National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Odyssey Access Client (FIPS Edition), Version 4.56

Report Number: CCEVS-VR-VID10245-2008
Dated: September 23, 2008
Version: 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

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the Odyssey Access Client (FIPS Edition), Version 4.56, a product of Juniper Networks,

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The Odyssey Access Client (FIPS Edition), Version 4.56, hereafter referred to as OAC or the product, is a software-only access client for wireless and wired 802.1X networks. The OAC provides IEEE 802.1X access client software that supports Wireless Local Area Network (WLAN) security protocols required for wireless access to LANs. In conjunction with an 802.1X-compatible authentication server (not part of the TOE), OAC supports mutual authentication between the user and the network, protects the confidentiality of user data between the client node and the trusted network, and maintains data privacy over the wireless link. OAC also supports wired 802.1X network connections. OAC includes a FIPS 140-2 Level 1 validated cryptographic module.

The evaluation of the Odyssey Access Client (FIPS Edition) was performed by the SAIC Common Criteria Testing Laboratory (CCTL) in the United States and was completed during July 2008. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC with support from Juniper Networks. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL3, augmented with Basic Flaw Remediation (ALC_FLR.2) from the Common Criteria version 2.3 [CC] using the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is further conformant to the US Government Protection Profile Wireless Local Area Network (WLAN) Client for Basic Robustness Environments, March 2006, Version 1.0.

The Strength of Function (SOF) claim is SOF-basic.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site http://www.niap-ccevs.org/cc-scheme.

2. Identification

Target of Evaluation:	Odyssey Access Client (FIPS Edition), Version 4.56
Developer:	Juniper Networks 1194 North Mathilda Avenue Sunnyvale, CA 94089-1206
Security of Target	Juniper Networks Odyssey Access Client (FIPS Edition) Security Target, Version 1.0, August 5, 2008
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, Maryland 21046
Evaluators	Cynthia Reese, SAIC Marie Evencie Pierre, SAIC
Validator:	Robin J. Medlock, The MITRE Corporation Sunil J. Trivedi, The MITRE Corporation
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005
Protection Profile:	US Government Protection Profile Wireless Local Area Network (WLAN) Client for Basic Robustness Environments, March 2006, Version 1.0

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

- **Security Audit** - The TOE is able to generate audit records for errors detected during cryptographic key transfer, destruction of a cryptographic key, dropping a packet that

fails to satisfy the Wireless Client Encryption Policy set by an administrator, changing the TOE encryption algorithm or turning off the cryptographic feature, changes to cryptographic key data, and success or failure of the self test. For each audit record, the TOE records date and time of the event, type of the event, subject identity (if it is applicable) and success or failure of the event. The TOE relies on the IT environment to supply a reliable time stamp from which it can obtain the date and time recorded in the audit record.

- **Cryptographic Support** - The TOE incorporates the Odyssey Security Component, which is a FIPS 140-2 Level 1 validated cryptographic module. It provides key generation and the following FIPS-validated cryptographic algorithms to support secure wireless communications in the evaluated configuration:
  - Advanced Encryption Standard (AES) – symmetric data encryption and decryption (CBC and CCM modes), message authentication (CCM mode)
  - Digital Signature Algorithm (DSA) – digital signature generation and verification
  - Rivest-Shamir-Adelman (RSA) – digital signature generation and verification, and asymmetric encryption for key wrapping
  - Keyed-Hash Message Authentication Code (HMAC) with supporting Secure Hash Algorithm (SHA-1) – message authentication.

  In addition, the Odyssey Security Component implements the Diffie-Hellman key agreement algorithm, which is a non-approved algorithm that nevertheless is allowed for use in FIPS 140-2 mode for key agreement purposes.
- **User Data Protection** - The TOE enforces the Wireless Client Encryption Policy between the WLAN client and the WLAN access point or system. The Wireless Client Encryption Policy requires the encryption of user data between the client and the access point. In implementing the Wireless Client Encryption Policy, the TOE in its evaluated configuration supports authentication protocols that require the network to authenticate to the TOE (as well as authenticating the TOE user to the network) before establishing secure communication between the WLAN client and the WLAN access point or system.
- **Security Management** - The TOE provides GUI tools to support management and administration of the access client. The management functions available include enabling and disabling security audit, configuring the TOE in FIPS mode to support communication in conformance with the Wireless Client Encryption Policy, and managing the functions of the FIPS 140 validated cryptographic module. The TOE relies on the IT environment to define an Administrator security management role and to enforce restrictions on access to management functions to the Administrator.
- **Protection of TSF** - The TOE protects TOE Security Function (TSF) data by providing cryptographic functions to verify the integrity of all TOE data and stored TOE executable code. The TOE runs the suite of self-tests provided by its FIPS validated module during the initial start up, after manual entry of master key material and upon the administrator's request. The self-tests demonstrate the correctness of the TOE's cryptographic operations.

A summary of the SFRs for the TOE and IT environment are included in the following tables.

TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN_EXP.1 Explicit: Audit Data Generation
FCS: Cryptographic support	FCS_BCM_EXP.1 Explicit: Baseline Cryptographic Module
	FCS_CKM.1(1): Cryptographic Key Generation (AES, HMAC)
	FCS_CKM_EXP.2 Explicit: Cryptographic Key Establishment
	FCS_CKM.4 Cryptographic Key Destruction
	FCS_COP_EXP.1 Explicit: Random Number Generation
	FCS_COP_EXP.2(1) Explicit: Cryptographic Operation (AES)
	FCS_COP_EXP.2(2) Explicit: Cryptographic Operation (Message Authentication for WPA2 Association)
	FCS_COP_EXP.2(3) Explicit: Cryptographic Operation (Message Authentication for xSec Association)
	FCS_COP_EXP.2(4) Explicit: Cryptographic Operation (Digital Signature Verification – DSA)
	FCS_COP_EXP.2(5) Explicit: Cryptographic Operation (Digital Signature Verification – RSA)
	FCS_COP_EXP.2(6) Explicit: Cryptographic Operation (Asymmetric Encryption for Key Wrapping)
	FCS_COP_EXP.2(7) Explicit: Cryptographic Operation (Diffie-Hellman Key Agreement)
	FCS_COP_EXP.2(8) Explicit: Cryptographic Operation (Secure Hash for Integrity Verification)
FDP: User data protection	FDP_IFC.1 Subset information flow control (Wireless Client Encryption Policy)
	FDP_IFF.1 Simple Security Attributes (Wireless Client Policy)
	FDP_RIP.1(1) Subset Residual Information Protection
FMT: Security management	FMT_MSA.2 Secure Security Attributes
	FMT_MSA.3 Static Attribute Initialization
	FMT_SMF.1(1) Specification of Management Functions (Cryptographic Function)
	FMT_SMF.1(2) Specification of Management Functions (Audit Record Generation)
	FMT_SMF.1(3) Management of TSF data (Cryptographic Key Data)
FPT: Protection of the TSF	FPT_TST_EXP.1 TSF Testing
	FPT_TST_EXP.2 TSF Testing of Cryptographic Modules
FTP: Trusted path	FTP_ITC.1 Inter-TSF Trusted Channel

IT Environment Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.2 User identity association
	FAU_SAA.1 Potential violation analysis
	FAU_SAR.1 Audit Review
	FAU_SAR.2 Restricted Audit Review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1 Selective audit
	FAU_STG.1 Protected audit trail storage
	FAU_STG.3 Action in case of possible audit data loss
FCS: Cryptographic Support	FCS_CKM.1(2) Cryptographic Key Generation (DSA)
	FCS_CKM.1(3) Cryptographic Key Generation (RSA)
	FCS_COP_EXP.2(9) Explicit: Cryptographic Operation (Digital Signature Generation– DSA)
	FCS_COP_EXP.2(10) Explicit: Cryptographic Operation (Digital Signature Generation– RSA)
FDP: User Data Protection	FDP_RIP.1(2) Subset Residual Information Protection
FIA: Identification & Authentication	FIA_USB.1 User-subject Binding
FMT: Security Management	FMT_MOF.1 Management of Security Functions Behavior
	FMT_MTD.1 Management of TSF Data (Time TSF Data)
	FMT_SMR.1 Security Roles
FPT: Protection of the TSF	FPT_RVM.1 Non Bypassability of the TSP
	FPT_SEP.1 TOE IT Environment Domain Separation
	FPT_STM.1 Reliable Time Stamps

4. Assumptions and Clarification of Scope

4.1 Secure Usage Assumptions

This section describes the secure usage assumptions, which are those items that the TOE itself cannot implement or enforce

A.BASIC_ROBUSTNESS_IT_ ENVIRONMENT	The TOE is a Wireless LAN client and is expected to be installed in an IT environment (e.g. PC hardware and O/S) that can appropriately address those threats and policies identified in "Table 3: Basic Robustness Threats NOT Applicable to the TOE"[1] and meets the IT environmental requirements necessary to support the correct operation of the TOE.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.

4.2 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 (EAL3 augmented with Basic Flaw Remediation (ALC_FLR.2) 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 EAL3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. OAC provides a number of EAP authentication methods, including EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security),

[1] See Table 3 in Section 3.2 of the US Government Protection Profile Wireless Local Area Network (WLAN) Client For Basic Robustness Environments, March 2006, Version 1.0.

and EAP-PEAP (Protected EAP) that support mutual authentication of the user and network.

OAC also supports EAP-FAST (Flexible Authentication via Secure Tunneling) and EAP-LEAP (Lightweight EAP), but these proprietary protocols have documented vulnerabilities and so are excluded from the evaluated configuration. In addition, it is possible to configure a network connection without data encryption. This can only be done when associating in open mode and is typical for wireless hotspots. Because it is inherently insecure, it is not included in the evaluated configuration.

5. TOE depends on the IT environment for the following:
   - To use FIPS 140-2 compliant encryption with WPA2, an adapter driver that is compatible with the Odyssey Security Component must be installed on the computer on which the TOE is installed. Juniper Networks has made a driver available that works with the Atheros 5000 family of chipsets, which are used in many wireless adapters. Juniper has verified operation with: Cisco Aironet CB21 a/b/g Wireless CardBus Adapter; Netgear WAG511 802.11a/b/g Dual Band PC Card; and 3Com 3CRPAG175B Wireless 802.11 a/b/g PC card.
   - To support wireless network authentication, the network must include at least one 802.1X-compliant access point.
   - To support wired network authentication, the network must include at least one 802.1X-compliant switch or hub.
   - To associate to a network using xSec, the network must include xSec-compliant hardware capable of implementing the xSec protocol.
   - To support mutual authentication, the network must include at least one 802.1X-compatible authentication server – e.g., a RADIUS server such as Steel-Belted RADIUS version 5.4.

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

5. Architectural Information

The following figure is a high-level architecture of the TOE within its intended environment.

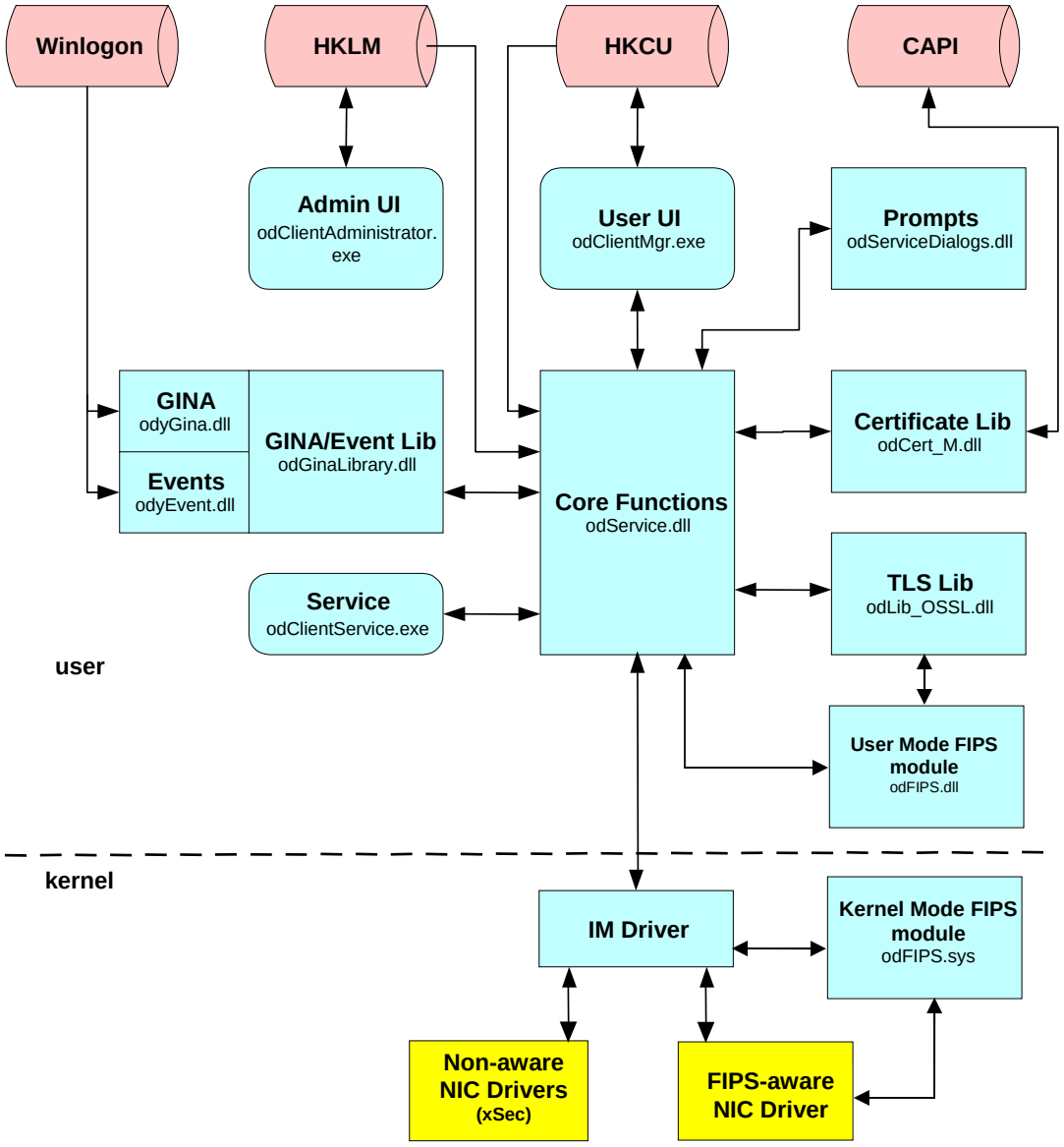

Figure 1: TOE High-Level Architecture

The components of the TOE are shaded in blue in the preceding figure. The TOE is composed of two types of components:

- User mode components
- Kernel mode component.

The user mode components rely on the operating system in the environment of the TOE, while the IM driver runs in the kernel of the operating system.

The user mode components of the TOE comprise Service Components, User Interface Components and Windows Logon Components, as follows:

- Service Components:

- Service (odClientService.exe) – runs as a Windows service under the Service Control Manager (SCM) and hosts odService.dll
- Core function (odService.dll) – core logic for radio control, authentication and key management
- TLS Lib (odLib_OSSL.dll) – implements Transport Layer Security (TLS) for use by Extensible Authentication Protocol (EAP)
- Certificate Lib (odCert_M.dll) – provides certificate and certificate store functions, via Microsoft Cryptographic API (CAPI). Separate implementations are available for non-Windows platforms, but these are not in the evaluated configuration
- odSCard.dll (not depicted in Figure 1) – provides a support library and interface for an installed Subscriber Identity Module (SIM) smart card

Each of the Service Components contributes directly or indirectly to supporting the TOE security functions.

- User Interface Components:
  - User UI (odClientMgr.exe) – this is the Odyssey Client Manager. It is a user configuration utility that enables the user to configure and control the OAC. It manages OAC data stored in the registry of the underlying operating system (specifically, in HKCU), and displays the status of the client and its network connections
  - Administrator UI (odClientAdministrator.exe) – this is the Odyssey Client Administrator. It is an administration utility that enables an administrator to configure and lock initial and connection settings. It manages OAC data stored in the registry of the underlying operating system (specifically, in HKLM), and is restricted to users that have administrator privilege in the underlying operating system.
  - Prompts (odServiceDialogs.dll) – displays various auxiliary dialogs and prompts that are called asynchronously by the Odyssey Service (e.g., password, token, certificate trust)
  - odTray.exe (not depicted in Figure 1) – application that runs in the Windows in-tray section of the desktop. It displays the OAC tray icon and shows the general status of the TOE
  - Resource files (not depicted in Figure 1) – comprises various localizable resources that are segregated into several resource DLLs

  The User UI and Administrator UI contribute directly or indirectly to supporting the TOE security functions.

- Windows Logon Components
  - GINA (odyGina.dll) – intercepts the Microsoft graphical identification and authentication (GINA) library to allow users to connect to the network using their Windows logon credentials prior to Windows logon

- Events (odyEvent.dll) – registers as a Winlogon Notification Package, which allows 802.1X connection immediately after Windows logon and prior to display of the desktop. This permits timely connection to network resources, such as logon scripts and mapped drives
- GINA/Event Lib (odGinaLibrary.dll) – provides services to odyGina and odyEvent. It manages user authentication just before or after Windows logon and manages machine authentication
- odLogin.dll (not depicted in Figure 1) – registers as a Windows Network Provider and captures the username and password upon Windows logon for 802.1X authentication.

Each of the Windows Logon components contributes directly or indirectly to supporting the TOE security functions.

On the other hand, the TOE's kernel component runs as an intermediate (IM) driver between the TOE user components and the Network Interface Card within the environment of the TOE:

- IM Driver (OdysseyIM4.sys) – comprises a Network Driver Interface Specification (NDIS) intermediate driver that communicates with odService via I/O Request Packet (IRP) and provides the following services:
  - Issues OIDs to the NIC driver
  - Transmits and receives EAPOL (EAP over LAN) packets
  - Receives status indications from the NIC driver
  - Manages MEDIA_CONNECT/DISCONNECT.

To support FIPS mode, the TOE includes the Odyssey Security Component (odFIPS module), which is FIPS 140-2 Level 1 certified. The odFIPS module comprises two components: odFIPS.dll for Windows user mode; and odFIPS.sys for Windows kernel mode.

Each of the kernel mode components contributes directly or indirectly to supporting the TOE security functions. In particular, the IM driver ensures all packets to be sent to the network interface card are encrypted.

The TOE provides separate graphical user interfaces (GUIs) for users and administrators. Users can access the TOE through its "Odyssey Client Manager" interface. Depending on the TOE's configuration, the user can use the Client Manager to perform some or all of the following tasks:

- Connect to a network using a wireless or wired connection
- Reconnect to a Network
- Re-authenticate to a Network
- View Connection Information
- Add a Wireless or Wired Adapter

- Create a user profile and configure authentication for that profile
- Add or edit network properties
- Configure trusted servers.

Administrators access the TOE through its "Odyssey Client Administrator" interface. The Client Administrator provides the administrator with the following set of tools to perform the following tasks:

- Connection Settings – Configure when the client connects to the network (at Windows startup, prior to Windows logon, after Windows logon but before the desktop appears, or after the desktop appears)
- Initial Settings – Specify initial settings for user network connections and to configure preconfigured installers, updated user configuration files, or network settings for user connections that take place prior to Windows logon
- Machine Account – configure a machine network connection
- Permissions Editor – apply customized feature-by-feature restrictions on the user's ability to modify TOE configurations
- Merge Rules – set rules used in creating a settings update file or a new custom installer
- Custom Installer – create a preconfigured installer file from the initial or machine settings
- Script Composer – create configuration scripts used to define or update client configurations
- Plugin Settings – enables, disables, or reloads plug-ins for OAC.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

1. Juniper Networks Odyssey Access Client (FIPS Edition) Security Target, Version 1.0, August 5, 2008.
2. Juniper Networks Odyssey Access Client for Windows Administration Guide, Enterprise Edition FIPS Edition Release 4.56, July 2008
3. Juniper Networks Odyssey Access Client for Windows User Guide, Enterprise Edition FIPS Edition Release 4.56, April 2008
4. Juniper Networks Odyssey Access Client for Windows Release Notes, Enterprise Edition FIPS Edition Release 4.56, April 2008

7. IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. The evaluation team determined that both the test configuration of the vendor testing and of the team testing efforts substantiated the evaluated configuration as specified in the Security Target and in the installation and configuration guidance. Additional information regarding the test configuration the evaluation team testing activity is included in the Final Evaluation Report.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered all the security functional requirements in the ST. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL3 evaluation.

7.1.1 Test Configuration for Wireless Test Bed

This section describes the test configuration for WPA2 and wireless xSec. The test bed is depicted in the figure below:

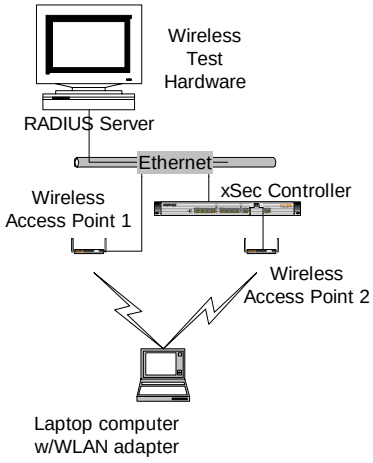

Figure 2: Wireless Test Bed

Hardware

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - None
- IT Environment Hardware
  - RADIUS Server: Generic Windows 2003 Server computer. The purpose of this component is to host Juniper Steel-Belted RADIUS. This may be a virtual machine.
  - xSec Controller: Aruba 800 Mobility Controller. The purpose of this component is to terminate the xSec connection in all tests involving xSec.
  - Wireless Access Point 1: Generic 802.11 WPA2-compatible wireless access points. (A Cisco 1130 will be used.) The access point acts as the 802.11 endpoint and as the 802.1x authenticator
  - Wireless Access Point 2: Aruba 52 access point. This access point acts as the 802.11 endpoint and as the 802.1x authenticator for the xSec connections.
  - Client computer: Generic Windows XP SP 2 computer. The purpose of this component is to host the TOE for all wireless tests. The client computer must have a wireless LAN adapter using the Atheros 500X chipset or the Intel Pro/Wireless chipset. (A Cisco Aironet CB21AG will be used.)Two client computers will be used. One will have a Cisco Aironet CB21AG PC Card, which uses the Atheros chipset. The other client computer will have an integrated wireless adapter using the Intel chipset.

- Test Hardware
    - None.

Software

The following software is necessary to create the test configuration:

- TOE Software
    - Juniper Networks Odyssey Access Client FIPS Edition, Version 4.56. This component runs on the Client computer.
- IT Environment Software
    - Microsoft Windows XP SP 2 - This component runs on the Client computer. Its purpose is to provide the operating system for these computers. While this test plan only uses Windows XP SP 2, the TOE supports other Service Pack levels of Windows XP as well as all service pack levels of Windows 2000. The TOE comprises the same product and guidance documentation for all those variants of Windows. The design documentation also applies equally to all of them.
    - Microsoft Windows 2003 Server - This component runs on RADIUS Server computer. Its purpose is to provide the operating system for that computer.
    - Atheros/Juniper NIC Driver, version 1.3.1.0. This component runs on the client computer. Its purpose is to enable the wireless NIC to delegate cryptographic operations to the FIPS module when the TOE is in FIPS mode.
    - Intel/Juniper NIC Driver, version 11.1.1.16. This component runs on the client computer. Its purpose is to enable the wireless NIC to delegate cryptographic operations to the FIPS module when the TOE is in FIPS mode.
    - Juniper Networks Steel-Belted RADIUS, Version 5.4. This component runs on the Server computer. Its purpose is to act as the Authentication Server within the 802.1x protocol, supporting all tests that involve a network connection.
- Test Software

None.

7.1.2 Test Configuration for wired xSec Test Bed

This section describes the test configuration for wired xSec. The test bed is depicted in the figure below:

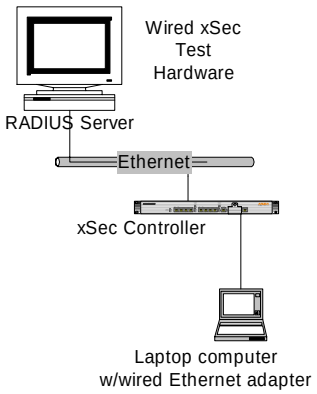

Figure 3: Wired xSec Test Bed

Hardware

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - None
- IT Environment Hardware
  - RADIUS Server: Generic Windows Server computer. The purpose of this component is to host Juniper Steel-Belted RADIUS.
  - xSec Controller: Aruba 800 Mobility Controller. The purpose of this component is to terminate the xSec connection in all tests involving xSec.
  - Client computer: Generic Windows XP computer with a generic wired Ethernet adapter. The purpose of this component is to host the TOE for all tests involving wired xSec.
- Test Hardware
  - None.

Software

The following software is necessary to create the test configuration:

- TOE Software
  - Juniper Networks Odyssey Access Client FIPS Edition, Version 4.56. This component runs on the Client computer.
- IT Environment Software
  - Microsoft Windows XP Professional, Service Pack 2 - This component runs on the Client computer. Its purpose is to provide the operating system for that computer.

- Microsoft Windows Server 2003 Standard Edition, Service Pack 2 - This component runs on the Server computer. Its purpose is to provide the operating system for that computer.
- Juniper Networks Steel-Belted RADIUS, Version 5.41. This component runs on the Server computer. Its purpose is to act as the Authentication Server within the 802.1x protocol, supporting all tests that involve a network connection.

- Test Software

None

7.2 Evaluator Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the TSFI and security functions as described in the functional specification. The evaluation team performed 50% of the developer's test suite. The evaluation team devised and conducted an independent set of team tests and penetration tests.

7.3 Strength of Function

The US Government Wireless Local Area Network (WLAN) Client Protection Profile (PP) provides rationale for the minimum strength of function claim made for the TOE security functional requirements. The rationale (provided in Section 6.7 of the US Government Wireless Local Area Network (WLAN) Client PP) is valid for this product's Security Target as no new security objectives were added.

8. Evaluated Configuration

This section describes the TOE in its evaluated configuration. Further details can be found in the Appendix A of the Juniper Networks Odyssey Access Client for Windows Administration Guide, Enterprise Edition FIPS Edition Release 4.56, July 2008.

9. Results of 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 EAL3 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.

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.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.
>
> A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 3) requirements. The rationale supporting each CEM work unit verdict is recorded in the "Final Evaluation Technical Report for Juniper Networks Odyssey Access Client (FIPS Edition) Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> Section 6.1, ST Evaluation: Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Juniper Odyssey Access Client (FIPS Edition) ST is a CC compliant ST.
>
> Section 6.2, TOE Evaluation: The verdicts for each CEM work unit in the Proprietary part of the ETR are each "PASS". Therefore, when configured and operated according to the guidance documentation identified in the Section 6, the Juniper Odyssey Access Client (FIPS Edition) TOE satisfies all of the security functional requirements stated in the Security Target, identified in Section 11.

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 following comments and recommendations are offered:

1. The evaluated version is not suitable for Windows Vista. Juniper markets a separate version, OAC 4.8 for Windows Vista which is not an evaluated version. Similarly other versions of OAC suitable for other operating systems and platform marketed by Juniper are not evaluated.

2. From the Juniper web site, http://www.juniper.net/products_and_services/aaa_and_802_1x/odyssey/, it appears that Juniper markets OAC together with an 802.1X-compatible RADIUS server such as Juniper Networks' Odyssey Access Server or Steel-Belted Radius®. It should be noted that 802.1X-compatible RADIUS servers were not part of this evaluation.

The Validation Team agreed with the conclusion of the SAIC CCTL Evaluation Team, and an EAL3 augmented with Basic Flaw Remediation (ALC_FLR.2) certificate rating is issued for the Juniper Network Odyssey Access Client (FIPS Edition), Version 4.56.

11. Security Target

Juniper Networks Odyssey Access Client (FIPS Edition) Security Target, Version 1.0, August 5, 2008 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex B of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report and evaluation.

ACL	**Access Control List**
ACM	**Configuration Management**
ADO	**Delivery and Operation**
ADV	**Development**
AEC	**Advanced Event Correlation**
AES	**Advanced Encryption Standard**
AGD	**Guidance Documents**
AMS	**Alert Management System**
API	**Application Programming Interfact**
ATE	**Tests**
AVA	**Vulnerability Assessment**
CC	**Common Criteria for Information Technology Security Evaluation**
CCEVS	**Common Criteria Evaluation and Validation Scheme**
CEM	**Common Methodology for Information Technology Security Evaluation**
CLI	**Command Line Interface**
CM	**Configuration Management**
EAL	**Evaluation Assurance Level**
EM	**Event Manager**
FAU	**Security Audit**
FDP	**User Data Protection**
FIA	**Identification and Authentication**
FMT	**Security Management**
FPT	**Protection of the TSF**
FTA	**TOE Access**
FTP	**Trusted Channels/Path**
GUI	**Graphical User Interface**
HTTPS	**Hypertext Transfer Protocols over SSL**
ID	**Identification**
IP	**Internet Protocol**

IT	**Information Technology**
NIAP	**National Information Assurance Partnership**
NIST	**National Institute of Standards and Technology**
NSA	**National Security Agency**
OS	**Operating System**
PC	**Personal Computer**
PP	**Protection Profile**
RSA	**Rivest Shamir Adleman**
SF	**Security Function**
SFP	**Security Function Policy**
SHA1	**Secure Hash Algorithm**
SOF	**Strength of Function**
SP	**Service Pack**
SQL	**Structured Query Language**
SSL	**Secure Socket Layer**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
TSC	**TSF Scope of Control**
TSF	**TOE Security Functions**
TSFI	**TOE Security Functions Interface**
TSP	**TOE Security Policy**

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS) http://www.niap-ccevs.org/cc-scheme
- SAIC CCTL http://www.saic.com/infosec/common-criteria
- Juniper Networks: http://www.juniper.net

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

Other Documents

- [ST] Juniper Networks Odyssey Access Client (FIPS Edition) Security Target, Version 1.0, August 5, 2008.