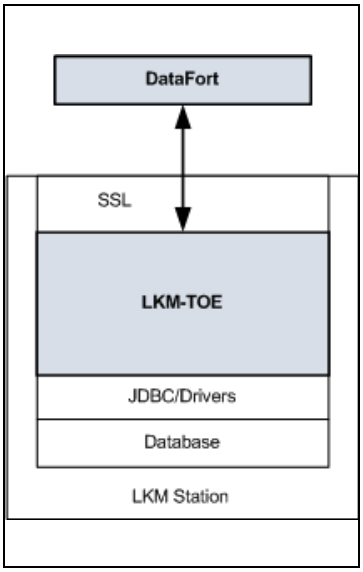

Figure 2: LKM Server

6.2 SECURITY FUNCTIONAL REQUIREMENTS

Note – Explicitly stated requirements for the TOE are denoted by _EXP.

Table 6.2-1 TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_STG_EXP.1	Partial protected audit trail storage
Class FCS: Cryptographic Support	
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.4	Cryptographic key destruction

FCS_CKM_EXP.5	Cryptographic key agreement: DH
FCS_CKM_EXP.6	Cryptographic key agreement: ECCDH
FCS_CKM_EXP.7	Cryptographic key export
FCS_CKM_EXP.8	Cryptographic key import
FCS_COP.1-AES	Cryptographic operation: AES
FCS_COP.1-RSA	Cryptographic operation: RSA
FCS_COP.1-3DES	Cryptographic operation: 3DES
FCS_COP_EXP.1	Cryptographic operation: HMAC-SHA
FCS_COP_EXP.2	Cryptographic operation: PRNG
FCS_COP_EXP.3	Cryptographic operation: SHA
FCS_COP_EXP.4	Cryptographic operation: AKEP2
FCS_COP_EXP.5	Cryptographic operation: Audit Log Signing
Class FDP: User Data Protection	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
Class FIA: Identification & Authentication	
FIA_EAU_EXP.5	IT entity authentication mechanisms
FIA_EID_EXP.1	Partial IT entity timing of identification
FIA_UAU_EXP.5	Multiple authentication mechanisms
FIA_UID_EXP.2	Partial user identification before any action
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data

FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Class FPT: Protection of TSF	
FPT_FLS.1	Failure with preservation of secure state
FPT_RCV.4	Function recovery
FPT_RVM_EXP.1	Partial non-bypassability of the TSP
FPT_SEP_EXP.1	Partial TSF domain separation
FPT_STM_EXP.1	Partial reliable time stamps
Class FTP: Trusted path	
FTP_ITC_EXP.1	Partial trusted channels

Table 6.2-2 IT Environment Security Functional Requirements

Note: Environment Security Functional Requirements are denoted by _ENV.

Class FAU: Security Audit	
FAU_STG_ENV.1	Partial protected audit trail storage
Class FIA: Identification and Authentication	
FIA_EAU_ENV.2	IT entity authentication before any action
FIA_EID_ENV.2	IT entity identification before any action
FIA_UAU_ENV.5	Multiple authentication mechanisms
FIA_UID_ENV.2	User identification before any action
Class FPT: Protection of TSF	
FPT_RVM_ENV.1	Partial non-bypassability of the TSP
FPT_SEP_ENV.1	Partial TSF domain separation
FPT_STM_ENV.1	Partial reliable time stamps
Class FTP: Protection of TSF	
FTP_ITC_ENV.1	Trusted channel - management station

7 DOCUMENTATION

The following documentation was used as evidence for the evaluation of the TOE. Documents that are publically available are shown in **boldface.**

7.1 DESIGN DOCUMENTATION

Document	Revision	Date
DataFort FC520v2 Security Policy Model, Doc ID: 11337-r-1-8	r1-8	None
DCCH2 FPGA Design Documentation, Doc ID 16850-r1-2	r1-2	2005-03-15
DCC-SEP HLD, Doc ID 29650-v1-r18	v1-r18	2008-01-04
DCC-SEP LLD, DocID 29983-v2-r19	v2-r19	2008-01-04
Decru DataFort FC520 v2, LKM 2.5.1 Functional Specification SAN Proxy Functional Specification, Doc ID 18672-r1-15	r1-15	2007-12-08
Decru DataFort FC520v2, LKM 2.5.1 Common Criteria EAL4 Low Level Design Documentation Roadmap and Addendum	1.4	None
Decru DataFort FC520v2, LKM 2.5.1 Decru Host Authentication Subsystem: Low Level Design Documentation for Common Criteria EAL4 Evaluation	1.5	2008-08-21
Decru DataFort FC520v2, LKM 2.5.1 DFC Subsystem: Low Level Design Documentation For Common Criteria EAL4 Evaluation	1.3	2008-01-10
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification LCD Interface, Doc ID 18781-1-4	r1-4	2007-11-11
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification High Availability and CryptoShred, Doc ID: 18770-r1-7	r1-7	2007-11-10
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification LKM Software Audit Functional Specification, Doc ID: 18760-r1-6	r1-6	2007-11-10
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification Management Configuration Properties, Doc ID: 18783-r1-5	r1-5	2007-11-11
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification SAN MenuShell/Dcrlogin Management Interface, Doc ID 18782-r1-4	r1-4	2007-12-08

Decru DataFort FC520v2, LKM 2.5.1 Functional Specification SAN WebUI Management Interface, Doc ID 18784-r1-11	r1-11	2007-12-08
Decru DataFort FC520v2, LKM 2.5.1 Functional Specification, Doc ID 18761-r1-31	r1-31	2008-02-19
Decru DataFort FC520v2, LKM 2.5.1 Hardware Subsystem: Low Level Design Documentation for Common Criteria EAL4 Evaluation	1.4	2008-01-16
Decru DataFort FC520v2, LKM 2.5.1 LKM Software High Level Design Documentation For Common Criteria EAL4 Evaluation	1.9	2008-08-26
Decru DataFort FC520v2, LKM 2.5.1 LKM Software Low Level Design Documentation For Common Criteria EAL4 Evaluation	1.16	None
Decru DataFort FC520v2, LKM 2.5.1 Management Subsystem: Low Level Design Documentation for Common Criteria EAL4 Evaluation	2.0	2008-10-30
Decru DataFort FC520v2, LKM 2.5.1 SAN Proxy Decru Host Authentication, Doc ID 18767-r1-5	r1-5	2007-12-08
Decru DataFort FC520v2, LKM 2.5.1 SAN Proxy Virtualization and Port-mapping, Doc ID 18769-r1-5	r1-5	2007-12-08
Decru DataFort FC520v2, LKM 2.5.1 TOE Underlying Hardware and Software for the IT Environment	0.3	2008-08-20
Decru DataFort FC520v2, LKM 2.5.1 Windows DHA Functional Specification	1.1	2008-01-03
Decru DCCH Hardware Guides	1.0B	2008-08-11
Decru Smart Card, Doc ID 14031-r1-4	r1-4	2007-11-11
DFC HLD, Doc ID 29408-v1-r28	v1-r28	2007-11-11
FC520v2 Audit Functional Specification, Doc ID: 18760-r1-11	r1-11	2008-08-08
FC520v2 SAN Proxy Decru Host Authentication, Doc ID 18767-r1-5	r1-5	2007-12-08
FC520v2 WebCLI Management Interface, Doc ID 14031-r8	r8	2008-07-08
FIPS Addendum, Doc ID 17778-r1-0	r1-0	2005-05-26
Hardware HLD, DocID 32996-v1-4	v1-4	2008-07-25

LKM Software Functional Specification, Doc ID 18779-r1-9	r1-9	2008-08-08
Management HLD, DocID 29381-v1-r26	v1-26	2008-01-16
SAN ST to FSP Mapping, DocID 27950-r1-9	r1-9	2007-11-11
SEP 2.0 Cryptographic Key Management, Doc ID 15727- r3-1	r3-1	2007-06-29
SEP 2.0 Cryptographic Key Management, Doc ID 15727-r2-2	r2-2	2005-06-03
SEP FPGA Reference Manual, Doc ID: 17497_fpga-r1-3	r1-3	2005-05-12
SEP Microcontroller Command Reference, Doc ID: 17497-uc-r1-3	r1-3	2005-05-12
SEP Microcontroller Design, DocID 15725-r1-5	r1-5	2005-03-15
Trusted Channels Decru DataFort FC520v2, LKM 2.5.1 Functional Specification, DocID 27998-r1-2	r1-2	2007-11-11
Windows DHA Functional Specification	1.1	2008-01-03

7.2 INSTALLATION AND GUIDANCE DOCUMENTATION

Document	Revision	Date
DataFort Administration Guide for FC-Series DataFort Appliance, Part №: 210-03944 A0 (090208_FC222)	A0	-09-02
DataFort Common Criteria Mode Log Messages	None	None
Decru Host Authentication, Part №: 30-000318 A0 (101608_DHA20)	A0	2008-10-16
Decru Lifetime Key Management Server Software Administration Guide, Part №: 210-04034 A0 v 2.5.1 012308	2.5.1	2008-01-23
Operating the DataFort Appliance in Common Criteria Mode, Part №: 30-000348 A0 (10318)	A0	2008-10-31

7.3 CONFIGURATION MANAGEMENT AND LIFECYCLE DOCUMENTATION

Document	Revision	Date
Bugzilla Usage	None	2006-02-23
BuildEnvironment	r13	2006-09-29

Building Security, Document № 03-FS20-4002-021-C	r7	2007-05-10
CC: DECRU Configuration Management Policies, 267-00119_A0	None	None
Configuration List	r26	2008-10-31
Decru CVS Instructions	None	None
Decru DataFort FC520v2 Configuration Management Addendum (ACM_AUT.1, Decru Acceptance Plan)	1.0	2007-08-22
Decru DataFort FC520v2 Life Cycle Support Documentation (ALC_LCD.1, ALC_TAT.1, ALC_DVS.1 and ALC_FLR.1) (Common Criteria Part III)	1.0	2008-05-26
Design Guidelines	None	None
Document Management and versioning	r5	2006-04-18
FPGA Development Workflow	r11	2007-04-04
FPGA Image Release to Manufacturing	None	None
Guidelines for reporting a defect in Bugzilla	r5	2006-06-16
Hardware Board Guidelines	r12	2007-04-25
Hardware Tool Description	r8	2008-05-29
Hardware_Cad_Tools	r8	2007-04-05
HW ALC	None	None
Mechanical Workflow	r5	2007-03-29
MFG ALC-Life Cycle	None	None
PM Phase Reviews	r30	2007-03-28
QA ACM Policy	None	None
Release Engineering Plan	1.1	2007-04-25
Release Model	r12	2007-03-28
Tracking Bugs Per Release	r3	2007-03-28
Tracking Vulnerabilities	r8	2007-04-20
TWiki Access Control	r33	2007-04-02
User Scenarios & Requirements: Bridging the Gap between Marketing's PRD and Development's Design	None	None
Using TRAP	r7	2007-04-18
Web Changes Alert	16	2005-03-27
Work Flow	r15	2007-03-28

7.4 DELIVERY AND OPERATION DOCUMENTATION

Document	Revision	Date
CC ADO-Delivery and Operations	None	None
Delivery and Operation Conformance	r3	2007-05-24
Limiting Access to System Software Images on the Decru Production Line, Doc № 267-00158	11	None
Marketing Part Numbers for FC-Series 2.2.2	v5	None
OS Release Process, Doc № 267-00141	A	None

7.5 TEST DOCUMENTATION

Document	Revision	Date
DataFort FC520v2 Test Plan for Common Criteria Evaluation (EAL4) Testing	1.9.0	2008-10-29
Decru DataFort FC520v2, LKM 2.5.1 Test Plan for Common Criteria Evaluation (EAL4) Testing Automated Tests	1.6	2008-09-10
NetApp SSBU DataFort FC520v2 Test Cases for Common Criteria Evaluation (EAL4) Testing	2.0.0	None

7.6 VULNERABILITY ASSESSMENT DOCUMENTATION

Document	Revision	Date
DataFort Vulnerability Analysis Plan	1.1	2008-03-22
Decru DataFort FC520v2, LKM 2.5.1 Vulnerability Analysis	1.2	2008-05-02
Decru SAN Evidence for AVA_MSU.2 The misuse analysis of the guidance, Doc ID: 33632	1.4	2008-06-02
Public Vulnerability Screening	1.1	2008-03-22
Strength of Function Analysis, DocID: 33631	1.2	2008-10-29
THIRD PARTY SW KEYWORD LIST: extracted from SAN 2.2.1 branch and modified for relevance to the SAN product.	None	None
Vulnerability Tracking Process	1.1	2008-03-22

7.7 SECURITY TARGET

Document	Revision	Date
NetApp DataFort FC520v2, LKM 2.5.1 Common Security Target	3.3	2008-10-31

8 IT PRODUCT TESTING

This section describes the testing efforts of the Vendor and the evaluation team.

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

Vendor testing was performed by NetApp Quality Assurance personnel at their site in California.

All of the evaluation team's testing was conducted at:

NetApp, Inc., 1260 Crossman Avenue, Bldg 10, Sunnyvale CA, 94089

The testing was performed according to the following schedule:

10/20/08	ALC, ACM audit interviews, Jabil Security visit
10/21/08	Installation of TOE in evaluated configuration
10/22/08 – 10/23/08	Penetration (Vulnerability) Testing Execution of Developer's Functional Tests
10/24/08	Independent (Team-Defined) Testing

The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, were well written and complete.

8.1 INSTALLATION TESTING

The installation was performed by the evaluation team. The Target of Evaluation was installed following the procedures defined in the following documents:

- *Operating FC-Series DataFort Appliances in Common Criteria Mode, Part number: 30-000348 A0 (102108)*

- *OPERATION GUIDE - Decru Host Authentication, Part number: 30-000318 A0 (070908_DHA20)*

- *DataFort Administration Guide for FC-Series DataFort Appliance,* Part number: 210-03944 A0 (081208_FC222)

- *Decru Lifetime Key Management Server Software Administration Guide*, Part number: 210-04034 A0 v 2.5.1 012308

The test installation resulted in a successful installation of the TOE in the evaluated configuration. All of the TOE components were installed correctly for the evaluated configuration by following the procedures documented. After installation, the evaluated configuration of the TOE was tested without having to change any of the configuration parameters or rerun any of the installation steps.

8.2 DEVELOPER TESTING

The set of developer tests consists of 210 manual test procedures and a number automated testing scenarios. The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. After the test cases were defined, test procedures were written to exercise each test case. Most of the developer test cases were manual, i.e. all test steps including setup and cleanup steps were performed by a user entering commands through the WebCLI or using the WebUI console. The tests were written to exercise the security–relevant interfaces and to exercise the functions of the TOE. Automated tests were devised by the developer to exercise security functions in the Security Audit and User Data Protection group. The test tools used for running the tests have been listed in both the Developer Test Plan and the Evaluator Test plan and Report.

The evaluation team ran a sample of the functional test procedures provided by the vendor:

The vendor submitted a verified set of manual and automated test cases. The evaluation team ran 48 manual test procedure files which corresponded to approximately 24%, and 25% of the automated test scenarios. For the evaluator testing a stringent standard for success was applied. A test was considered a success only if the actual results obtained by the evaluator when the test was run matched the expected and actual results documented *for each test step* in that test procedure when it was run by the developer.

All of the developer functional tests were run successfully. The developer test procedure documents meet the CC standards and the evaluators have confidence that the entire set of functional tests were run by the developers on the evaluated configuration of the TOE.

8.3 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team devised a test subset for independent testing. The evaluation team's strategy in developing the team-defined tests of the TOE was to supplement the developer functional tests and the penetration tests. The team-defined functional tests were devised to exercise possible areas of misuse of the TOE or vulnerabilities to the TOE that were discovered while running the developer functional and penetration tests.

All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. The evaluation team devised 5 independent tests and performed four of those tests. Test Independent # 2 wasn't executed as planned due to failure of equipment.

Security Functions	**SFRs**	**Tests**
To verify that the adding a route cluster member functionality is not available post initialization.	n/a	Test Independent # 4
TSFI test for db export	n/a	Test Independent # 5
User Data Protection	FDP_IFF.1	Test Independent # 1 Test Independent # 2
Trusted Path/Channels	FTP_ITC_EXP.1	Test Independent # 3

The independent test cases defined were executed by the evaluation team after the TOE was installed in the evaluated configuration consistent with the Security Target. The test tools used for running the tests have been listed in both the Developer Test Plan and the Evaluator Test plan and Report.

The validation team relied on the evaluation team's report of the independent testing effort and concluded that the testing was successful.

8.4 EVALUATION TEAM PENETRATION TESTING

For its penetration tests, the evaluation team evaluated the developer's vulnerability analysis document, the independent test plan, the guidance documentation and the TOE design to identify potential penetration test cases. Penetration tests were selected based on the evaluation team's experience with evaluating the developer's design, guidance, test, and vulnerability assessment documentation.

The evaluation team created a penetration test plan. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team performed seven penetration tests.

1	The evaluator used nmap tool to verify that only the allowed services were running in the DataFort™ FC520v2 appliances, LKM and Management stations in the CC evaluated configuration.
2	The evaluator used Nessus tool to scan TOE components for any known vulnerabilities (database updated as of 10/22/2008).
3	Testing Access to TSF data: - Attempts to corrupting/modify/remove/rename configuration file and verify the behavior of the TOE - Attempts to remove/modify Log file(s) - Attempts to import compromised encryption keys to the DataFort™ FC520v2 - Attempts to modifying permissions stored in the SEP and configdb.
4	Testing through WebCLI/WebUI Interfaces: - Attempts to execute commands through WebCLI from unauthorized roles - Attempts to bypass I&A mechanisms through WeUI by using invalid UID/PW (long UID/PW, using special characters as part of UID etc.).
5	Verify Backdoor Login Access Not Permitted (via serial port, and/or LKM and Management stations)
6	Verify that DCS commands will not be executed in the CC evaluated configuration.
7	Injection Attacks - Handling mal-formatted commands - Setting system properties to command strings - Injection attacks in WebUI - Attacks to Key records in the LKM workstation

The testing was performed by the evaluation team after the TOE was installed in the evaluated configuration consistent with the Security Target.

The validation team relied on the evaluation team's report of the penetration testing effort and concluded that the testing was successful.

9 EVALUATED CONFIGURATION

9.1 TEST SOFTWARE AND HARDWARE

The test configuration consists of two FC520v2 DataForts, an LKM server software application, a Microsoft Windows 2003 based host, a Microsoft Windows 2003 based server, a Unix based server, a Unix based log server, a tape library and disk array.

The TOE includes the following test bed components:

- DataForts
- LKM software
- Mangement work station
- Data I/O servers
- Remote log file server
- DHA server and software

The IT Environment includes the following test bed components:

- Windows 2003 operating system
- Unix operating system
- FC tape library
- FC disk array
- FC switch

9.2 TEST TOOLS AND SCRIPTS

- Nmap (http://nmap.org/)
- Nessus (http://www.nessus.org/)
- Internet Explorer
- EMC PowerPath v4.5.0
- IOMonkey
- Cygwin tool
- dd (Unix command for data I/O)
- Wireshark v1.0.0

10 RESULTS OF THE EVALUATION

The evaluation team conducted the evaluation in accordance with the CC and the CEM

The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In the Final ETR, all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team.

In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the following documents:

- Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, Decru DataFort FC520v2, LKM 2.5.1

- Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE – EAL 4, Decru DataFort FC520v2, LKM 2.5.1

The evaluation team determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL4) requirements augmented with ALC_FLR.1, Basic Flaw Remediation. The rationale supporting each CEM work unit verdict is recorded in the ETR. Therefore, when configured according to the guidance documentation enumerated in section 0 of this report, the TOE is CC compliant.

The validator observations support the evaluation team's conclusion that Decru DataFort FC520v2, LKM 2.5.1 meets the claims stated in the Security Target.

11 VALIDATION COMMENTS/RECOMMENDATIONS

1. The password composition rules, as enforced, enforce only an 8 characters limitation with no further restrictions (i.e., minimum numbers of particular character classes). Systems requiring compliance with DOD 8500.2 or NIST 800-53 controls may require procedural mitigations for stronger password composition.

2. 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. 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, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Additionally, 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. The non-approved algorithms, as well as the cryptography not covered by the FIPS certification have only been asserted as tested by the vendor.

12 LIST OF ACRONYMS

Acronym	Description
CC	Common Criteria [for IT Security Evaluation]
CLI	Command Line Interface
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

13 BIBLIOGRAPHY

The validation team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, version 2.3, August 2005, Part 1.
- *Common Criteria for Information Technology Security Evaluation*, version 2.3, August 2005, Part 2.
- *Common Criteria for Information Technology Security Evaluation*, version 2.3, August 2005, Part 3.
- *Common Evaluation Methodology for Information Technology Security*, version 2.3, August 2005.
- *Decru DataFort FC520v2, LKM 2.5.1 Security Target*, Version 3.3

- *Evaluation Technical Report For a Target of Evaluation, Volume 1: Decru SAN_ASE_ETR_Volume 1_Version 2.0*
- *Evaluation Technical Report For a Target of Evaluation, Volume 2: Decru SAN ETR Vol-2 V2.0*
- *Evaluator Test Plan and Report EAL4 Evaluation Decru DataFort FC520v2, LKM 2.5.1*