Juniper Networks Odyssey Access Client (FIPS Edition) Security Target

Version 1.0
05 August 2008

Prepared for:
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089-1206

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

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation, ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation (TOE) is Odyssey Access Client (FIPS Edition), Version 4.56, provided by Juniper Networks. Odyssey Access Client (OAC) is a software-only access client for wireless and wired 802.1X networks. It 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 Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claim (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Juniper Networks Odyssey Access Client (FIPS Edition) Security Target

ST Version – Version 1.0

ST Date – 05 August 2008

TOE Identification – Odyssey Access Client (FIPS Edition), Version 4.56

TOE Developer – Juniper Networks

Evaluation Sponsor – Juniper Networks

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This TOE is conformant to the following Common Criteria (CC) specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - Assurance Level: EAL 3 Augmented with ALC_FLR.2
    - Strength of Function (SOF) Claim: SOF-basic

- The TOE is further conformant to the US Government Protection Profile Wireless Local Area Network (WLAN) Client For Basic Robustness Environments, March 2006, Version 1.0.

1.3 Conventions, Terminology and Acronyms

1.3.1 Conventions

This Security Target reproduces the security requirements specified in the US Government Protection Profile Wireless Local Area Network (WLAN) Client For Basic Robustness Environments, March 2006, Version 1.0, including the formatting conventions used in the PP. These conventions are described in the subsection "Conventions and Terminology" on page v of the PP. Where the Security Target completes assignment and selection operations left incomplete in the PP, or performs tailoring in the form of refinements, the following conventions are used:

- Security Functional Requirements (SFRs) – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FMT_MTD.1(1) and FMT_MTD.1(1) indicate that the ST includes two iterations of the FMT_MTD.1 requirement, 1 and 2.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The PP also specifies a number of explicitly stated security functional requirements. Explicitly stated requirements provide for the specification of a new class or family of components to be created to address TOE-specific requirements that are not readily drawn from the CC. The PP convention, reproduced in this ST, is to append _EXP to the end of each component to denote that it has been explicitly stated (e.g., FCS_BCM_EXP.1 refers to Baseline Cryptographic Module requirements).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

Refer to the US Government Protection Profile Wireless Local Area Network (WLAN) Client For Basic Robustness Environments, March 2006, Version 1.0 for a complete list of terminology that may be used within this ST.

2. TOE Description

The Target of Evaluation (TOE) is Juniper Network's Odyssey Access Client (FIPS Edition), Version 4.56 hereafter referred to as Odyssey Access Client (OAC). OAC is a software-only access client for wireless and wired 802.1X networks. It 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.

2.1 TOE Overview

The capabilities provided by the TOE are briefly as follows:

- Configure and control wired and wireless network adapters
- Connect to WLAN access points or peer-to-peer wireless networks adhering to IEEE 802.11 WLAN standards
- Associate with WLAN access points using various supported modes
- Authenticate to a wired or wireless network using 802.1X and various supported authentication methods, including certificate-based authentication methods and smart cards
- Configure authentication profiles to allow connections to different networks with different credentials
- Configure FIPS 140-2 compliant encryption for network connections and communications.

In order to establish a wireless connection with an access point, a wireless client must associate with the access point. OAC supports the following association modes:

- Open – for connecting to a network through an access point that does not require a WEP (Wired-Equivalent Privacy) key for association
- Shared – for connecting to a network through an access point that requires at least one preconfigured WEP key for association
- WPA – for connecting to a network through an access point that implements Wi-Fi Protected Access (WPA), which complies with a subset of IEEE 802.11i
- WPA2 – for connecting to a network through an access point that implements WPA2 (Wi-Fi Protected Access 2), which complies with IEEE 802.11i
- xSec – for connecting to a network using xSec, a proprietary layer 2 secure encryption protocol. Connections using xSec require layer 2 xSec-compliant hardware in the network in addition to the network access point.

In order for a wireless client device to access a secure network, the user of the client device must be authenticated by the network. OAC supports the IEEE 802.1X protocol, which provides authenticated access to a LAN. In a wireless network, 802.1X authentication occurs after the client has associated to an access point using an 802.11 association method. Wired networks use 802.1X without any 802.11 association. In turn, 802.1X uses the Extensible Authentication Protocol (EAP) to perform authentication. EAP is a common framework for transporting authentication protocols. OAC provides a number of EAP authentication methods, including the following that support mutual authentication of the user and network:

- EAP-TLS (Transport Layer Security) – uses client and server certificates to provide mutual authentication of the user and network

- EAP-TTLS (Tunneled Transport Layer Security) – a proprietary protocol designed to provide the same cryptographic strength as EAP-TLS without the requirement for a user certificate (although a user certificate may optionally be used). Only the authentication servers require certificates. Authentication is performed using a password or other user credential that is transported in a secure encrypted "tunnel" established using the server certificate.
- EAP-PEAP (Protected EAP) – a proprietary protocol that works similarly to EAP-TTLS and also provides mutual authentication.

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 order to protect user credentials during authentication and user data once a connection with the network has been established, OAC provides various encryption methods. The choice of encryption method for a specific connection depends on the association mode and the requirements of the network access point. OAC supports the following encryption methods:

- WEP – this is available for open mode association and is required in shared mode. It is required when the network access points require shared mode association with WEP keys or WEP encryption (WEP encryption and decryption is not included in the evaluated configuration)
- TKIP (Temporal Key Integrity Protocol) – used when network access points require WPA association and are configured for TKIP data encryption (TKIP encryption and decryption is not included in the evaluated configuration)
- AES (Advanced Encryption Standard) – used when network access points require WPA or WPA2 association and are configured for AES data encryption. In addition, this method is required when associating to hardware that supports xSec.

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.

OAC includes the Odyssey Security Component, a FIPS 140-2 Level 1 certified cryptographic module (Certificate #569) that implements the cryptographic algorithms supporting WLAN operations using WPA2 or xSec association mode. These include AES encryption and the cryptographic algorithms that support the key management protocols.

FIPS mode encryption has a number of requirements that must be satisfied in order for it to be used:

- The configured association mode must be WPA2 or xSec
- The client machine must include an adapter driver that is compatible with the Odyssey encryption module (if WPA2 association is used)
- The network must include a switch that supports xSec (if xSec association is used)
- The configured encryption method must be AES
- If a profile is used, the configured authentication method must be EAP-TLS, EAP-TTLS or PEAP.

2.2 TOE Architecture

The TOE can be installed on a client running:

- Windows 2000 Professional or Server
- Windows XP Home or Professional.

In order to connect to a WLAN, the computer on which the TOE is installed must be equipped with a wireless adapter card and a driver that supports Microsoft-defined 802.11 OIDs (Object Identifiers). In addition, the wireless network must include at least one 802.1X-compliant access point.

In order to authenticate to a network using a wired connection, the computer on which the TOE is installed must be equipped with a network card that is adapted for a wired connection. In addition, the wired network must include at least one 802.1X-compliant switch or hub.

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

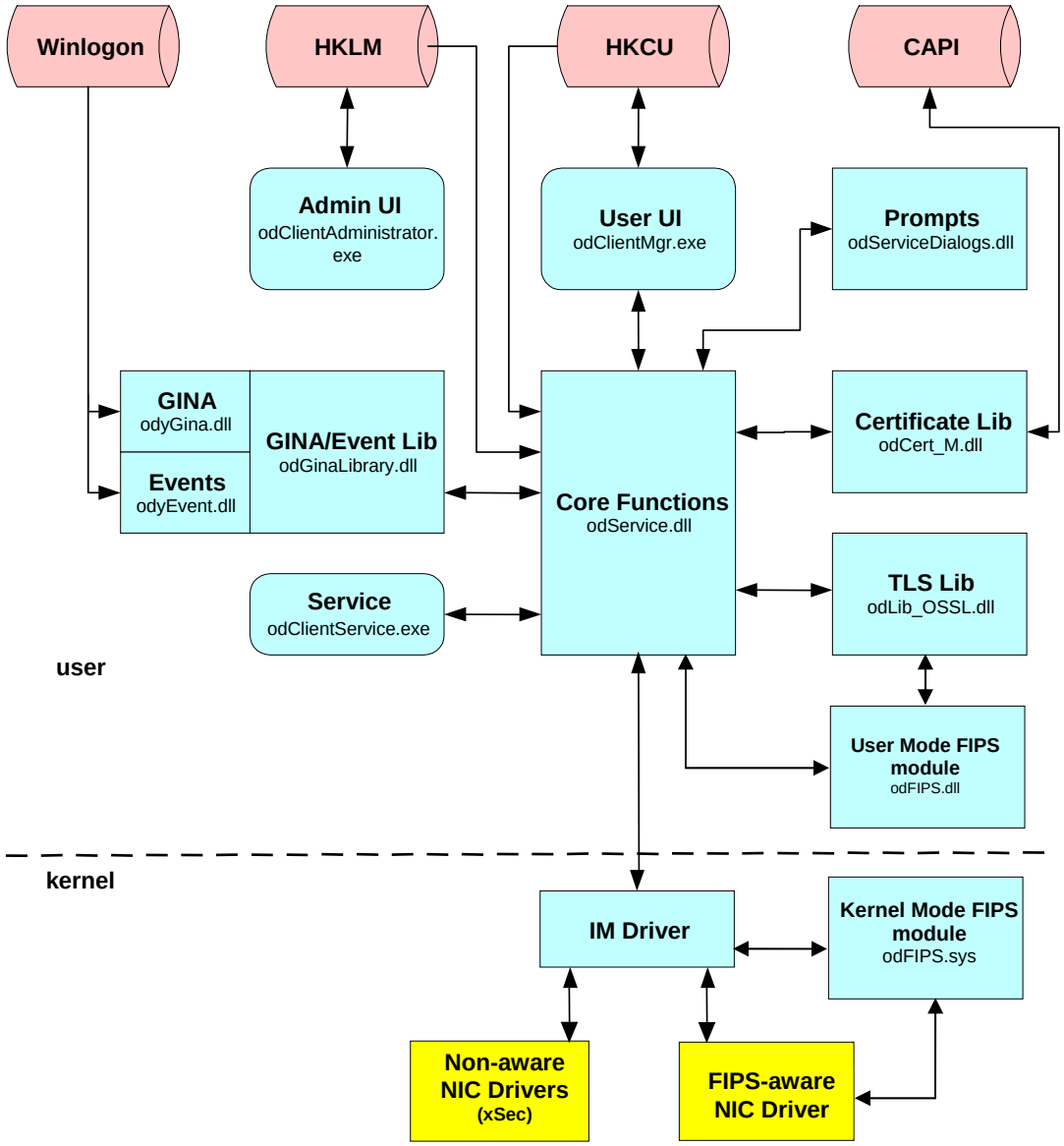

Figure 1: TOE High-Level Architecture

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.

2.2.1 Physical Boundaries

The TOE is the Odyssey Access Client FIPS Edition, Version 4.56. The TOE must be installed, configured and operated according to the TOE evaluated FIPS 140-2 mode. The required FIPS configuration instructions are provided in the User and Administration guidance. The TOE comprises the software components described in Section 2.2 above, and is delivered on a single CD-ROM or can be downloaded as a single installer file. It runs on the Windows 2000 Server, Windows 2000 Professional, Windows XP Home, and Windows XP Professional operating systems, with their supporting hardware platforms, which are in the IT environment.

The TOE relies on the following operating system components:

- Microsoft Windows HKLM and HKCU registries for storage of configuration information
- Microsoft Windows Crypto API to provide a certificate store, including Trusted Root CA certificates, and FIPS-validated private-key signing in TLS mode
- Microsoft Windows Logon, to enable coordination of TOE operation with the timing of network connection and user login
- Other Microsoft Windows APIs for general operating system support of the TOE (e.g., GUI support, file system)

In addition, the IT environment must include the following:

- To use wireless capabilities, the computer on which the TOE is installed must be equipped with a wireless adapter card and a driver that supports the Microsoft-defined 802.11 OIDs and is 802.1X compliant
- To authenticate to a network using a wired connection, the computer on which the TOE is installed must be equipped with a network card adapted for a wired connection
- 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.
- To support the EAP-TLS authentication protocol, the TOE must be able to access a client user certificate, either from the user's personal certificate store, or from a smartcard
- The computer on which the TOE is installed must be running Microsoft Internet Explorer 5.5 or later. The TOE makes use of Microsoft's Enhanced Cryptographic Support Provider (ECSP), which is bundled as part of Internet Explorer 5.5 and later, in order to access the certificate store.

2.2.2 Logical Boundaries

This section identifies the security functions that the evaluated configuration of the TOE will provide. It also discusses the TOE's requirements for security functionality to be provided in the IT environment.

The security functions provided by the TOE comprise:

- Security Audit
- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF.

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 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.

2.2.2.4 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.

2.2.2.5 Protection of the 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.

2.2.2.6 Security Functionality in the IT Environment

The TOE comprises wireless network client software installed as part of a larger system operating within a Basic Robustness environment. As such, many of the functions normally required in such an environment are not expected to be provided by the TOE. Instead, the IT environment is required to provide functions in support of the following:

- Security Audit – association of auditable events with the user identity that caused the event; monitoring of audited events to detect potential violations of the TSP; capabilities to allow the Administrator, and only the Administrator, to search, sort, order and review the audited events; capabilities to select which auditable events are actually audited; secure storage of the audited events; and alerting of the Administrator if the audit trail exceeds an Administrator-set percentage of audit storage capacity
- Cryptographic Support – generation of DSA and RSA key pairs associated with user certificates
- Identification and Authentication – binding of users with subjects acting on behalf of the user
- User Data Protection – removal of information content of a resource when the resource is allocated to a network packet
- Security Management – association of a user with an Administrator role; restriction of use of the TOE security management functions to the Administrator; restriction of setting the IT environment system time to the Administrator
- Protection of the TSF – protection of the TOE and the IT environment from tampering; protection of the TOE and the IT environment from bypass; provision of a reliable time stamp.

2.3 TOE Documentation

Juniper Networks provides documentation that describes the installation process for the TOE and guidance for subsequent administration and use of the system security features. These documents are the Odyssey Client User and Administration Guide FIPS Edition and the Odyssey Client User Guide FIPS Edition.

3. Security Environment

The TOE is intended for a basic robustness environment. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. In general, basic robustness results in "good commercial practices" that counter threats based on casual and accidental disclosure or compromise of data protected by the TOE.

This section describes the assumptions, threats, and policies that are relevant to both the TOE and the WLAN TOE environment. The first section describes the secure usage assumptions, which are those items that the TOE itself cannot implement or enforce. The next section covers the threats that are expected to exist in a basic robustness environment. The final section discusses the DoD policies relevant to the operation of a WLAN client in a basic robustness environment.

3.1 Assumptions

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.

3.2 Threats

T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.CRYPTO_COMPROMISE	A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.

[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.

T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

3.3 Organizational Policies

P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

4. Security Objectives

4.1 Security Objectives for the TOE

This section identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified.

O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.CORRECT_ TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-1 or 140-2 validated cryptographic services.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE.
O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
O.CONFIGURATION_ IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified and corrected, with the TOE being redistributed promptly.
O.DOCUMENTED_ DESIGN	The design of the TOE is adequately and accurately documented.
O.PARTIAL_ FUNCTIONAL_TESTING	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.VULNERABILITY_ ANALYSIS	The TOE will undergo some vulnerability analysis demonstrate that the design and implementation of the TOE does not contain any obvious flaws.

4.2 Security Objectives for the Environment of the TOE

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures.

OE.BASIC_ROBUSTNESS_OS	The TOE 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"[2] and meets the IT environmental requirements necessary to support the correct operation of the TOE.

[2] 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.

OE.CRYPTOGRAPHY	The TOE IT environment shall use NIST FIPS 140-1 or 140-2 validated cryptographic services.
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
OE.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
OE.RESIDUAL_ INFORMATION	The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
OE.SELF_ PROTECTION	The TOE IT environment will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through their interfaces.
OE.TIME_STAMPS	The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
OE.TOE_ACCESS	The TOE IT environment will provide mechanisms that control a user's logical access to the TOE.

5. IT Security Requirements

This section specifies the security requirements for the TOE and its IT environment. The statement of security functional requirements (SFRs) reproduces the requirements specified in the US Government Protection Profile Wireless Local Area Network (WLAN) Client For Basic Robustness Environments, March 2006, Version 1.0, with operations completed as appropriate. These requirements comprise both functional components drawn from Part 2 of the CC and requirements explicitly stated without reference to the CC. The statement of SFRs iterates a requirement from the PP to fully specify the cryptographic capabilities of the TOE and adds key generation requirements (drawn from CC Part 2) that are not stated in the PP.

The minimum strength of function claim for the TOE SFRs is SOF-Basic. There are no specific SFRs for which an explicit strength of function claim is made.

The Security Assurance Requirements (SARs) are those requirements comprising Evaluation Assurance Level 3 (EAL3) as defined in Part 3 of the CC plus ALC_FLR.2.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are being satisfied by the TOE.

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)

Requirement Class	Requirement Component
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

Table 1: TOE Security Functional Components

5.1.1 Security Audit

5.1.1.1 FAU_GEN_EXP.1 Explicit: Audit Data Generation

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

a) All auditable events listed in Table ~~10~~ **2**;

Table ~~10~~ 2 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM_EXP.2	Error(s) detected during cryptographic key transfer	None
FCS_CKM.4	Destruction of a cryptographic key	None
~~FDP_IFC.1~~	~~Dropping a packet that fails to satisfy the Wireless Client Encryption Policy~~	~~MAC address of source and destination devices~~[3]
FMT_SMF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_SMF.1(3)	Changes to the cryptographic key data	None – the TOE **SHALL NOT** record cryptographic keys in the audit log.
FPT_TST_EXP.1	Execution of the self test	Success or Failure of test
FPT_TST_EXP.2	Execution of the self test	Success or Failure of test

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table ~~10~~ **2** Auditable Events].

5.1.2 Cryptographic Support

5.1.2.1 FCS_BCM_EXP.1 Explicit: Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS 140-1/2 when performing FIPS approved cryptographic functions in FIPS approved cryptographic modes of operation.

FCS_BCM_EXP.1.2 The cryptographic module implemented shall have a minimum overall rating of Level 1.

FCS_BCM_EXP.1.3 The FIPS validation testing of the TOE cryptographic module(s) shall be in conformance with FIPS 140-1, 140-2, or the most recently approved FIPS 140 standard for which NIST is accepting validation reports from Cryptographic Modules Testing laboratories.

5.1.2.2 FCS_CKM.1(1) Cryptographic Key Generation (AES, HMAC)

FCS_CKM.1(1).1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**FIPS 186-2 General Purpose**] and specified cryptographic key sizes [**128, 160, 256 bits**] that meet the following: [**FIPS 186-2**].

[3] This specific audit event is included in the US Government Protection Profile WLAN Client for Basic Robustness Environments, rationale for removing this event from the Security Target is provided in Section 7.

5.1.2.3 FCS_CKM_EXP.2 Explicit: Cryptographic Key Establishment

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading, [**Cryptographic Key Establishment by dynamic generation**]. The cryptomodule shall be able to accept as input and be able to output in the following circumstances [**never**] in accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-1 or 140-2 Key Management Security Levels 1, Key Entry and Output.

Note that Manual Loading is available for wireless networks only. Keys for encrypted wired connections are always dynamically generated.

5.1.2.4 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a **cryptographic key zeroization method** that meets the following: [

a) The Key Zeroization Requirements in FIPS PUB 140-1 or 140-2 Key Management Security Level 1;

b) Zeroization of all private cryptographic keys, plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete; and

c) The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times with an alternating pattern.

d) The TSF shall overwrite each intermediate storage area for private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters three or more times with an alternating pattern upon the transfer of the key/CSPs to another location.]

5.1.2.5 FCS_COP_EXP.1 Explicit: Random Number Generation

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved cryptomodule running in a FIPS-approved mode.

5.1.2.6 FCS_COP_EXP.2(1) Explicit: Cryptographic Operation

FCS_COP_EXP.2(1).1 A cryptomodule shall perform encryption and decryption in support of the Wireless Client Encryption Policy using ~~a~~ [**AES**] operating in [**the modes specified below**] supporting minimum FIPS approved key sizes of [

- **CBC mode: 256 bits (for xSec association)**
- **CTR mode: 128 bits (for WPA2 association)**].

5.1.2.7 FCS_COP_EXP.2(2) Explicit: Cryptographic Operation (Message Authentication for WPA2 Association)

FCS_COP_EXP.2(2).1 A cryptomodule shall perform **message authentication** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**AES**] operating in [**CCM mode**] supporting minimum FIPS approved key sizes of [**128 bits**].

5.1.2.8 FCS_COP_EXP.2(3) Explicit: Cryptographic Operation (Message Authentication for xSec Association)

FCS_COP_EXP.2(3).1 A cryptomodule shall perform **message authentication** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**HMAC-SHA1**] operating in [**mode not applicable**] supporting minimum FIPS approved key sizes of [**160 bits**].

5.1.2.9 FCS_COP_EXP.2(4) Explicit: Cryptographic Operation (Digital Signature Verification – DSA)

FCS_COP_EXP.2(4).1 A cryptomodule shall perform **digital signature verification** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**DSA**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**512, 576, 640, 704, 768, 832, 896, 960, and 1024 bits**].

5.1.2.10 FCS_COP_EXP.2(5) Explicit: Cryptographic Operation (Digital Signature Verification – RSA)

FCS_COP_EXP.2(5).1 A cryptomodule shall perform **digital signature verification** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**RSASSA-PKCS1_V1_5**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**1024, 1536, 2048, 3072, and 4096 bits**].

5.1.2.11 FCS_COP_EXP.2(6) Explicit: Cryptographic Operation (Asymmetric Encryption for Key Wrapping)

FCS_COP_EXP.2(6).1 A cryptomodule shall perform **asymmetric encryption for key wrapping** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**RSASSA-PKCS1_V1_5**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**1024, 1536, 2048, 3072, and 4096 bits**].

5.1.2.12 FCS_COP_EXP.2(7) Explicit: Cryptographic Operation (Diffie-Hellman Key Agreement)

FCS_COP_EXP.2(7).1 A cryptomodule shall perform **key agreement** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**Diffie-Hellman Key Agreement**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**128, 256 bits**].

5.1.2.13 FCS_COP_EXP.2(8) Explicit: Cryptographic Operation (Secure Hash for Integrity Verification)

FCS_COP_EXP.2(8).1 A cryptomodule shall perform **secure hashing** ~~encryption and decryption~~ in support of the ~~Wireless Client Encryption Policy~~ TSF Testing requirement using ~~a~~ [**SHA-1**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved ~~key~~ digest sizes of [**160 bits**].

5.1.3 User Data Protection

5.1.3.1 FDP_IFC.1 Subset Information Flow Control (Wireless Client Encryption Policy)

FDP_IFC.1.1 The TSF shall enforce the [Wireless Client Encryption Policy] on [subjects: client, access point/system; information: network packets; operations: receive packet and transmit packet].

5.1.3.2 FDP_IFF.1 Simple Security Attributes (Wireless Client Policy)

FDP_IFF.1.1 The TSF shall enforce the [Wireless Client Encryption Policy] based on the following types of subject and information security attributes: [subjects: client, access point/system; information: encryption/decryption flag, direction of travel at the network interface]

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

- If the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification.
- If the direction of travel is from the operating system to the network interface and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE must encrypt user data via FCS_COP_EXP.2.1 and if successful transmit the packet via the wireless interface.

- The direction of travel is from the network interface to the operating system and the encryption/decryption flag indicates the TOE should perform encryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 and if successful pass that information to the operating system.
- [***no additional information flow Specified Access Point/System Policy Rules***].

FDP_IFF.1.3 The TSF shall enforce the following information flow control rules: [***no additional information flow control SFP rules***]

FDP_IFF.1.4 The TSF shall provide the following [***no additional SFP capabilities***]

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [***no explicit authorization rules***]

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [***no explicit denial rules***]

Application Note: The evaluated configuration of the TOE does not support transmission of unencrypted network packets. In effect, the "encryption/decryption flag" is always set to "true".

5.1.3.3 FDP_RIP.1(1) Subset Residual Information Protection

FDP_RIP.1(1).1 The TSF shall ~~be~~ ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] the following objects [network packet objects].

5.1.4 Security Management

5.1.4.1 FMT_MSA.2 Secure Security Attributes

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

Application Note: An administrator following the guidance documentation will only result in secure values for security attributes. If an administrator does not follow the guidance documentation, the TOE can be made to accept insecure values.

5.1.4.2 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Wireless Client Encryption Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 FMT_SMF.1(1) Specification of Management Functions (Cryptographic Function)

FMT_SMF.1(1).1 The TSF shall be capable of performing the following security management functions: [set the encryption/decryption of network packets (via FCS_COP_EXP.2) in conformance with the Wireless Client Policy].

Application Note: The evaluated configuration of the TOE does not support transmission of unencrypted network packets. In effect, the "encryption/decryption flag" is always set to "true".

5.1.4.4 FMT_SMF.1(2) Specification of Management Functions (Audit Record Generation)

FMT_SMF.1(2).1 The TSF shall be capable of performing the following security management functions: [enable or disable Security Audit (FAU_GEN_EXP.1)].

5.1.4.5 FMT_SMF.1(3) Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1(3).1 The TSF shall be capable of performing the following security management functions: [set, modify, and delete the cryptographic keys and key data in support of the Wireless Client Policy ~~and enable/disable verification of cryptographic key testing~~].

5.1.5 Protection of the TSF

5.1.5.1 FPT_TST_EXP.1 TSF Testing

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests *during initial start-up* **and** *at the request of the authorized user* to demonstrate the correct operation of **the hardware portions of the TSF.**

FPT_TST_EXP.1.2 The TSF shall provide authorized users with the capability to **use a TSF-provided cryptographic function** to verify the integrity of **all TSF data except the following: audit data.**

FPT_TST_EXP.1.3 The TSF shall provide authorized users with the capability to **use a TSF-provided cryptographic function** to verify the integrity of stored TSF executable code.

5.1.5.2 FPT_TST_EXP.2 TSF Testing of Cryptographic Modules

FPT_TST_EXP.2.1 The TSF shall run the suite of self-tests provided by the FIPS 140-1 or 140-2 cryptomodule during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.

FPT_TST_EXP.2.2 The TSF shall be able to run the suite of self-tests provided by the FIPS 140-1 or 140-2 cryptomodule immediately after the generation of a key.

5.1.6 Trusted Path

5.1.6.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**secure communication of network packets in support of the Wireless Client Encryption Policy**].

5.2 Security Functional Requirements for the IT Environment

The following table identifies the SFRs for the TOE IT environment.

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

Requirement Class	Requirement Component
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

Table 3: TOE IT Environment Security Functional Components

5.2.1 Security Audit

5.2.1.1 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 The **TOE IT environment** shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.2 FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The **TOE IT environment** shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP

FAU_SAA.1.2 The **TOE IT environment** shall enforce the following rules for monitoring audited events:

a) Accumulation **of a single auditable event** or combination of [auditable events in Table **2** ~~10~~] known to indicate a potential security violation;

b) *no additional rules*

5.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The **TOE IT environment** shall provide **only** the [Administrator] with the capability to read [all audit data] from the audit records.

FAU_SAR.1.2 Refinement: The TOE IT environment shall provide the audit records in a manner suitable for the **Administrator** to interpret the information.

5.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The **TOE IT environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The **TOE IT environment** shall provide the ability to perform *searches*, *sorting*, *ordering* of audit data based on [criteria with logical relations].

5.2.1.6 FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The **TOE IT environment** shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a.) [***subject, identity, host identity***]
b.) [**no additional audit attributes**].

5.2.1.7 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **TOE IT environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The **TOE IT environment** shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

5.2.1.8 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The **TOE IT environment** shall [immediately alert the administrators by displaying a message at the local console] if the audit trail exceeds [an Administrator-settable percentage of storage capacity].

5.2.2 Cryptographic Support

5.2.2.1 FCS_CKM.1(2) Cryptographic Key Generation (DSA)

FCS_CKM.1(2).1 The ~~TSF~~ **TOE IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**FIPS 186-2 General Purpose**] and specified cryptographic key sizes [**512, 576, 640, 704, 768, 832, 896, 960, and 1024 bits**] that meet the following: [**FIPS 186-2**].

5.2.2.2 FCS_CKM.1(3) Cryptographic Key Generation (RSA)

FCS_CKM.1(3).1 The ~~TSF~~ **TOE IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**FIPS 186-2 General Purpose**] and specified cryptographic key sizes [**1024, 1536, 2048, 3072, and 4096 bits**] that meet the following: [**FIPS 186-2**].

5.2.2.3 FCS_COP_EXP.2(9) Explicit: Cryptographic Operation (Digital Signature Generation– DSA)

FCS_COP_EXP.2(9).1 The TOE IT environment shall perform **digital signature generation** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**DSA**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**512, 576, 640, 704, 768, 832, 896, 960, and 1024 bits**].

5.2.2.4 FCS_COP_EXP.2(10) Explicit: Cryptographic Operation (Digital Signature Generation– RSA)

FCS_COP_EXP.2(10).1 The TOE IT environment shall perform **digital signature generation** ~~encryption and decryption~~ in support of the Wireless Client Encryption Policy using ~~a~~ [**RSASSA-PKCS1_V1_5**] operating in [**mode not applicable**] supporting ~~minimum~~ FIPS approved key sizes of [**1024, 1536, 2048, 3072, and 4096 bits**].

5.2.3 Identification and Authentication

5.2.3.1 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The **TOE IT environment** shall associate the following user security attributes with subjects acting on the behalf of that user: [authentication credentials].

FIA_USB.1.2 The **TOE IT environment** shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**none**].

FIA_USB.1.3 The **TOE IT environment** shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [**none**].

5.2.4 User Data Protection

5.2.4.1 FDP_RIP.1(2) Subset Residual Information Protection

FDP_RIP.1(2).1 The **TOE IT environment** shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects [network packet objects].

5.2.5 Security Management

5.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The **TOE IT environment** shall restrict the ability to *determine the behavior* of the functions: [encryption/decryption of network packets (FMT_SMF.1(1), FMT_SMF.1(3)), audit (FMT_SMF.1(2))] to [the administrator].

5.2.5.2 FMT_MTD.1 Management of TSF Data (Time TSF Data)

FMT_MTD.1.1 The **TOE IT environment** shall restrict the ability to *set* the [time and date used to form the time stamps in FPT_STM.1] to [the Administrator].

5.2.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The **TOE IT environment** shall maintain the role [Administrator].

FMT_SMR.1.2 The **TOE IT environment** shall be able to associate users with roles.

5.2.6 Protection of the TSF

5.2.6.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **TOE IT environment** shall be able to provide reliable time **and date** stamps for **the TOE and** its own use.

5.2.6.2 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The **TOE IT environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.6.3 FPT_SEP.1 TOE IT Environment Domain Separation

FPT_SEP.1.1 The **TOE IT environment** shall maintain a security domain that protects **the TOE and the TOE IT environment** from interference and tampering by untrusted subjects initiating actions through the **IT environment kernel interface**.

FPT_SEP.1.2 The TOE IT environment shall enforce separation between the security domains of subjects in the **TOE IT environment's** Scope of Control.

5.3 TOE Security Assurance Requirements

This section addresses each EAL 3 assurance class.

The following table identifies the Security Assurance Requirements (SARs).

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 4: TOE Security Assurance Components

5.3.1 Configuration management

5.3.1.1 ACM_CAP.3 Generation support and acceptance procedures

Developer Action Elements

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.

Content and Presentation of Evidence Elements

ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.

ACM_CAP.3.9c	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c	The CM system shall provide measures such that only authorised changes are made to the configuration items.
	Evaluator Action Elements
ACM_CAP.3.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 ACM_SCP.1 TOE CM coverage

	Developer Action Elements
ACM_SCP.1.1d	The developer shall provide a list of configuration items for the TOE.
	Content and Presentation of Evidence Elements
ACM_SCP.1.1c	The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
	Evaluator Action Elements
ACM_SCP.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation

5.3.2.1 ADO_DEL.1 Delivery procedures

	Developer Action Elements
ADO_DEL.1.1d	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d	The developer shall use the delivery procedures.
	Content and Presentation of Evidence Elements
ADO_DEL.1.1c	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
	Evaluator Action Elements
ADO_DEL.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

	Developer Action Elements
ADO_IGS.1.1d	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
	Content and Presentation of Evidence Elements
ADO_IGS.1.1c	The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
	Evaluator Action Elements
ADO_IGS.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e	The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development

5.3.3.1 ADV_FSP.1 Fully defined external interfaces

Developer Action Elements

ADV_FSP.1.1d The developer shall provide a functional specification.

Content and Presentation of Evidence Elements

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

Evaluator Action Elements

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 ADV_HLD.2 Security enforcing high-level design

Developer Action Elements

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

Content and Presentation of Evidence Elements

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator Action Elements

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 ADV_RCR.1 Informal correspondence demonstration

Developer Action Elements

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and Presentation of Evidence Elements

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator Action Elements

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents

5.3.4.1 AGD_ADM.1 Administrator guidance

Developer Action Elements

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

Content and Presentation of Evidence Elements

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator Action Elements

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 AGD_USR.1 User guidance

Developer Action Elements

AGD_USR.1.1d The developer shall provide user guidance.

Content and Presentation of Evidence Elements

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
	Evaluator Action Elements
AGD_USR.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support

5.3.5.1 ALC_DVS.1 Identification of security measures

	Developer Action Elements
ALC_DVS.1.1d	The developer shall produce development security documentation.
	Content and Presentation of Evidence Elements
ALC_DVS.1.1c	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
	Evaluator Action Elements
ALC_DVS.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e	The evaluator shall confirm that the security measures are being applied.

5.3.5.2 ALC_FLR.2 Flaw reporting procedures

	Developer Action Elements
ALC_FLR.2.1d	The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d	The developer shall provide flaw remediation guidance addressed to TOE users.
	Content and Presentation of Evidence Elements
ALC_FLR.2.1c	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5c	The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c	The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7c	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
	Evaluator Action Elements
ALC_FLR.2.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests

5.3.6.1 ATE_COV.2 Analysis of coverage

Developer Action Elements

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

Content and Presentation of Evidence Elements

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator Action Elements

ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 ATE_DPT.1 Testing: high-level design

Developer Action Elements

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

Content and Presentation of Evidence Elements

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator Action Elements

ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 ATE_FUN.1 Functional testing

Developer Action Elements

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

Content and Presentation of Evidence Elements

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator Action Elements

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 ATE_IND.2 Independent testing - sample

Developer Action Elements

ATE_IND.2.1d The developer shall provide the TOE for testing.

	Content and Presentation of Evidence Elements
ATE_IND.2.1c	The TOE shall be suitable for testing.
ATE_IND.2.2c	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
	Evaluator Action Elements
ATE_IND.2.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment

5.3.7.1 AVA_MSU.1 Validation of analysis

	Developer Action Elements
AVA_MSU.1.1d	The developer shall provide guidance documentation.
	Content and Presentation of Evidence Elements
AVA_MSU.1.1c	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
	Evaluator Action Elements
AVA_MSU.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e	The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e	The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 AVA_SOF.1 Strength of TOE security function evaluation

	Developer Action Elements
AVA_SOF.1.1d	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
	Content and Presentation of Evidence Elements
AVA_SOF.1.1c	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
	Evaluator Action Elements
AVA_SOF.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e	The evaluator shall confirm that the strength claims are correct.

5.3.7.3 AVA_VLA.1 Developer vulnerability analysis

Developer Action Elements

AVA_VLA.1.1d	The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d	The developer shall provide vulnerability analysis documentation.

Content and Presentation of Evidence Elements

AVA_VLA.1.1c	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator Action Elements

AVA_VLA.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the TOE security functions and TOE assurance measures.

6.1 TOE Security Functions

The following security functions are defined for the TOE:

- Security Audit
- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF.

Of these security functions, Cryptographic Support, User Data Protection, and Protection of the TSF are realized by probabilistic or permutational mechanisms. In most cases, these mechanisms are cryptographic in nature. However, the Cryptographic Support security function includes a mechanism for key establishment by entry of a pre-shared key (PSK), which can be a passphrase from which the PSK is generated, or the PSK itself. The passphrase comprises a minimum 8 and maximum 63 ASCII characters. The claimed strength of function for the Cryptographic Support function is SOF-Basic.

6.1.1 Security Audit

The TSF can generate audit records of the following auditable events:

- Errors detected during cryptographic key transfer
- Destruction of a cryptographic key
- Changing the TOE encryption algorithm, including the selection not to encrypt communications
- Changes to the cryptographic key data
- Execution of TSF self tests
- Execution by TSF of cryptographic module self-tests.

The TSF records within each audit record the data and time of the event, the type of event, the subject identity (i.e., the TOE module that generated the event) and the outcome (success or failure) of the event. The TSF obtains its date and time stamp from the IT environment.

The TSF also records, for the identified specific event types, the following additional data:

Auditable Events	Additional Audit Record Contents
Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
Execution of TSF self test	Success or Failure of tests
Execution by TSF of cryptographic module self-tests	Success or Failure of tests

The TSF specifically does not record any cryptographic keys in the audit log.

The Security Audit security function is designed to satisfy the following security functional requirement:

- FAU_GEN_EXP.1: OAC provides the ability to audit the required auditable events and record within each audit event the required date/time, event type, subject, and event outcome.

6.1.2 Cryptographic Support

The TSF includes the Odyssey Security Component (OSC), a software cryptomodule that has been validated as meeting the requirements for a FIPS 140-2 Level 1 cryptographic module (Certificate #569). In its evaluated configuration, the TOE operates in FIPS mode, thus ensuring that all cryptographic operations are performed by FIPS approved cryptographic functions in FIPS approved cryptographic modes of operation.

When operating in FIPS mode, the TSF provides cryptographic functions in support of the Wireless Client Encryption Policy depending on the configured association mode, either WPA2 or xSec. The cryptographic functions used in WPA2 association mode are:

- Encryption and decryption using AES in CTR mode with 128-bit key size
- Message authentication using AES in CCM mode with 128-bit key size.

The cryptographic functions used in xSec association mode are:

- Encryption and decryption using AES in CBC mode with 256-bit key size
- Message authentication using HMAC-SHA1 with 160-bit key size.

The TOE supports key establishment by manual entry by providing the capability to manually enter a pre-shared key (PSK), which can be a passphrase that is used to generate the PSK, or the PSK itself. Manual key entry is available in WPA2 association mode only.

The PSK or PMK is not used directly for encryption and decryption of data. Instead, a temporal key that is used to encrypt and decrypt data is generated by a 4-way handshake as defined in 802.11i (and also used in xSec mode). The handshake uses the master keying material (PSK or PMK) as a seed for a pseudo-random number generator. The temporal key is generated whenever the client associates with an access point.

The key establishment protocol can involve the use of DSA (with key sizes of 512, 576, 640, 704, 768, 832, 896, 960, 1024 bits) or RSA (with key sizes of 1024, 1536, 2048, 3072, 4096 bits) for digital signature generation and verification and the use of RSA (with key sizes of 1024, 1536, 2048, 3072, 4096 bits) for asymmetric encryption in support of key wrapping. The OSC also implements the Diffie-Hellman key agreement algorithm, which is not FIPS approved but which is allowed in FIPS 140 mode for key agreement purposes.

The OSC implements a FIPS-validated pseudo-random number generator that conforms to FIPS 186-2 (RNG Certificate #79) and which is used as part of the key generation process for AES, HMAC and DSA keys.

The OSC provides methods to zeroize plaintext secret and private keys and CSPs within the module. The key zeroization methods have been validated against the requirements of FIPS 140-2. When necessary, the TOE zeroizes any and all private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters that are outside the boundary of the OSC by overwriting the key or parameter three times with an alternating pattern.

The cryptographic algorithms implemented within the OSC and used by the TOE conform to the following standards:

- AES: FIPS 197 Advanced Encryption Standard
- HMAC: FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- SHA1: FIPS 180-2 Secure Hash Standard
- DSA: FIPS 186-2 Digital Signature Standard
- RSA: PKCS #1 v2.1: RSA Cryptography Standard
- Diffie-Hellman: RFC 2631 – Diffie-Hellman Key Agreement.

The Cryptographic Support security function is designed to satisfy the following security functional requirements:

- FCS_BCM_EXP.1: The OSC, which is the cryptographic module within the TOE, is FIPS 140-2 Level 1 validated (Certificate #569).
- FCS_CKM.1(1): The OSC generates AES and HMAC keys in support of the cryptographic operations provided by the OSC.

- FCS_CKM_EXP.2: The OSC provides a means for manually entering master keying material (a Pre Shared Key).
- FCS_CKM.4: The OSC provides a FIPS 140-2 validated method to zeroize its cryptographic keys and CSPs. The TSF zeroizes its cryptographic keys and CSPs (that are outside the boundary of the OSC) by overwriting three times with an alternating pattern.
- FCS_COP_EXP.1: The OSC implements a FIPS 140-2 Level 1 validated pseudo-random number generator.
- FCS_COP_EXP.2(1-7): The OSC implements the cryptographic algorithms required to support the key management protocols implemented by the TOE and to encrypt and decrypt network packets in accordance with the Wireless Client Encryption Policy.

6.1.3 User Data Protection

The TSF implements the Wireless Client Encryption Policy to ensure that all network packets transmitted by the client to the network are encrypted. Similarly, the TSF decrypts all network packets received from the network before passing them to the client. The evaluated configuration of the TOE does not support transmission of unencrypted network packets – in the evaluated configuration, the "encryption/decryption flag" specified by the Wireless Client Encryption Policy is always set to "encryption".

In its evaluated configuration, the TOE supports authentication protocols (EAP-TLS, EAP-TTLS and EAP-PEAP) that provide mutual authentication between the client and network, thus establishing a trusted channel (initiated by the TOE) between the client and the network access point.

The TSF does not allocate or release the memory resources used for network packet objects. The TSF receives buffers from the operating system in the IT environment, containing data to be encrypted and passed on to NDIS, and receives encrypted data packets from the upper boundary of the IM driver that are decrypted and passed on to the operating system. Nevertheless, the TSF also ensures that the buffers are not padded out with previously transmitted or otherwise residual information, either when transmitting data to the network or receiving it from the network.

The TSF is not responsible for network packet objects (buffers) allocated and released outside the TOE. The ST specifies FDP_RIP.1(2) to address this situation.

The User Data Protection security function is designed to satisfy the following security functional requirements:

- FDP_IFC.1, FDP_IFF.1: The TOE in its evaluated configuration operates in FIPS mode, ensuring all data to be sent to the network is encrypted using a FIPS 140-2 Level 1 cryptographic module, and all data received from the network is decrypted using the same cryptographic module.
- FDP_RIP.1(1): The TOE ensures that any previous information content of buffers used for network packets is not available when a new buffer is received by the TOE, either from the operating system or the network interface.
- FTP_ITC.1: The TOE establishes a mutually authenticated, logically distinct, communication channel between itself and the network access point for the secure transmission of network packets.

6.1.4 Security management

The TSF provides the Odyssey Client Administrator to support security management of the TOE. It enables the administrator to configure and lock initial and connection settings, ensuring that the user of the TOE cannot take the TOE out of FIPS mode or out of its evaluated configuration. The TSF stores configuration settings in the registry of the underlying operating system and the Odyssey Client Administrator provides the administrator with the capability to manage these settings. The Odyssey Client Administrator ensures values assigned to security attributes are valid with respect to the secure state of the TSF.

The Odyssey Client Administrator allows the administrator to configure the TOE in FIPS mode, so that encryption of transmitted network packets (and decryption of received network packets) in accordance with the Wireless Client

Encryption Policy is enforced by default and cannot be disabled by the TOE user. The Odyssey Client Administrator also provides the administrator with the means to manage cryptographic keys and to enable or disable cryptographic key testing by the cryptomodule. The administrator also uses the Odyssey Client Administrator to enable and disable auditing by the TSF.

The Security Management security function is designed to satisfy the following security functional requirements:

- FMT_MSA.2: The Odyssey Client Administrator component of the TOE ensures values assigned to security attributes are valid with respect to the secure state of the TSF.
- FMT_MSA.3: The Odyssey Client Administrator component of the TOE restricts to the Administrator the ability to specify alternative initial values to override default restrictive values of the security attributes within the scope of the Wireless Client Encryption Policy.
- FMT_SMF.1(1), FMT_SMF.1(2), FMT_SMF.1(3): The Odyssey Client Administrator component of the TOE provides the ability to: enable encryption and decryption of network packets, by configuring the TOE in FIPS mode; enable or disable security auditing; manage cryptographic keys and key data in support of the Wireless Client Encryption Policy, and enable or disable cryptographic key testing by the cryptomodule.

6.1.5 Protection of the TSF

The TSF provides the TOE administrator with the capability to invoke integrity tests of the stored executable code of the TSF, using the SHA-1 secure hash function implemented by the FIPS 140-2 Level 1 validated Odyssey Security Component.

The TSF also uses the SHA-1 function to initially generate a cryptographic hash of all the TSF data, which is stored in the HKLM part of the registry in the underlying operating system. The TSF data includes: default user configuration (for new users); administrative constraints (i.e., rules applied by the administrator to all users); and allowed TLS cipher suites. At the request of the administrator, the TSF re-calculates the cryptographic hash over the TSF data and compares this with its stored value to verify the continued integrity of the TSF data. It should be noted that the cryptographic hash calculation does not include audit data generated by the TSF.

During start-up of the TSF, the Odyssey Security Component executes its suite of self-tests that verify the integrity of the cryptomodule and the cryptographic algorithms it contains. The self-tests can also be executed on request by the administrator.

The TSF also provides the capability to run the cryptomodule self-tests after the manual entry of master key material. Due to the disruptive nature of the self-tests (which block all data transfer for several seconds), the TSF does not run the tests for dynamic keys that can be generated many times during a session.

The Protection of the TSF security function is designed to satisfy the following security functional requirements:

- FPT_TST_EXP.1: The TSF provides the Administrator with the capability of verifying the integrity of the TSF executable code and all TSF data (excluding audit data) using a cryptographic function provided by the OSC. Note that the TSF does not include any hardware.
- FPT_TST_EXP.2: The TSF runs the self-tests provided by the OSC during initial start-up and at the request of the Administrator. It can also run these tests following the manual entry of master key material.
- FCS_COP_EXP.2(8): The OSC implements the SHA-1 secure hash algorithm used by the TSF to verify the integrity of TSF executable code and TSF data.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Juniper Networks ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Juniper

Networks ensures changes to the implementation representation and all other configuration items are properly controlled. Juniper Networks performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- Configuration Management Plan

The Configuration management assurance measure satisfies the following assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and operation

Juniper Networks provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Juniper Networks' delivery procedures describe all applicable procedures to be used to detect modification to the TOE and detection of attempts to masquerade as the developer. Juniper Networks also provides documentation that describes procedures to maintain security when distributing the TOE to the user and the steps necessary to the TOE in accordance with the evaluated configuration.

These activities are documented in:

- Delivery Plan
- Installation, Generation and Start-up Guide

The Delivery and operation assurance measure satisfies the following assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Juniper Networks has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the external TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and its interfaces; and correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- Functional Specification
- High-Level Design
- Correspondence Document

The Development assurance measure satisfies the following assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance documents

Juniper Networks provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE. This includes identification of the interfaces, parameters, and security relevant events related to the administrative functions.

These activities are documented in:

- Administrator Manual
- User Guide

The Guidance documents assurance measure satisfies the following assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Juniper Networks ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Juniper Networks applies security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE. In addition, Juniper identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable.

The Life cycle support assurance measure satisfies the following assurance requirements:

- ALC_DVS.1
- ALC_FLR.2

6.2.6 Tests

Juniper Networks has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. The documentation identifies each security function to be tested, describes the goal of the test the test procedures, and ordering dependencies when appropriate. The documentation also provides an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- Test Plan
- Test Results

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.1

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

Juniper Networks has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

Juniper Networks performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

As documented in this Security Target (ST), the TOE (Juniper Network's Odyssey Access Client FIPS Edition, Version 4.56) complies with the US Government Protection Profile Wireless Local Area Network (WLAN) Client for Basic Robustness Environments, March 2006, Version 1.0.

The Security Environment, Objectives, and Requirements in this ST have been reproduced from the WLAN PP, as indicated below:

- Except as noted below, all threats, organizational security policies and assumptions have been included and no new threats, organizational security policies or assumptions have been introduced.
- Except as noted below, all of the WLAN PP security objectives have been included without modification.
- All operations have been completed on the requirements in compliance with the PP as indicated using bold and bold-italic text in Section 5.1 and 5.2.
- References to tables and section headings within the requirement statements have been changed as the tables and sections in the ST do not have the same numbers as in the WLAN PP. This applies to FAU_GEN_EXP.1

The statement of the assumption A.BASIC_ROBUSTNESS_IT_ENVIRONMENT has been modified to represent correctly the TOE type. The word "device" has been replaced with "client". Section 1 of the WLAN PP is clear in indicating that conformant TOEs are not restricted to hardware-only solutions.

The statement of the security objective for the IT environment OE.BASIC_ROBUSTNESS_OS has been modified to represent correctly the TOE type. The words "is a Wireless LAN card and" have been removed. Section 1 of the WLAN PP is clear in indicating that conformant TOEs are not restricted to hardware-only solutions.

The ST adds OE.CRYPTOGRAPHY to specify that cryptographic operations performed in the IT environment in support of TOE cryptographic operations must be NIST FIPS 140-1 or 140-2 validated, consistent with P.CRYPTOGRAPHY. This is necessary because the TOE provides capabilities, based on cryptographic services, beyond those required by the PP (specifically, mutual authentication between the client and the network). While the TOE implements all the functionality required to satisfy the PP requirements, it utilizes certificates obtained from the IT environment to establish mutual authentication.

The ST iterates FCS_COP_EXP.2 to specify additional cryptographic algorithms provided by the TOE.

The ST adds FCS_CKM.1(1) to specify the key generation requirements to support the additional operations defined in FCS_COP_EXP.2(2, 3, 4, 7). While the PP does not preclude key generation by the cryptomodule within the TOE, it specifies key establishment by manual entry and does not include any requirements for key generation.

The ST adds FTP_ITC.1 to specify the capability of the TOE to mutually authenticate the client and the network. This capability is consistent with and supports the operation of the Wireless Client Encryption Policy defined in the PP (in FDP_IFC.1 and FDP_IFF.1).

The ST adds FCS_CKM.1(2, 3) as requirements on the IT environment to satisfy the dependencies of FCS_COP_EXP.2(4-6) on appropriate key generation capabilities. The TOE does not generate DSA or RSA parameters, but performs actions using information from certificates in the IT environment.

The following additional tailoring of specific security requirements has been performed:

- FAU_GEN_EXP.1: The auditable event associated with FDP_IFC.1 has been removed, since this event is not applicable to the TOE. The TOE has no knowledge of the expected contents of a network data packet. The TOE unconditionally applies the decryption algorithm to received packets and passes the result up the network stack. Depending on the scenario, a received packet that failed to satisfy the Wireless Client Encryption Policy (i.e., was unencrypted or improperly encrypted) would either: a) fail the layer 2 checksum and be silently discarded by the environment before entering the TOE, or b) pass the layer 2 checksum, have the decryption algorithm applied by the TOE, and be passed up to the next higher layer (which would discard it without notifying the TOE). Packets to be transmitted do not have the Wireless

Client Encryption Policy applied to them before they enter the TOE. In no case is the TOE given an outgoing packet that is supposed to have the Wireless Client Encryption Policy applied.

- FCS_COP_EXP.2(2-8): These requirements are refined to identify the specific cryptographic operations that are being specified rather than encryption and decryption algorithms.
- FDP_RIP.1: The PP iterates FDP_RIP.1 without identification. The ST identifies FDP_RIP.1(1) as the TOE security requirement, and FDP_RIP.1(2) as the IT environment security requirement.
- FDP_RIP.1(1): Removed "be", which is grammatically incorrect and which is not part of the CC Part 2 definition.
- FPT_TST.1: The ST presents this as an explicitly stated requirement (FPT_TST_EXP.1), which appears to be the PP's intention. All references to this SFR in the PP, except where it is actually stated in the set of TOE security functional requirements, are to FPT_TST_EXP.1, including rationale in Section 6.8 of the PP justifying the explicit statement of the requirement.
- FAU_SEL.1: The PP indicates this SFR as FAU_SEL, when in fact it should be FAU_SEL.1. The ST author changed the FAU_SEL. to FAU_SEL.1.
- FAU_STG.3: The ST implicitly selects "none" as the "other actions determined by the ST AUTHOR", but has removed this from the operation, in order to improve the readability of the requirement.
- FMT_SMF.1.1(3) – the following words have been removed "and enable/disable verification of cryptographic key testing". The words are interpreted to require the ability to disable key testing which conflicts with the FIPS 140-2 requirements. The PP requires the product include a FIPS 140-2 certified module. Therefore, the words were struck to resolve the conflict.

The vendor has elected to pursue a more rigorous assurance level, increased from EAL2 augmented with ACM_SCP.1, ALC_FLR.2 and AVA_MSU.1 as specified in the WLAN PP, to EAL3 augmented with ALC_FLR.2, as specified in section 1.2 of this ST. Section 8.3 of the ST provides a rationale for the target Evaluation Assurance Level.

8. Rationale

The functional and assurance requirements presented in this ST are mutually supportive and their combination meet the stated security objectives and further demonstrate the completeness and sufficiency of the requirements as a whole as reflected throughout this section.

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Strength of Functions
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

The US Government Wireless Local Area Network (WLAN) Client PP provides rationale for the security objectives demonstrating that security objectives are suitable to cover the intended environment. The rationale (provided in Section 6.1 of the US Government Wireless Local Area Network (WLAN) Client PP) is valid for the PP objectives reproduced in this ST and is not further discussed. As described in Section 7 of this ST, the ST specifies the following security objective in addition to those specified in the PP:

- OE.CRYPTOGRAPHY: This objective for the IT environment specifies that the IT environment will use NIST FIPS 140-1 or 140-2 validated cryptographic services, which is necessary to ensure that the organizational security policy P.CRYPTOGRAPHY is satisfied.

8.2 Security Requirements Rationale

Sections 6.2, 6.3 and 6.4 of the US Government Wireless Local Area Network (WLAN) Client PP provides rationale for the security requirements, demonstrating that the security requirements are suitable to address the IT security objectives. This rationale is valid for the PP requirements reproduced in the ST and is not further discussed. As described in Section 7 of this ST, the ST specifies the following requirements in addition to those specified in the PP:

- FCS_CKM.1(1): This requirement specifies key generation operations performed by the FIPS 140-2 validated cryptographic module in support of the cryptographic operations specified for the TOE and therefore contribute to satisfying O.CRYPTOGRAPHY
- FCS_CKM.1(2, 3): These requirements on the IT environment specify key generation operations for keying material associated with user certificates. The TOE uses the associated user certificates in establishing mutually authenticated communications with the wireless network, and therefore these requirements contribute to satisfying OE.CRYPTOGRAPHY
- FCS_COP_EXP.2(2-7): These requirements specify additional cryptographic functionality provided by the FIPS 140-2 validated cryptographic module that support the operation of the Wireless Client Encryption Policy and therefore contribute to satisfying O.CRYPTOGRAPHY
- FCS_COP_EXP.2(8): This requirement specifies the TSF-provided cryptographic function used to verify the integrity of TSF data and TSF executable code in support of FPT_TST_EXP.1 and therefore contributes to satisfying O.CORRECT_TSF_OPERATION

- FTP_ITC.1: This requirement specifies the mutually authenticated. Logically distinct, communication channel between the TOE and the network access point for the secure transmission of network packets. Mutual authentication and data encryption are performed using the FIPS approved algorithms provided by the FIPS 140 validated cryptographic module of the TOE in support of the Wireless Client Encryption Policy and therefore this requirement contributes to satisfying O.CRYPTOGRAPHY.

8.3 Security Assurance Requirements Rationale

The US Government Wireless Local Area Network (WLAN) Client PP provides rationale for the security assurance requirements, demonstrating that they are sufficient given the statement of security environment and security objectives. The rationale is provided in Section 6.5 of the US Government Wireless Local Area Network (WLAN) Client PP and is valid for this ST as no new security requirements or security objectives were added.

This ST increases the assurance claim in the PP to EAL3 augmented with ALC_FLR.2. This entails the following changes to the set of assurance requirements specified in the PP: ACM_CAP.3 replaces ACM_CAP.2; ADV_HLD.2 replaces ADV_HLD.1; ALC_DVS.1 is added; ATE_COV.2 replaces ATE_COV.1; and ATE_DPT.1 is added. The sponsor has chosen to increase the assurance claim due to the requirements of its customers, who are requesting EAL3 TOEs for their environments.

8.4 Strength of Functions Rationale

The US Government Wireless Local Area Network (WLAN) Client 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 ST as no new security objectives were added.

8.5 Requirement Dependency Rationale

The US Government Wireless Local Area Network (WLAN) Client PP requirements have been evaluated and it has been determined that all dependencies have been satisfactorily addressed in the US Government Wireless Local Area Network (WLAN) Client PP. The following table therefore analyzes the dependencies only of the requirements that have been added to this ST.

ST Requirement	CC Dependencies and Explicitly Stated Requirement Dependencies	ST Dependencies
FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP_EXP.2(1), FCS_COP_EXP.2(2), FCS_COP_EXP.2(3), FCS_COP_EXP.2(7), FCS_CKM.4, FMT_MSA.2
FCS_COP_EXP.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP_EXP.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP_EXP.2(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(2). In addition, see rationale below
FCS_COP_EXP.2(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(3). In addition, see rationale below
FCS_COP_EXP.2(6)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(3). In addition, see rationale below
FCS_COP_EXP.2(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1(1), FCS_CKM.4, FMT_MSA.2
FCS_COP_EXP.2(8)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	None – see rationale below

ST Requirement	CC Dependencies and Explicitly Stated Requirement Dependencies	ST Dependencies
FTP_ITC.1	None	FCS_COP_EXP.2(1-7)
FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP_EXP.2(4). In addition, see rationale below
FCS_CKM.1(3)	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP_EXP.2(5), FCS_COP_EXP.2(6). In addition, see rationale below
ACM_CAP.3	ALC_DVS.1	ALC_DVS.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	ADV_FSP.1, ADV_RCR.1
ALC_DVS.1	None	None
ATE_COV.2	ADV_FSP.1, ATE_FUN.1	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	ADV_HLD.2, ATE_FUN.1

Table 5: ST Dependency Analysis

The PP defines the dependencies of FCS_COP_EXP.2 as [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2. Since CC Part 2 also identifies FDP_ITC.2 as a possible dependency, this has been included in the above table for completeness.

FCS_COP_EXP.2(4-6) specify requirements for cryptographic operations using DSA and RSA. The TOE performs these operations using keying material associated with certificates provided by the IT environment. The requirements for generating these keys are specified by FCS_CKM.1(2) and FCS_CKM.1(3). However, the TOE does not have any reliance on other aspects of the cryptographic key lifecycle, such as cryptographic key destruction (FCS_CKM.4) or use of secure security attributes (FMT_MSA.2). As such, these dependencies have not been specified as security requirements in the IT environment of the TOE.

FCS_COP_EXP.2(8) specifies a requirement for secure hashing using SHA-1. This is an unkeyed cryptographic algorithm, and as such the key management and secure security attribute requirements specified by FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 are not applicable.

8.6 Explicitly Stated Requirements Rationale

The US Government Wireless Local Area Network (WLAN) Client PP provides rationale for the explicitly stated security requirements, demonstrating that the explicitly stated security requirements are necessary, because the Common Criteria requirements were found to be insufficient as stated. The rationale (provided in Section 6.8 of the US Government Wireless Local Area Network (WLAN) Client PP) is valid for this ST as the only explicitly stated security functional requirements added to this ST are iterations of FCS_COP_EXP.2.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functional and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The following table demonstrates the relationship between security requirements and security functions.

	Security Audit	Cryptographic Support	User Data Protection	Security Management	Protection of the TOE Security Functions
FAU_GEN_EXP.1	X				
FCS_BCM_EXP.1		X			
FCS_CKM.1(1)		X			
FCS_CKM_EXP.2		X			
FCS_CKM.4		X			
FCS_COP_EXP.1		X			
FCS_COP_EXP.2(1)		X			
FCS_COP_EXP.2(2)		X			
FCS_COP_EXP.2(3)		X			
FCS_COP_EXP.2(4)		X			
FCS_COP_EXP.2(5)		X			
FCS_COP_EXP.2(6)		X			
FCS_COP_EXP.2(7)		X			
FCS_COP_EXP.2(8)					X
FDP_IFC.1			X		
FDP_IFF.1			X		
FDP_RIP.1(1)			X		
FMT_MSA.2				X	
FMT_MSA.3				X	
FMT_SMF.1(1)				X	
FMT_SMF.1(2)				X	
FMT_SMF.1(3)				X	
FPT_TST_EXP.1					X
FPT_TST_EXP.2					X
FTP_ITC.1			X		

Table 6: Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.