Indian CC Certification Scheme (IC3S)

Certification Report

Report Number: **STQC/CC/11-12/06/CR**

Product / system: FORT FOX HARDWARE DATA DIODE

Dated: 18 December 2012

Version: 1.0

Government of India

Ministry of Communication & Information Technology

Department of Electronics and Information Technology

Standardization, Testing and Quality Certification Directorate

6. CGO Complex, Lodi Road, New Delhi – 110003

India

Product developer:	Fox-IT BV, Olof Palmestraat 6, 2616 LM Delft, P.O. box 638, 2600 AP Delft, The Netherlands
TOE evaluation sponsored by:	Fox-IT BV, Olof Palmestraat 6, 2616 LM Delft, P.O. box 638, 2600 AP Delft, The Netherlands
Evaluation facility:	Common Criteria Test Laboratory (CCTL), ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	Tapas Bandopadhyay Malabika Ghose Subhendu Das
Evaluation report:	STQC IT (KOL)/STQC/CC/1112/06/ETRv1.1
Validation Personnel:	Mitali Chatterjee & B K Mondal

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Fox-IT BV
Developer	Fox-IT BV
Product and Version	Fort Fox Hardware Data Diode (FFHDD), Version: FFHDD2
Brief description of product	The product which is the Target of Evaluation (TOE) is a hardware data diode identified as Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2. The TOE is a physical hardware device housed in a single 19" rack component. It is uniquely labeled with a serial number on the rear panel. The unique TOE reference starts with the version number (FFHDD2) followed by a unique four-digit serial number and ends with a plus sign (+).
Security Target	Fort Fox Hardware Data Diode Security Target Common Criteria FFHDD – EAL 4+ Version 2.06
CC Part 2	Conformant
CC Part 3	Conformant
EAL	EAL4+ (augmented with AVA_VAN.4 and ALC_DVS.2).
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	**18th December 2012**

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of

security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification service for evaluating the security functions or mechanisms of the IT products. It also provides a framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/DIT);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Schème (IC3S)
- STQC/CC/DO2 : Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The product Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2 has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognised under the IC3S scheme of STQC IT Certification Body.

The developer and sponsor is Fox-IT BV, Olof Palmestraat 6, 2616 LM Delft, P.O. box 638, 2600 AP Delft, The Netherlands.

The certification process was concluded with the completion of this certification report.

This evaluation was completed on 27th July, 2012. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B12 of this report. The product Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2 will be included in the list of the products certified under I3CS Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in . Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B1 Executive Summary

B 1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer, Fox-IT BV and the Evaluation Technical Report [ETR] written by CCTL, ERTL (East), Kolkata. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4+) have been met.

B 1.2 Evaluated product and TOE

The product evaluated was:

Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2 is a unidirectional device, which is used at the boundary of two computer networks and allows data to travel only in one direction. It has two data interface one bidirectional 'INPUT' interface and another unidirectional 'OUTPUT' interface. The 'INPUT' interface is usually connected to the computer network, at lower security level whereas the 'OUTPUT' interface is connected to the higher security side.

The one way physical connection of the TOE allows information to be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level), without compromising the confidentiality of the information on the High Security Level.

To ensure signals can only pass in one direction, but not vice versa, the TOE deploys a light source and corresponding photocell. Fiber-optic cables are used to minimize the electromagnetic radiation when the TOE input is connected to the Low Security Level Server and the TOE output is connected to the High Security Level Server.

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B6).

B 1.3 Security Claims

The [ST] specifies the security objective of the TOE and the threat that they counter (Refer 4.1 of ST). Security Functional Requirements (SFRs) (listed in 5.1 of ST) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/11-12/06 dated 31st May 2011.

The TOE as described in the [ST] (Refer 1.4 of ST) is a physical hardware device housed in a single 19" rack component was supplied by the developer.

The TOE was evaluated through evaluation of its documentation, site visit; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and CCTL, Kolkata Operating Procedure OP-07.

The evaluation has been carried out under written agreement [dated 7-7-2011] between CCTL, Kolkata and the sponsor.

B 1.5 Independence of Certifier

In the last two years, the certifier did not render any consulting - or other services for the company ordering the certification and there was no relationship between them which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the stated conditions as detailed in this certification report. This certificate is not an endorsement of the IT product by the Certification Body or any other organisation that recognises or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.

The specific scope of certification should be clearly understood by reading this report along with the [ST]. The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].

The TOE should be used in accordance with the supporting guidance documentation.

This Certification report is only valid for the evaluated TOE.

B 2 Identification of TOE

The TOE is identified as: Fort Fox Hardware Data Diode (FFHDD,) Version FFHDD2. The TOE is a physical hardware device housed in a single 19" rack component. It is uniquely labeled with a

serial number on the rear panel. The unique TOE reference starts with the version number (FFHDD2) followed by a unique four-digit serial number and ends with a plus sign (+).

B 3 Security policy / Security functions

- There are no organizational security policies that the TOE must meet.

- The only security function that the TOE provides is as follows:
  Information flow control
  The TOE allows information to flow through it, in a single direction from the Bidirectional Input (Low Security Level Transceiver) to the Unidirectional Output (High Security Level Transceiver).

B 4 Assumptions

There is no personnel assumption associated with the TOE

B 4.1 Physical Environmental Assumptions

Physical Assumptions

Assumption code	Description
A.PHYSICAL	The intended operation environment shall store and operate the TOE in accordance with the requirements of the High Security Level side.

IT Environment Assumptions

Assumption code	Description
A.NETWORK	The TOE is the only method of interconnecting the Low Security Level network and High Security Level network. This prevents a threat agent from circumventing the security being provided by the TOE through an untrustworthy product.

B 5 Architectural Information

The TOE architecturally prevents bypass of its security-enforcing functionality by ensuring that data cannot flow from the Output TSFI to the Input TSFI.
The TOE is pure hardware and does not have any memory, settings, or other things that can be changed. The only TSFIs that are accessible to attackers are, “Input” and “Output” TSFI. The data those received on the Input TSFI are not interpreted by the TSF and all data those received on the Output TSFI are ignored. In this way the TOE architecturally protects itself from tampering.

The security of the TSF rests on a single component: the transceiver module connected with the "Output" TSFI. The TSF is active instantly through this transceiver module and whose physical properties are not affected by initialization. In this way the secure initialization process of the TSF is ensured.

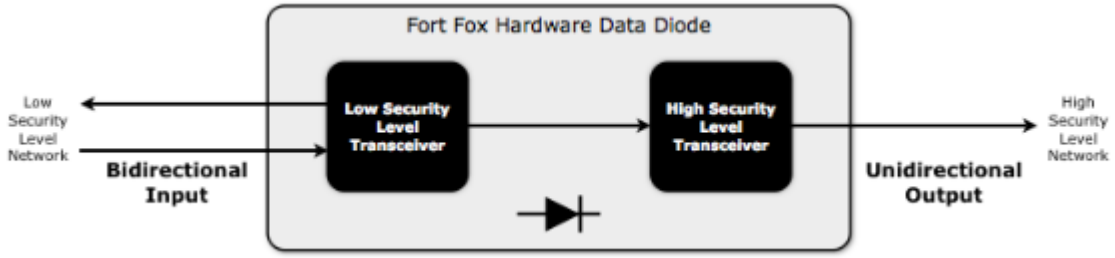

Figure 1: Fort Fox Hardware Data Diode Functional Block Diagram

B 6 Evaluated configuration

The TOE is defined uniquely by its name and version number Fort Fox Data Diode, version FFHDD2 and can be identified by a unique TOE reference starts with the version number (FFHDD2) followed by a unique four-digit serial number and ends with a plus sign (+).
The TOE needs no specific configuration settings as there is only one configuration defined.

B 7 Documentation

The list of documents supplied by the developer as evaluation evidences to the evaluators at the evaluation facility are given below

1. Security Target, Common criteria FFHDD – EAL4+ ,ver 2.06
2. Fort Fox Hardware Data Diode: Security Architecture Description: Common Criteria FFHDD – EAL 7+, ver 2.03
3. Functional Specification and Security Policy Model, Common Criteria FFHDD – EAL7+,ver. 2.04
4. Document (TDS document)named as "Complete semiformal modular design with formal high-level design presentation Common Criteria FFHDD – EAL7+" version 2.05
5. Implementation Representation of the TSF: Common Criteria FFHDD – EAL7+ ,ver2.04
6. Product Delivery Procedure, Preparative procedures and operational user guidance, version 2.03
7. Product Delivery Procedure, Preparative procedures and operational user guidance, version 2.03
8. Advance Support, version 2.06
9. Product Delivery Procedure, Preparative procedures and operational user guidance, version 2.03
10. Sufficiency of Security Measures version 2.05 (DVS)
11. Measurable Life-Cycle Model, version 2.06

12. Compliance with implementation standards - all parts version 2.04 (TAT)
13. Rigorous analysis of coverage and Implementation representation version 2.03 (COV)
14. Developer's Test Documentation "Ordered Functional Testing", version 2.03

.

B 8 Product Testing

B 8.1 IT Product Testing by Developer

The developers test effort is summarized as below.

Table 1: Developers Test Effort

#	Aspects	Validator's comments
1	On overall developer **testing strategy & approach** employed	The developer has carried out tests, conforming to the TOE security environment, as described in the [ST] and covering all the security functionalities. Testing was done manually.
2	**On TOE test configurations**: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards.	The TOE was tested in the defined test configuration consistent with the [ST].
3	**On depth of testing** in respect of all functionalities of all TSFs:	The developer has carried out testing taking into the TOE security function of "Unidirectional flow of traffic" as described in the [ST] and covering all the TSFIs. The tests also take care the interaction among subsystems and modules.
4	**On test results:** A description of the overall developer testing results	The results obtained by the developer are consistent, reproducible and matching with the expected results. The tests were repeated at CCTL, Kolkata and it is found that the test results are tallying.

The validator analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was found to be complete.

B 8.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

.

Table 2: Evaluators test effort

#	Aspects	Validator's comments
1	On overall evaluator **testing strategy & approach**	The evaluators repeated all the developers' tests relating to the security functionalities of the TOE; in addition to that they developed test cases that augment the developer tests and conducted the same independently at CCTL, Kolkata. The Independent tests at CCTL were planned and conducted with following objectives: 1. To verify Unidirectional Data Packets flow through the TOE as claimed. 2. To verify the overall functionality of the TOE in intended operational environment (i.e., using RED / BLACK Server) 3. To verify unidirectional flow of Optical signal through the TOE, as specified. 4. To verify the Implementation of the SFR enforcing module of the TOE as per design
2	**On TOE test configurations**: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards.	The evaluators have examined the TOE and found that the TOE is pre-configured and no variation in configuration is possible. The description of the test set–up given in the developer's test documentation and the results are reproducible. The typical test configuration of the TOE is to use it at the boundary of two computer networks, connecting, its bi-directional 'INPUT' interface to the low security side and unidirectional 'OUTPUT' interface to the high security side. It is observed that the test configuration is consistent with the description as given in the [ST] .
3	**On depth of testing** in respect of all functionalities of all TSFs	The evaluators have repeated the developer's tests at CCTL, Kolkata to verify the reproducibility of test results and to ensure the coverage of all TSFIs, as mentioned in the FSP document. While making the test strategy for independent tests at CCTL, consideration was given to cover all security functional requirements (as defined in the [ST]), interfaces visible to the users, sub-systems and modules of the TOE, in respect of their behaviours and implementation correctness.
4	**On test results:** A description of the overall evaluator testing results	The evaluator conducted tests on the TOE and confirm that the TSF operates as specified. The results were found to be in compliance with the claim made in the [ST].

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results

B 8.3 Vulnerability Analysis and Penetration testing

In search of potential vulnerabilities, the evaluator has conducted public domain search, focussing on the type of the TOE. The 'url' http://nvd.nist.gov/ has been searched:

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

As the TOE is not a software product the above 'url is not applicable for this TOE. The database does not contain any record with the keyword "data diode".

The [ST] has identified T.TRANSFER as the threat that the TOE should be able to mitigated, if the same is operated in the specified operational environment. The identified threat is addressed by the TOE through its security mechanism of "unidirectional flow" of traffic. This security mechanism is realized by the TOE through its SFR enforcing module. Considering the threat, proposed operating environment and user accessible interfaces, the following attack scenarios hypothesized.

Table 3: Hypothezied attack scenarios

Attack scenarios	Description
Attack Scenario 1a (Deliberate)	Attacker at 'Output' side tries to pass information through the TOE to 'Input' side, without replacing or tampering the hardware inside the TOE.
Attack Scenario 1b (Accidental)	Attacker at 'Output' side pass information through the TOE to 'Input' side, accidentally, without replacing or tampering the hardware inside the TOE.
Attack Scenario 2	Attacker at 'Input' side tries to get information through the TOE from 'Output' side.
Attack Scenario 3	Attacker at 'Output' side tries to bypass the security mechanism of the TOE to pass information to 'Input' side.
Attack Scenario 4	Attacker at the 'Input' side tries to bypass the security mechanism of the TOE to get information from 'Output' side.

The TOE documents like, [ST], Functional specification (FSP),TOE architecture & Design (TDS), TOE Preparatory guidance document etc were also analysed to map the attack scenarios. Once the attack scenarios are mapped with the TOE interfaces, architecture, design and implementation details (of SFRs), then those may also be identified as potential vulnerabilities, specific to the TOE realization.

The attack potentials for each attack scenarios/potential vulnerabilities were calculated using guidance given in [CEM] and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement and same were used to plan for penetration testing.

Considering the intended attack scenarios, the penetration testing has been planned and conducted as follows:

The developer made two assumptions in the [ST] in respect of intended operating environment of the TOE:

1. The TOE is operated and stored within a physically secure environment that, at minimum, meets the requirements for the High Security Level side. This mitigates the risk that unauthorized personnel have access to the TOE at any time
2. The TOE is the only way to connect the two networks

Considering the assumptions made in the [ST], the attack scenario 3 is discarded and not considered for penetration testing. The estimated attack potentials for attack scenarios 2 & 4 are beyond high and hence kept out of the scope of penetration testing.
Hence, the TOE must be capable of protecting the information of 'high security side' ('OUTPUT') of the TOE from being accessed from the 'low security side' ('INPUT'). Further, there may be some possibility of information leakage from the 'high security side' through some accidental means (non-specific/non-predicted) under any condition (attack scenario 1b).
Considering these, the evaluators planned to verify the availability of information carried through **optical signal** from the output interface to the input interface of the TOE. Hence, if the TOE is able to protect the flow of intelligence through the optical signal from 'output' to 'input' side, then the attack becomes null and void, irrespective of the attack scenarios.
So the objective of penetration testing was set as "**It is not possible to transmit any intelligence from 'OUTPUT' side to 'INPUT' side of the TOE through optical signal**" which addresses both attack scenarios (1a & 1b).
The two interfaces 'INPUT' and 'OUTPUT' of the TOE are responsible for communication of the information through the TOE. These are optical inputs and hence optical test signal was chosen for conducting the test.

Penetration Test effort

Table 4: Penetration test effort

#	Aspects	Validator's comments
1	On overall evaluator **testing strategy & approach**	The vulnerabilities with 'High' attack potential are selected for Penetration testing. This TOE transmits data packets unidirectionally, i.e., from 'input' side to 'output' side. The 'input' side is called as BLACK side and the 'output' side is called as RED side. For designing attack scenarios, the environments of these two sides have been considered. The device takes optical signal as input. Optical signal has been used to simulate attacks sending signal from 'output' side.
2	**On TOE test configurations**: The particular configurations of the TOE that were tested,	The TOE is received as hardware and then connection has been done as per preparative procedure document.

#	Aspects	Validator's comments
	including whether any privileged code were required to set up the test or clean up afterwards.	
3	**On depth of penetration testing**	The penetration testing was conducted considering the listed attack scenarios with High attack potential focusing on the issues like bypassing and direct attack of TSFs. The threat T.TRANSFER has been analysed in the intended operational environment. The evaluation evidences have been methodically analysed to design these scenarios.
4	**On test results:** A description of the overall evaluator penetration testing results	Penetration testing was carried out for each of the identified potential vulnerabilities which are candidate for testing. The evaluator could not able to exploit the identified vulnerabilities.

Residual vulnerabilities

Considering the attack potential as 'High', no identified vulnerabilities could be exploited by the evaluators. Hence the TOE does not contain any exploitable vulnerability for 'High Attack Potential'. However, these vulnerabilities may be exploited with higher attack potential. The identified vulnerabilities with more than 'High Attack Potential' are not considered for Penetration testing. Hence, these vulnerabilities may be considered as residual vulnerabilities.

B 9 Evaluation Results

The evaluation results have been presented by the evaluator in the [ETR]

The TOE was evaluated through evaluation of its documentation, site visit; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and laboratory operative procedure [OP-07].

Documentation evaluation results: The documents for TOE and its development life cycle provided by the developer were analyzed by the Evaluator in view of the requirements of the respective work units of the [CEM] and the same was recorded in work sheets in the [ETR]. The deficiencies and clarifications, if any, were communicated to the developer by the Evaluator through observation reports (OR). The responses of the developer were scrutinized by the evaluator and recorded in the respective work sheets. Further ORs were raised and cycle was carried out for several iterations till all the deficiencies were addressed and requirements for each work units met. The final version of the respective evaluation evidences were found to comply with the requirements of CCv3.1 for EAL4+.

Site visit:

The TOE is designed, developed and manufactured at Fox-IT, with their partner organization Engg Spirit at Netherlands. One evaluator performed the sub-activity, 'Site Visit' at the development and manufacturing sites in Netherlands on 15-17th Feb 2012, with the following objectives

- Related to configuration management system
    - To observe the use of the CM system as described in the CM plan
    - To evidence application of Configuration Management System to ensure that the integrity of the TOE is preserved throughout its life cycle
- Related to delivery of the TOE
    - To evidence measures, procedures, and standards concerned with secure delivery of the TOE, ensuring that the security protection offered by the TOE is not compromised during the transfer to the user.
    - To observe the practical application of delivery procedures as described in the delivery documentation
- Related to security of development environment

The evaluator, in the site visit report, have opined for corrections in different documents to align them with the practices those are followed on the floor and as well as some process corrections like formal Memorandum of Understanding (MoU) with 'Engg Spirit', maintenance of Test logs of the TOE and/or its components, maintenance of records pertaining to the important activities of TOE manufacturing.
The modified documents and corrections in TOE manufacturing process (as evident from the documentation of TOE) were found to be consistent with the practice and satisfy the requirements of EAL 4+.

B 10 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that the TOE satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL 4+ Certification**.

However it should be noted that there are no **Protection Profile** compliance claims

B 11 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report

FSP: Functional Specification

IC3S: Indian Common Criteria Certification Scheme

IT: Information Technology

PP: Protection Profile

ST: Security Target

TOE: Target of Evaluation

TDS: TOE Design Specification.

TSF: TOE Security Function

TSFI: TOE Security Function Interface

B 12 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM}: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Fort Fox Hardware Data Diode Security Target Common Criteria FFHDD – EAL 4+ Version 2.06
6. [ETR]: Evaluation Technical Report No. STQC IT (KOL)/STQC/CC/1112/06/ETR, Version No. 1.1
7. [OP-07]: CCTL operating procedure