National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Owl Computing Technologies
Data Diode Network Interface Card
Version 4

Report Number: **CCEVS-VR-07-0018**
Dated: **February 01, 2007**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Shaun Gilmore
National Security Agency
Ft. Meade, MD

Santosh Chokhani
Orion Security Solutions
McLean, VA

Common Criteria Testing Laboratory
Mike Boberski
Tammy Compton
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary 1
1.1 Evaluation Details 1
1.3 Threats to Security 2
2 Identification 3
2.1 ST and TOE Identification 3
2.2 TOE Overview 3
2.3 IT Security Environment 4
2.3.1 Physical Boundaries 4
2.3.2 Logical Boundaries 5
3 Security Policy 6
4 Assumptions 7
5 Architectural Information 7
6 Documentation 7
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 8
7.3 Evaluation Team Penetration Testing 8
8 Evaluated Configuration 9
9 Results of the Evaluation 9
10 Validator Comments/Recommendations 10
11 Annexes 10
12 Security Target 10
13 Glossary 11
14 Abbreviations 13
15 Bibliography 14

1 Executive Summary

The evaluation of Owl Computing Technologies Data Diode Network Interface Card version 4 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on February 1, 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.3 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Owl Computing Technologies Data Diode Network Interface Card version 4 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Evaluation Details

Evaluation Completion: February 1, 2007

TOE Hardware Identification – Owl Computing Technologies, Inc. Data Diode Network Interface Card Version 4

TOE Software Identification – Owl Computing Technologies, Inc. Data Diode Network Drivers

- Version 4.16 for Windows
- Version 4.0 for Solaris
- Version 4.1 for Linux

Developer:

Owl Computing Technologies, Inc.
38A Grove Street, Suite 101
Ridgefield, CT, 06877

CCTL:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Validation Team:

Shaun Gilmore
National Security Agency (NSA)
9800 Savage Rd
Ft. Meade, MD 20755

Santosh Chokhani
Orion Security Solutions
McLean, VA

Evaluation Class: EAL 4

Completion Date: February 01, 2007

1.2 Threats to Security

The Security Target identified the following threat for the evaluated product.

T.WRONGWAY An attacker may be able to cause Information to flow inappropriately from one attached host to another.

2 Identification

2.1 ST and TOE Identification

ST: Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification

TOE Identification: Owl Computing Technologies Data Diode Network Interface Card version 4 with the following software drivers:

- Version 4.16 for Windows
- Version 4.0 for Solaris
- Version 4.1 for Linux

CC Identification – Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408).

Protection Profile (PP) Identification – The TOE does not claim conformance to a PP.

CEM Identification –*Common Methodology for Information Technology Security Evaluation*: Evaluation Methodology, Version 1.0, August 1999.

2.2 TOE Overview

The Target of Evaluation (TOE) is offered by Owl as a single Data Diode Network Interface Card (a Send-Only NIC or Receive-Only DDNIC) with its associated driver software, or as a pair of Data Diode Network Interface Cards with their associated driver software modules. Any host that supports a PCI Bus is sufficient for the correct operation of the TSF; therefore the host is not part of the TOE.

Each type Data Diode Network Interface Card allows information to move across it in only one direction, and therefore protects its Host System from information flow across the Data Diode Network Interface Card in the reverse direction. Data sent across the PCI Bus of sending host system (via driver software) are staged, queued, segmented and framed in the Send-Only DDNIC, and output through the Optical Transmitter of the Send-Only DDNIC. Data presented to the Optical Receiver of the Receive-Only DDNIC is reassembled into the original message in the Receive-Only DDNIC, and then transferred through the PCI Bus of the receiving host system to driver software in the receiving host system.

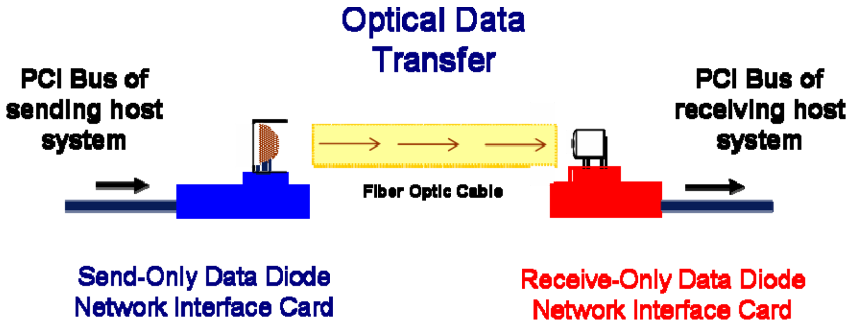
Optical Data Transfer
PCI Bus of sending host system
PCI Bus of receiving host system
Fiber Optic Cable
Send-Only Data Diode Network Interface Card
Receive-Only Data Diode Network Interface Card

Figure 1 - High Level view of the Data Diode Interface

The Owl Data Diode System consists of a pair of Owl Computing Technologies, Inc. Data Diode Network Interface Cards (DDNICs) connected to each other through optical interfaces and a fiber optic cable, for unconditional and unidirectional information flow control between two separate host systems. The one-way information transfer occurs via an optical link consisting of one light source (at the source computer) and one light detector (at the destination computer) and using single one-way board component-level information paths in each DDNIC. No information of any kind, including handshaking protocols, (as in TCP/IP, SCSI, USB, Serial/Parallel Ports, etc.) travels from the destination computer back to the source computer.

The Owl Data Diode System moves packet data directly between a Send-Only DDNIC and a Receive-Only DDNIC via the optical interfaces of the DDNICs. Data sent across the PCI Bus of sending host system (via driver software) are staged, queued, segmented and framed in the Send-Only DDNIC, and output through the Optical Transmitter of the Send-Only DDNIC. The output of the Send-Only DDNIC is sent through a fiber optic cable connected to the Optical Receiver of the Receive-Only DDNIC. The data is then reassembled into the original message in the Receive-Only DDNIC, and then transferred through the PCI Bus of the receiving host system to driver software on the receiving host system.

2.3 IT Security Environment

The TOE security environment consists of the organizational security policies and usage assumptions as they relate to TOE. The TOE provides for a level of protection that is appropriate for IT environments that require control over what information is accessed by the users on the systems. It is suitable for use in both commercial and government environments. The organizational security policies enforced by the TOE are sufficient to mitigate and counter any implied threat to the assets protected by the TOE.

2.3.1 Physical Boundaries

The non-TSF portions of the Send-Only DDNIC and the Receive-Only DDNIC each include three functional components, the Asynchronous Transfer Mode (ATM) Segmentation and Reassembly Controller (SAR), the ATM Physical Interface Device (PHY), and the Optical Component (either the Fiber Optic Transmitter in theSend-Only DDNIC or the Fiber Optic Receiver in the Receive-Only DDNIC). The SAR connects directly to the PCI bus of the host system and to the PHY. Note that the Send-Only DDNIC's Optical Transmitter has only a light source and does not have a light detector and the Receive-Only DDNIC's Optical Receiver has only a light detector and does not have a light source. The absence of the light detector in the Send-Only DDNIC and the absence of the light source in the Receive-Only DDNIC are part of the TSF enforcing mechanism. The TSF is enforced at the physical level.

In addition to the physical enforcement of the TSF by having only an Optical Transmitter (the Send-Only DDNIC) or an Optical Receiver (the Receive-Only DDNIC), each Owl DDNIC provides a single one-way data path for information travel between the PHY and the Optical Component (either the Optical Transmitter in the Send-Only DDNIC or the Optical Receiver in the Receive-Only DDNIC). The path is physical in nature and consists of components at the board level. The components provide an impedance-matched electrically conductive path between the Physical Interface Device (PHY) and the Optical Component.. The path between the PHY and the Optical Component in each DDNIC is the only impedance-matched electrically conductive path available between the two devices, and therefore cannot be bypassed.

In addition to providing an impedance-matched electrically conductive path between the PHY and the Optical Component of each DDNIC, there is provided an electrically conductive path between the host-system power and the Optical Component. (There is no electrically conductive path from the host-system power to the location of where there there is no installed Optical Component.)

Each Owl DDNIC has two external interfaces. One interface is the Peripheral Component Interface (PCI). The PCI of the DDNIC interfaces to the host system PCI bus. The PCI allows the exchange of information between the host system and its DDNIC. Information exchanged at the PCI consists of information to be transferred through the DDNIC and control and operation information used within a DDNIC and between DDNIC and its host system. The other interface of the DDNIC is the optical interface. The optical interface is used to connect the DDNIC to a fiber optic network. Typically in the Owl Data Diode System, the fiber optic network consists of a fiber optic cable connected to another DDNIC. These interfaces of the DDNIC do not enforce the TSF and cannot be used to modify the TSF, as the TSF are physically enforced by each DDNIC at the board-component level.

2.3.2 Logical Boundaries

The logical boundaries of the TOE can be described in the terms of the security functions that the TOE provides.

User Data Protection: Each DDNIC protects itself by not exporting any interface that can be used to modify the TOE and thereby the Target Security Functions (TSF) of the TOE. The only interfaces exported are the PCI Bus and the network fiber optical interface of the DDNIC, which are not relevant to the TSF. Furthermore, no interface is exported which can alter the operation of the TOE since the TOE has been manufactured to physically enforce its policies and would have to be physically modified to change its behavior and violate the TSF. Since the TOE environment is assumed to provide adequate physical protection it is essentially impossible to modify the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interfaces are limited to primarily support only network traffic. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic. The TOE includes two Data Diode NIC integrated circuit cards that are each connected to a standard PCI slot in a computer and may be connected to each other using fiber optic network interfaces and a fiber optic cable.

Given the assumption that all relevant data must pass through the TOE, and all information received by the TOE is unconditionally subject to its unidirectional information flow policy, there is no possibility to bypass this security mechanism. There is only one path for information flow through each Owl Data Diode Network Interface Card, and that path only allows unidirectional information flow across the card. As there is physically only one path available for information flow, that path cannot be bypassed.

For the unidirectional flow to occur across a given DDNIC, the DDNIC must function correctly. If a DDNIC is not functioning or is malfunctioning, only unidirectional information flow is permitted, or no information flow occurs. The Send-Only DDNIC only allows information to flow from the host system across the card to the external optical interface. The Receive-Only DDNIC only allows information to flow from the external optical interface across the card to the host system.

The Owl Data Diode System becomes part of the security domains of the two separate host systems for its own execution. The Owl Data Diode System works in conjunction with the separation that exists between the security domains of two separate host networks. The security domain in which each Owl DDNIC is hosted protects the DDNIC from interference and tampering by untrusted subjects. Furthermore, each DDNIC protects itself by not exporting any interface that can be used to modify the Target Security Functions (TSF) of the DDNIC. The only interfaces exported are the PCI Bus interface and the optical interface of the DDNIC, which are not relevant to the TSF. No interface is exported which can alter the operation of the TOE since the TOE has been manufactured to physically enforce its policies and would have to be physically modified to violate the TSF.

TSF Protection: Each DDNIC protects itself by not exporting any interface that can be used to modify the TOE and thereby the Target Security Functions (TSF) of the TOE. The only interfaces exported are the PCI Bus and the network fiber optical interface of the DDNIC, which are not relevant to the TSF. Furthermore, no interface is exported which can alter the operation of the TOE since the TOE has been manufactured to physically enforce its policies and would have to be physically modified to change its behavior and violate the TSF. Since the TOE environment is assumed to provide adequate physical protection it is essentially impossible to modify the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic.

3 Security Policy

The Security Target identified the following Security Policies for the evaluated product:

P.ONEWAY	Information must be able to flow only in a single direction between attached hosts.

4 Assumptions

The following assumptions are identified in the Security Target:

A.ADMIN The administrator will properly adhere to the TOE guidance.

A.CONNECTION The TOE will be installed such that all relevant network traffic will flow through the TOE and hence be subject to itself information flow policy.

A.PHYSICAL The TOE will be physically protected to a degree commensurate with the value of the information it is intended to protect.

5 Architectural Information

The Owl Computing Technologies, Incorporated (Owl) Data Diode System provides an absolute one-way connection between a sending host system or network and a receiving host system or network. Information is permitted to flow from the sending host system or network to the receiving host system or network. Data, information, or communications originating at the receiving host system or network are not allowed to flow to the sending host system or network via the Owl Data Diode System.

The Target of Evaluation (TOE) comprises two Owl Data Diode Network Interface Cards (DDNICs), the Send-Only DDNIC and the Receive-Only DDNIC, and their respective driver software. The DDNICs are manufactured to Owl's specifications using commercial-off-the-shelf (COTS) Asynchronous Transfer Mode network interface card components. Driver software is designed, written, and packaged by Owl.

Each Data Diode NIC connects to a standard PCI slot in a host system and each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode Network Interface Card (DDNIC) is used only for sending information, the Send-Only DDNIC. The other DDNIC is used only for receiving information, the Receive-Only DDNIC. The Send-Only DDNIC exports light pulses converted by the Optical Transmitter from electrical voltages. The Receive-Only DDNIC imports light pulses received at the photo detector of the Optical Receiver of the Receive-Only DDNIC and converts the light pulses to electrical voltages.

6 Documentation

Purchasers of Owl Computing Technologies Data Diode Network Interface Card version 4 will receive the following documentation:

- Owl Computing Technologies, Inc., Version 4 Card (type 236) OEM Installation Manual for All Operating Systems, Document Release 01i, 6/09/2006.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

Owl's approach to security testing for Owl Computing Technologies Data Diode Network Interface Card version 4 involved tests of interfaces identified in the Functional Specification and the High-Level Design. Each test is directly mapped to the security function tested. The vendor tested both of the TOE Security Functions Information Flow and TOE Self Protection.

The vendor's tests completed successfully and the vendor archived all test results in the Configuration Management repository.

The developer's test configuration consisted of two machines with an ATM network between them. In the base configuration as submitted for EAL4 testing, the two machines are connected only with a single simplex optical fiber. The test configuration included both versions of the TOE.

SAIC and the vendor consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configuration in the ETR, Part 2.

The Evaluation Team determined that the vendor's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team followed the procedures in the OEM Installation Manual and User Guide, Version 1m to install the TOE. The evaluation team installed one send and one receive card using the procedures provided.

The evaluation team executed the entire vendor test suite consisting of six manual tests. They completely analyzed the results from the completed vendor test suite run. This ensures that the Evaluation Team adequately addressed all security functions. The Evaluation Team used the developer's test configurations to perform the tests.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team conducted a brainstorming session to identify penetration test cases based on the vendor's vulnerability assessment documentation. The Evaluation Team used the vendor's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence

8 Evaluated Configuration

The team executed the tests in the following test configuration:

- One laptop computer with a send-only card was used to transmit data over a simplex optical fiber,
- One laptop computer with a receive-only card was used to receive data over a simplex optical fiber,
- An additional pair of production cards were supplied for inspection
- One version of the TOE was tested: Version 4
- Driver Software (V4.16 for Windows)

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.3 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance components. 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.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for Owl Computing Technologies Data Diode Network Interface Card version 4 Part 2, dated January 26, 2007" which is considered proprietary.

Section 6.2, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> “The verdicts for each CEM work unit in the ETR sections included in Section 15 are each “PASS”. Therefore, when configured according to the following guidance documentation:
>
> - Owl Computing Technologies, Inc., Version 4 Card (type 236) OEM Installation Manual for All Operating Systems, Document Release 01i, 6/09/2006
>
> The Data Diode TOE satisfies the – Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification, Version r01g, 12/08/06. ”

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The TOE is relatively simplistic in nature due to its technology type and consequently the testing and evaluation as a whole was very straight forward. The validator has no additional recommendations or precautions concerning the TOE.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification, Version r01g, 12/08/06.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4.

13 Glossary

The following definitions are used throughout this document:

ATM PHY: The Asynchronous Transfer Mode (ATM) Physical Interface Device (ATM PHY or PHY) is a high performance physical layer interface device on the Data Diode Network Interface Cards that generates and receives high-speed data streams. The ATM PHY receives 53-byte ATM cells from the SAR and produces analog signals that are passed to the transceiver. The interface into the ATM PHY from the SAR uses the UTOPIA protocol and the interface to the transceiver is SONET over analog power pins.
They are the Segmentation and Reassembly Controller, the Asynchronous Transfer Mode (ATM) Physical Interface Device, and the ATM Multimode Fiber Transceiver.

Data Diode Network Interface Card (DDNIC): A network interface card consisting of three functional components; the Segmentation and Reassembly Controller (SAR), the ATM Physical Interface Device (PHY), and the ATM Multimode Fiber Transceiver. The DDNICs are manufactured to Owl's specifications and use commercial-off-the-shelf (COTS) Asynchronous Transfer Mode network interface card components. One Data Diode Network Interface Card (DDNIC) is used only for sending information, the Send-Only DDNIC. The other DDNIC is used only for receiving information, the Receive-Only DDNIC. The Send-Only DDNIC exports light pulses converted by the Optical Transceiver from electrical voltages. The Receive-Only DDNIC imports light pulses received at the photo detector of the Optical Transceiver of the Receive-Only DDNIC and converts the light pulses to electrical voltages.

Data Diode Host: A computer system or network in which a Data Diode is installed. The host system or network is the system that provides power to the Data Diode. The Data Diode is digitally connected to the host via the Peripheral Component Interface (PCI).

Gateway: Also called a router, a gateway is a program or a special-purpose host that transfers network traffic with an identifiable network address from one network to another until the final destination is reached.

Host: A general term for a computer system. Once specific application software or hardware is installed on a host it assumes the role of Data Diode Host, gateway, receiving Host, Sending Host.

NIC: Network Interface Card that provides the physical interface to a network.

PCI: The Peripheral Component Interface connects to the PCI Bus of the host system.is the device driver interface into the TOE from the host computer. The PCI Bus is an open architecture bus structure to control devices. Composed of a PCI BIOS, CPU, CPU cache, system cache, system memory, PCI Bridge, and Peripheral bus.

Receive-Only DDNIC: The Receive-Only DDNIC only allows information for transfer to flow from its optical interface across the Receive-Only DDNIC and to the host system. All information presented for transfer to the Receive-Only DDNIC is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDNIC and through the optical interface of the Receive-Only DDNIC. This non-bypassability of the TOE is enforced at the physical level.

Receiving Host: A host system or network in which a Receive-Only DDNIC is installed. The Receiveing Host is to receive information through the Receive-Only Data Diode Network Interface Card.

SAR: The Segmentation and Reassembly Controller (SAR). The SAR is a functional component of the Data Diode Network Interface Card. The SAR. The SAR connects directly to the PCI bus of the host system and to the PHY. When transmitting, the SAR segments the data into 48 byte ATM data payloads or "cells.” The SAR then frames each cell with AAL5 headers for complete 53-byte ATM cells, which are then sent on for framing and serialization. When receiving, ATM data cells are transferred and reassembled directly into host memory by the SAR into pre-allocated memory buffers.

Sending Host: A host system or network in which a Send-Only DDNIC is insta..ed. The Sending Host is to send information through the Send-only Data Diode Network interface Card.

Send-Only DDNIC: The Send-Only DDNIC only allows information for transfer to flow from the host system across the DDNIC through the optical interface. All information presented to the Send-Only DDNIC is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDNIC through the optical interface across the Send-Only DDNIC and into the host system. This non-bypassability of the TOE is enforced at the physical level.

SONET Protocol: The interface between the ATM PHY and the transceiver provides both Transmission Convergence (TC) and Physical Media Dependent (PMD) sub-layer functions of an ATM PHY suitable for ATM networks.

UTOPIA Protocol: The UTOPIA (Universal Test and Operations PHY Interface for ATM) interface is the protocol used between the SAR and the ATM PHY. UTOPIA is a standard data path handshake protocol.

14 Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CM	Configuration Management
DDNIC	Data Diode Network Interface Card
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IATF	Information Assurance Technical Framework
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
QA	Quality Assurance
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTAP/CCEVS	Trusted Technology Assessment Program / Common Criteria Evaluation and Validation Scheme

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408).

[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[5] Evaluation Technical Report for the Owl Data Diode Product Part II.

[6] Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification, Version r01g, 12/08/06.

[7] Owl Computing Technologies, Inc., Version 4 Card (type 236) OEM Installation Manual for All Operating Systems, Document Release 01i, 6/09/2006.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.