Network Device Collaborative Protection Profile (NDcPP) Extended Package
Wireless Local Area Network (WLAN) Access Systems

May 29, 2015
Version 1.0

Table of Contents

List of Tables

1 Introduction

This Extended Package (EP) describes security requirements for a Wireless Local Area Network (WLAN) Access System (defined to be a device or system at the edge of a private network that establishes an encrypted IEEE 802.11 link, which protects wireless data-in-transit from disclosure and modification) and is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. However, this EP is not complete in itself, but rather extends the *Security Requirements for Network Devices collaborative Protection Profile* (NDcPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDcPP.

1.1 Conformance Claims

The Security Requirements for Network Devices collaborative Protection Profile (NDcPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDcPP baseline with additional SFRs and associated 'Assurance Activities' specific to WLAN Access System network infrastructure devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

As an EP of the NDcPP, it is expected that the content of both this EP and the NDcPP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in so doing. An ST must identify the applicable versions of the NDcPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

1.3 Compliant Targets of Evaluations

This EP specifically addresses WLAN (IEEE 802.11) Access Systems. A compliant WLAN Access System is a system composed of hardware and software that is connected to a network and has an infrastructure role in the overall enterprise network. In particular, a WLAN Access System establishes a secure wireless (IEEE 802.11) link that provides an authenticated and encrypted path to an enterprise network and thereby decreases the risk of exposure of information transiting "over-the-air".

Since this EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

2 Security Problem Description

This Extended Package (EP) is written to address the situation when network packets cross the boundary between a wired private network and a wireless client via a WLAN Access System. The WLAN Access System provides secure communication between a user (wireless client) and a wired (trusted) network by supporting security functions such as administration, authentication, encryption, and the protection and handling of data in transit. To protect the data in-transit from disclosure and modification, a WLAN Access System is used to establish secure communications. The WLAN Access System provides one end of the secure cryptographic tunnel and performs encryption and decryption of network packets in accordance with a WLAN Access System security policy negotiated with its authenticated wireless client. It supports multiple simultaneous wireless connections and is capable of establishing and terminating multiple cryptographic tunnels to and from those peers.

The proper installation, configuration, and administration of the WLAN Access System are critical to its correct operation.

Note that this EP does not repeat the threats identified in the NDcPP, though they all apply given the conformance and hence dependence of this EP on the NDcPP. Note also that while the NDcPP contains only threats to the ability of the TOE to provide its security functions, this EP addresses only threats to resources in the operational environment. Together the threats of the NDcPP and those defined in this EP define the comprehensive set of security threats addressed by a WLAN Access System TOE.

2.1 Threats

2.1.1Unauthorized Disclosure of Information

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of nonexistent/insufficient WLAN data encryption that exposes the WLAN data in transit to rogue elements), then those internal devices may be susceptible to the unauthorized disclosure of information.

(T.NETWORK_DISCLOSURE)

2.1.2Inappropriate Access to Services

Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network.

(T. NETWORK_ACCESS)

2.1.3TSF Failure

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

(T.TSF_FAILURE)

2.1.4Compromise of Data Integrity

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.

(T.DATA_INTEGRITY)

2.1.5Replay Attack

If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the wireless network and send the packets at a later time, possibly unknown by the intended receiver.

(T.REPLAY_ATTACK)

2.2 Assumptions

The Assumptions for WLAN Access Systems can be found in Appendix A.1.1.

3 Security Objectives

3.1 Security Objectives for the TOE

The Security Problem described in Section 2 will be addressed by a combination of cryptographic capabilities. Compliant TOEs will provide security functionality that addresses threats to the TOE and enforces policies that are imposed by law or regulation. The following subsections provide a description of the security objectives required to meet the threats/policies previously discussed. The descriptions of the security objectives are in addition to that described in [NDcPP].

Note: in each subsection below particular security objectives are identified (highlighted by *O.*) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

3.1.1Data Protection

To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detecting modification of data that is transmitted outside of the TOE.

From an infiltration perspective, WLAN Access Systems serve not only to limit access to only specific WLAN users and systems, but determine whether network traffic will be encrypted or transmitted in plaintext. With these limits, network port scanning (above layer 3) by unauthorized entities can be prevented, and access to information on a protected network can be limited to that obtainable from properly authenticated WLAN client systems.

(O.CRYPTOGRAPHIC_FUNCTIONS -> FCS_COP.1(1), FCS_IPSEC_EXT.1, FCS_CKM.1(1), FCS_CKM.2(2), FCS_CKM.2(3), FIA_PSK_EXT.1)

3.1.2Authentication

To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability will allow a WLAN peer to establish WLAN connectivity with a WLAN Access System. WLAN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.

From both an ingress and egress perspective, WLAN Access Systems can be configured using a combination of authentication (e.g. EAP-TLS) and data encryption (e.g. 128-bit AES) to allow communication only between protected network resources and authorized WLAN client devices.

(O.AUTHENTICATION -> FTP_ITC.1, FCS_IPSEC_EXT.1, FIA_AFL.1, FIA_UAU.6, FIA_8021X_EXT.1, FTA_TSE.1)

3.1.3Insecure Operations

There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism.

(O.FAIL_SECURE -> FPT_FLS.1, FPT_TST_EXT.1)

3.1.4System Monitoring

To address the issues of administrators being able to monitor the operations of the WLAN Access System, this security objective, which originated in the NDcPP, is extended as follows.

Auditable events, specific to WLAN functionality and security have been added.

(O.SYSTEM_MONITORING -> FAU_GEN.1)

3.1.5TOE Administration

This security objective addresses the issues involved with remote administration of the WLAN Access System. Compliant TOEs will provide the functions necessary to address failed authentication attempts by a remote administrator.

(O.TOE_ADMINISTRATION -> FIA_AFL.1, FMT_SMR.1)

3.2 Security Objectives for the Operational Environment

The objectives that are required to be met by the TOE's operational environment are defined in Section A.2.2.

4 Security Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*, with additional extended functional components.

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with italicized text;
- Refinement made by EP author: Indicated with bold text and strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with italicized and underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3); and
- Extended SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

4.2 TOE Security Functional Requirements

Since this EP Extends the NDcPP, it is expected that several security functions are inherited from the base PP (and are not included here). This security functionality includes: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_IPSEC_EXT.1, FIA_X509_EXT.1, and FTP_TRP.1.

There are four SFR components that exist in the NDcPP that required some form of modification in this EP. There are ten newly introduced SFRs contained in this EP, and 13 additional audit events were specified as well.

4.2.1NDcPP Security Functional Requirement Direction

This section instructs the ST Author what selections must be made to certain SFRs contained in the NDcPP in order to support related SFRs in the WLAN Access System EP. This is captured by expressing the element where the mandatory selection has been made. The ST Author may complete the remaining selection items as they wish, to ensure specific capabilities or behavior is present in the TOE. In addition to providing the necessary selection required, there is an element, FPT_TST_EXT.1.2 that must be added to the NDcPP FPT_TST_EXT.1 component to be compliant with this EP.

Full assurance activities are not repeated for the requirements in this section, only the additional testing needed to supplement that already captured in the NDcPP is included. What is important for the evaluator when they assess the ST and TOE against the SFRs as specified here is that the proper selections have been made and the appropriate tests are performed to demonstrate compliance to the requirements.

4.2.1.1 FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) **Refinement:** The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES used in *CBC, CCMP*** [selection: GCM, GCMP] mode and cryptographic key sizes ***128 bits*** [selection: 192 bits, 256 bits] that meet the following: ***AES as specified in ISO 18033-3, CCMP as defined in NIST SP 800-38C and IEEE 802.11-2012,*** [selection: CBC as specified in ISO 10116, GCM as specified in ISO 19772, CCMP and GCMP as specified in NIST SP800-38D and IEEE 802.11ac-2013*)*].

Application Note: This requirement mandates two modes for AES with key size of 128 bits be implemented. It is not expected that these modes will both be used for all encryption/decryption functionality. Rather, the mandates serve particular purposes: to comply with the FCS_IPSEC requirements, CBC mode is mandated, and to comply with IEEE 802.11-2012, AES-CCMP (which uses AES in CCM as specified in SP 800-38C) must be implemented.

For the first selection of FCS_COP.1.1(1), the ST author should choose the additional mode or modes in which AES operates. For the second selection, the ST author should choose the key sizes that are supported by this functionality. 128-bit CCMP is required in order to comply with FCS_CKM.1.1(2). Note that optionally, AES-CCMP-256 or AES-GCMP-256 with cryptographic key size of 256 bits may be implemented for IEEE 802.11ac connections. In the future, one of these modes may be required.

Assurance Activity:

Test

In addition to those tests specified in the NDcPP, the evaluator shall perform the following tests.

AES-CCM Tests

The evaluator shall test the generation-encryption and decryption-verification functionality of AES-CCM for the following input parameter and tag lengths:

128 bit and 256 bit keys

Two payload lengths. One payload length shall be the shortest supported payload length, greater than or equal to zero bytes. The other payload length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits).

Two or three associated data lengths. One associated data length shall be 0, if supported. One associated data length shall be the shortest supported payload length, greater than or equal to zero bytes. One associated data length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits). If the implementation supports an associated data length of 216 bytes, an associated data length of 216 bytes shall be tested.

Nonce lengths. All supported nonce lengths between 7 and 13 bytes, inclusive, shall be tested.
Tag lengths. All supported tag lengths of 4, 6, 8, 10, 12, 14 and 16 bytes shall be tested.

Due to the restrictions that IEEE 802.11 specifies for this mode (nonce length of 13 and tag length of 8), it is acceptable to test a subset of the supported lengths as long as the selections fall into the ranges specified above. In this case, the evaluator shall ensure that these are the only supported lengths.
To test the generation-encryption functionality of AES-CCM, the evaluator shall perform the following four tests:

> **Test 1**. For EACH supported key and associated data length and ANY supported payload, nonce and tag length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
>
> **Test 2**. For EACH supported key and payload length and ANY supported associated data, nonce and tag length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
>
> **Test 3**. For EACH supported key and nonce length and ANY supported associated data, payload and tag length, the evaluator shall supply one key value and 10 associated data, payload and nonce value 3-tuples and obtain the resulting ciphertext.
>
> **Test 4**. For EACH supported key and tag length and ANY supported associated data, payload and nonce length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.

To determine correctness in each of the above tests, the evaluator shall compare the ciphertext with the result of generation-encryption of the same inputs with a known good implementation.

To test the decryption-verification functionality of AES-CCM, for EACH combination of supported associated data length, payload length, nonce length and tag length, the evaluator shall supply a key value and 15 nonce, associated data and ciphertext 3-tuples and obtain either a FAIL result or a PASS result with the decrypted payload. The evaluator shall supply 10 tuples that should FAIL and 5 that should PASS per set of 15.

Additionally, the evaluator shall use tests from the IEEE 802.11-02/362r6 document “Proposed Test vectors for IEEE 802.11 TGi”, dated September 10, 2002, Section 2.1 AES-CCMP Encapsulation Example and Section 2.2 Additional AES CCMP Test Vectors to further verify the IEEE 802.11-2012 implementation of AES-CCMP.

4.2.1.2 FCS_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications

FCS_IPSEC_EXT.1 is inherited from Appendix B of the NDcPP. However, for this EP it is considered mandatory (not selection-based) and must be included in the ST.

4.2.1.3 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 **Refinement:** The TSF shall be **capable of using IEEE 802.11-2012 (WPA2), IEEE 802.1X, IPsec, and** [selection: SSH, TLS, HTTPS, no other protocol] **to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: WLAN clients, audit servers, 802.1X authentication servers, and [*assignment: [other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: The intent of the above requirement is to use a cryptographic protocol to protect all external communications with authorized IT entities that the TOE interacts with to perform its functions. IEEE 802.11-2012 (WPA2) with IEEE 802.1X is required for communications with wireless clients; IPsec is required at least for communications with the authentication server.

If the TOE communicates with other necessary authorized IT entities (NTP server, audit server), then they must use IPsec or one of the other listed protocols (SSH, TLS and TLS/HTTPS are allowed), and the ST author makes the appropriate selections, then ensures the detailed requirements in Appendix B (of the NDcPP) corresponding to their selection are included in the ST if not already present. While there are no requirements on the party initiating the communication, the ST author lists in the assignment for FTP_ITC.1.3 the services for which the TOE can initiate the communication with the authorized IT entity.

The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage.

The remaining elements of this SFR are inherited directly from the base NDcPP, with no modifications. Communications with remote administrators are covered by FTP_TRP, inherited directly from the NDcPP.

Assurance Activity:

The evaluator shall perform the following activities in addition to the assurance activity specified in the base NDcPP for this SFR:

TSS

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Guidance

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Test

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.

Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Test 4: The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, physically interrupt an established connection. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Test 5: The evaluator shall first configure the access system to use only WPA2 (AES, with no fallback to TKIP), then ensure that a WPA2 (AES) connection can be made between the access system and a client device. Finally, the evaluator shall attempt to connect a client device that does not support AES to the access system and ensure that the access system rejects the connection (does not fall back to TKIP).

Further assurance activities are associated with the specific protocols.

4.2.1.4 FPT_TST_EXT.1 Extended: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests during initial start-up (on power on) and [selection: periodically during normal operation, at the request of the authorized user, at the conditions [assignment: *conditions under which self-tests should occur*]] to demonstrate the correct operation of the TSF: [assignment: *list of self-tests run by the TSF*].

FPT_TST_EXT.1.2 The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

Assurance Activity:

The evaluator shall perform the following activities in addition to the assurance activity specified in the base NDcPP for this SFR:

TSS

The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution, which includes the generation and protection of the "check value" used to ensure integrity as well as the verification step. This description shall also cover the digital signature service used in performing these functions. The evaluator also checks the operational guidance to ensure that any actions required by the administrator to initialize or operate this functionality are present.

Guidance

The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.

Test

The evaluator shall perform the following tests:

Test 1: Following the operational guidance, the evaluator shall initialize the integrity protection system. The evaluator shall perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors.

Test 2: The evaluator shall modify the TSF executable, and cause that executable to be loaded by the TSF. The evaluator shall observe that an integrity violation is triggered (care must be taken so that the integrity violation is determined to be the cause of the failure to load the module, and not the fact that the module was modified so that it was rendered unable to run because its format was corrupt).

4.2.2TOE Security Functional Requirements

Security functional requirements in the main body of this EP are divided into those that are inherited from the NDcPP and those that are specific to WLAN AS TOEs. This section contains requirements that must be met by the TOE and are not covered in the base NDcPP.

4.2.2.1 FCS_CKM.1(2) Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)

FCS_CKM.1.1(2) **Refinement:** The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [***PRF-384***] and [selection: PRF-704, no other] and specified cryptographic key sizes [***128 bits***] and [selection: 256 bits, no other key sizes] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: [***IEEE 802.11-2012***] and [selection: IEEE 802.11ac-2014, no other standards].

Application Note: The cryptographic key derivation algorithm required by IEEE 802.11-2012 (Section 11.6.1.2) and verified in WPA2 certification is PRF-384, which uses the HMAC-SHA-1 function and outputs 384 bits. The use of GCMP is defined in IEEE 802.11ac-2013 (Section 11.4.5) and requires a KDF based on HMAC-SHA-256 (for 128-bit symmetric keys) or HMAC-SHA-384 (for 256-bit symmetric keys). This KDF outputs 704 bits.

This requirement applies only to the keys that are generated/derived for the communications between the access point and the client once the client has been authenticated. It refers to the derivation of the GTK (through the RBG specified in this EP) as well as the derivation of the PTK from the PMK, which is done using a random value generated by the RBG specified in this EP, the HMAC function as specified in this EP, as well as other information. This is specified in IEEE 802.11-2012 primarily in chapter 11.

Assurance Activity:

TSS

The cryptographic primitives will be verified through assurance activities specified elsewhere in this EP. The evaluator shall verify that the TSS describes how the primitives defined and implemented by this EP are used by the TOE in establishing and maintaining secure connectivity to the wireless clients. This description shall include how the GTK and PTK are generated or derived. The TSS shall also provide a description of the developer's method(s) of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also proof of third-party testing that is performed (e.g. WPA2 certification). The evaluator shall ensure that the description of the testing methodology is of sufficient detail to determine the extent to which the details of the protocol specifics are tested.

Test

The evaluator shall also perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless client:

Step 1: The evaluator shall configure the access point to an unused channel and configure the WLAN sniffer to sniff only on that channel (i.e., lock the sniffer on the selected channel). The sniffer should also be configured to filter on the MAC address of the TOE and/or client.

Step 2: The evaluator shall configure the TOE to communicate with a WLAN client using IEEE 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and WLAN client, and allow the TOE to authenticate, associate and successfully complete the 4-way handshake with the client.

Step 4: The evaluator shall set a timer for 1 minute, at the end of which the evaluator shall disconnect the client from the TOE and stop the sniffer.

Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK from the 4-way handshake frames and pre-shared key as specified in IEEE 802.11-2012.

Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the client and TOE after the 4-way handshake successfully completed, and without the frame control

value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the PTK to decrypt the data portion of the packet as specified in IEEE 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text.

Step 7: The evaluator shall repeat Step 6 for the next 2 data frames between the TOE and client, and without frame control value 0x4208.

4.2.2.2 FCS_CKM.2(2) Cryptographic Key Distribution (PMK)

FCS_CKM.2.1(2) **Refinement:** The TSF shall **receive the 802.11 Pairwise Master Key (PMK)** in accordance with a specified cryptographic key distribution method: [***from 802.1X Authorization Server***] that meets the following: [***IEEE 802.11-2012***] **and does not expose the cryptographic keys**.

Application Note: This requirement applies to the Pairwise Master Key that is received from the RADIUS server by the TOE. The intent of this requirement is to ensure conformant TOEs implement 802.1X authentication prior to establishing secure communications with the client. The intent is that any WLAN AS evaluated against this EP will support WPA2-ENT and certificate-based authentication mechanisms and therefore disallows implementations that support only pre-shared keys. Because communications with the RADIUS server are required to be performed over an IPsec-protected connection, the transfer of the PMK will be protected.

Assurance Activity:

TSS

The evaluator shall examine the TSS to determine that it describes how the PMK is transferred (that is, through what EAP attribute) to the TSF.

Test

The evaluator shall establish a session between the TOE and a RADIUS server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the RADIUS server and the TOE during a successful attempt to connect a wireless client to the TOE to determine that the PMK is not exposed.

4.2.2.3 FCS_CKM.2(3) Cryptographic Key Distribution (GTK)

FCS_CKM.2.1(3) **Refinement:** The TSF shall distribute **Group Temporal Key (GTK)** in accordance with a specified cryptographic key distribution method: [**AES Key Wrap in an EAPOL-Key frame**] that meets the following: [**NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations**] **and does not expose the cryptographic keys**.

Application Note: This requirement applies to the Group Temporal Key (GTK) that is generated by the TOE for use in broadcast and multicast messages to clients to which it's connected. 802.11-2012 specifies the format for the transfer as well as the fact that it must be wrapped by the AES Key Wrap method specified in NIST SP 800-38F.

Assurance Activity:

TSS

The evaluator shall check the TSS to ensure that it describes how the GTK is wrapped prior to be distributed using the AES implementation specified in this EP, and also how the GTKs are distributed when multiple clients connect to the TOE.

Test

The evaluator shall also perform the following test using a packet sniffing tool to collect frames between a wireless client and the TOE (which may be performed in conjunction with the assurance activity for FCS_CKM.1.1(2).

To fully test the broadcast/multicast functionality, these steps shall be performed as the evaluator connects multiple clients to the TOE. The evaluator shall create at least two multicast groups among a subset of clients connected to the TOE, each consisting of at least two clients but less than all of the clients connected to the TOE. Some (but not all) of the clients shall be in both groups. The evaluator shall ensure that GTKs established are sent to the appropriate participating clients.

Step 1: The evaluator shall configure the access point to an unused channel and configure the WLAN sniffer to sniff only on that channel (i.e., lock the sniffer on the selected channel). The sniffer should also be configured to filter on the MAC address of the TOE and/or client.

Step 2: The evaluator shall configure the TOE to communicate with the client using IEEE 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and client, and allow the client to authenticate, associate and successfully complete the 4-way handshake with the TOE.

Step 4: The evaluator shall set a timer for 1 minute, at the end of which the evaluator shall disconnect the TOE from the client and stop the sniffer.

Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK and GTK from the 4-way handshake frames and pre- shared key as specified in IEEE 802.11-2012.

Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and client after the 4-way handshake successfully completed, and with the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the GTK to decrypt the data portion of the selected packet as specified in IEEE 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text.

Step 7: The evaluator shall repeat Step 6 for the next 2 data frames with frame control value 0x4208.

4.2.2.4 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 **Refinement:** The TSF shall detect when **an Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall [selection, choose one of: prevent the offending remote administrator from successfully authenticating until [assignment: *action*] is taken by a local Administrator; prevent the offending remote administrator from successfully authenticating until an Administrator defined time period has elapsed].

Application Note: This requirement does not apply to an administrator at the local console, since it does not make sense to lock a local administrator's account in this fashion. This could be addressed by (for example) requiring a separate account for local administrators or having the authentication mechanism implementation distinguish local and remote login attempts. The "action" taken by a local administrator is implementation specific and would be defined in the administrator guidance (for example, lockout reset or password reset). The ST author chooses one of the selections for handling of authentication failures depending on how the TOE has implemented this handler.

Assurance Activity:

TSS

The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.

Guidance

The evaluator shall also examine the operational guidance to ensure that instructions for configuring the number of successive unsuccessful authentication attempts (1.1) and time period (1.2, if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.

Test

The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., TLS, SSH):

Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached, attempts with valid credentials are not successful. For each action specified by the requirement, the evaluator shall show that following the operational guidance and performing each action to allow the remote administrator access are successful.

Test 2: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE and a time period after which valid logins will be allowed for a remote administrator. After exceeding the specified number of invalid login attempts

and showing that valid login is not possible, the evaluator shall show that waiting for the interval defined by the time period before another access attempt will result in the ability for the remote administrator to successfully log on using valid credentials.

4.2.2.5 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the administrative user under the conditions: when the user changes their password, [selection: following TSF-initiated locking (FTA_SSL), [assignment: *other conditions*], no other conditions].

Assurance Activity:

Test

The evaluator shall perform the following test for each of the conditions specified in the requirement:

Test 1: The evaluator shall attempt to change their password as directed by the operational guidance. While making this attempt, the evaluator shall verify that re-authentication is required.

4.2.2.6 FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Authenticator" role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

Application Note: This requirement covers the TOE's role as the authenticator in an 802.1X authentication exchange. If the exchange is completed successfully, the TOE will obtain the PMK from the RADIUS server and perform the 4-way handshake with the wireless client (supplicant) to begin 802.11 communications.

As indicated previously, there are at least three communication paths present during the exchange; two with the TOE as an endpoint and one with TOE acting as a transfer point only. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless client as specified in 802.1X-2007. The TOE also establishes (or has established) a RADIUS protocol connection (which is tunneled inside of an IPsec connection) with the RADIUS server. The wireless client and RADIUS server establish an EAP-TLS session (RFC 5216); in this transaction the TOE merely takes the EAP-TLS packets from its EAPOL/RADIUS endpoint and transfers them to the other endpoint. Because the specific authentication method (TLS in this case) is opaque to the TOE, there are no requirements with respect to RFC 5126 in this EP. However, the base RADIUS protocol (2865) has an update (3579) that will need to be addressed in the implementation and assurance activities. Additionally, RFC 5080 contains implementation issues that will need to be addressed by developers, but which levy no new requirements.

The point of performing 802.1X authentication is to provide access to the network (assuming the authentication was successful and that all 802.11 negotiations are performed successfully); in the terminology of 802.1X, this means the wireless client has access to the "controlled port" maintained by the TOE.

Assurance Activity:

TSS

In order to show that the TSF implements the 802.1X-2010 standard correctly, the evaluator shall ensure that the TSS contains the following information:

- The sections (clauses) of the standard that the TOE implements;
- For each identified section, any options selected in the implementation allowed by the standards are specified; and
- For each identified section, any non-conformance is identified and described, including a justification for the non-conformance.

Because the connection to the RADIUS server will be contained in an IPsec tunnel (FCS_IPSEC_EXT.1), the security mechanisms detailed in the RFCs identified in the requirement are not relied on to provide protection for these communications. Consequently, no extensive analysis of the RFCs is required. However, the evaluator shall ensure that the TSS describes the measures (documentation, testing) that are taken by the product developer to ensure that the TOE conforms to the RFCs listed in this requirement.

Test

Test 1: The evaluator shall demonstrate that a wireless client has no access to the test network. After successfully authenticating with a RADIUS server through the TOE, the evaluator shall demonstrate that the wireless client does have access to the test network.

Test 2: The evaluator shall demonstrate that a wireless client has no access to the test network. The evaluator shall attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.

Test 3: The evaluator shall demonstrate that a wireless client has no access to the test network. The evaluator shall attempt to authenticate using an invalid RADIUS certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.

Note: Tests 2 and 3 above are not tests that "EAP-TLS works", although that's a by-product of the test. The test is actually that a failed authentication (under two failure modes) results in denial of access to the network, which is the 3rd element of this component.

4.2.2.7 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for [selection: IEEE 802.11 WPA2-PSK, IPsec, no other protocols, [assignment: *other protocols that use pre-shared keys*]].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [selection: [assignment: *other supported lengths*], no other lengths];
- are composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall be able to [selection: accept, generate using the random bit generator specified in FCS_RBG_EXT.1] bit-based pre-shared keys.

Application Note: In the first selection, if other protocols can use pre-shared keys, they should be listed in the assignment as well; otherwise “no other protocols” should be chosen. The intent of this requirement is that all protocols will support both text-based and bit-based pre-shared keys.

For the length of the text-based pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.

For FIA_PSK_EXT.1.3, the ST author specifies whether the TSF merely accepts bit-based pre-shared keys, or is capable of generating them. If it generates them, the requirement specifies that they must be generated using the RBG provided by the TOE.

Assurance Activity:

TSS

The evaluator shall examine the TSS to ensure that it identifies all protocols that allow both text-based and bit-based pre-shared keys, and states that text-based pre-shared keys of 22 characters are supported. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by the protocol, and that this conditioning is consistent with the last selection in the FIA_PSK_EXT.1.3 requirement.

The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Guidance

The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.

The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both).

Test

The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.

Test 1: The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.

Test 2 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.

Test 3 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

Test 4 [conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

4.2.2.8 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-tests.

Application Note: The intent of this requirement is to express the fail secure capabilities that the TOE possesses. This means that the TOE must be able to attain a secure/safe state (shutdown) when any of the identified failures occurs.

Assurance Activity:

TSS

The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall first examine the TSS section to ensure that all failure modes specified in the ST are described. The evaluator shall review the TSS to determine that the definition of secure state is defined and is suitable to ensure protection of key material and user data.

Test

For each failure mode specified in the ST, the evaluator shall ensure that the TOE attains a secure state (shutdown) after initiating each failure mode type.

4.2.2.9 FMT_SMR.1 Security Management Roles

FMT_SMR.1.3 The TSF shall ensure that the ability to remotely administer the TOE from a wireless client shall be disabled by default.

Assurance Activity:

Guidance

The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.

Test

The evaluator shall perform the following test:

Test 1: The evaluator shall demonstrate that after configuring the TOE for first use from the operational guidance, it is possible to establish an administrative session with the TOE on the "wired" portion of the device. They shall then demonstrate that an identically configured wireless client that can successfully connect to the TOE cannot be used to perform administration.

4.2.2.10 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 **Refinement:** The TSF shall be able to deny establishment **of a wireless client session** based on **TOE interface, time, day**, [assignment: *other attributes*].

Application Note: The "TOE interface" can be specified in terms of the device in the TOE that the WLAN client is connecting to (e.g. specific WLAN access point(s)). "Time" and "day" refer to time-of-day and day-of-week respectively.

The assignment is to be used by the ST author to specify additional attributes on which denial of session establishment can be based.

Assurance Activity:

TSS

The evaluator shall examine the TSS to determine that all of the attributes on which a client session can be denied are specifically defined.

Guidance

The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

Test

The evaluator shall also perform the following test for each attribute:

Test 1: The evaluator successfully establishes a client session with a wireless client. The evaluator then follows the operational guidance to configure the system so that that client's access is denied based on a specific value of the attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting (for instance, the client is denied WLAN access based upon the TOE interface (e.g. WLAN access point) it is connecting to or the client is denied access based upon the time-of-day or day-of-week it is attempting connection on). The evaluator shall observe that the access attempt fails.

4.2.2.11 FAU_GEN.1 Audit Data Generation

There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the NDcPP. The following events should be combined with those of the NDcPP in the context of a conforming Security Target.

The following audit events are required for this EP.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1(2)	Failure of the key generation activity.	None.
FCS_CKM.2(2)	Failure of the key distribution activity.	None.
FCS_CKM.2(3)	Failure of the key distribution activity, including failures related to wrapping the GTK.	Identifier(s) for intended recipients of wrapped key.
FCS_COP.1(1)	Failure of WPA2 encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted, non-TOE endpoint of connection (IP address).
FCS_IPSEC_EXT.1	Protocol failures. Establishment/Terminiaton of an Ipsec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FTP_ITC.1	Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data.	Identification of the initiator and target of channel.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	None.
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (MAC address).
FIA_PSK_EXT.1	None.	None.
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_TST_EXT.1	Execution of this set of TSF self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.

Table 1: Auditable Events

Appendix A - Rationale

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats addressed by WLAN Access Systems; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artifacts that can be used for the evaluation activities associated with this document.

A.1 Security Problem Definition

A.1.1Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions are in addition to those defined in the NDcPP and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption Name	Assumption Definition
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Table 2: Assumptions

A.1.2Threats

The threats listed below are addressed by WLAN Access Systems. Note that these threats are in addition to those defined in the NDcPP, all of which apply to WLAN Access Systems.

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.

Table 3: Threats

A.1.3Organizational Security Policies

No organizational policies have been identified that are specific to WLAN Access Systems. However, all the organizational security policies in the NDcPP apply to WLAN Access Systems.

A.1.4Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

Threat or Assumption	Security Objectives
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.AUTHENTICATION and O.CRYPTOGRAPHIC_FUNCTIONS
T.NETWORK_ACCESS	O.AUTHENTICATION, O.TOE_ADMINISTRATION
T.TSF_FAILURE	O.FAIL_SECURE, O.SYSTEM_MONITORING
T.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS
T.REPLAY_ATTACK	O.AUTHENTICATION and O.CRYPTOGRAPHIC_FUNCTIONS

Table 4: Security Problem Definition Correspondence

A.2 Security Objectives

A.2.1Security Objectives for the TOE

The following table contains security objectives specific to WLAN Access Systems. These security objectives are in addition to those defined in the NDcPP, all of which apply to WLAN Access Systems. Note that while two of the NDcPP security objectives (O.SYSTEM_MONITORING and O.TOE_ADMINISTRATION) have been extended in this EP that does not affect the corresponding security objective definitions.

Security Objective Name	Security Objective Definition
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.FAIL_SECURE	Upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
O.SYSTEM_MONITORING	The TOE will provide a means to audit events specific to WLAN functionality and security.
O.TOE_ADMINISTRATION	The TOE will provide the functions necessary to address fialed authentication attempts by a remote administrator.

Table 5: Security Objectives for the TOE

A.2.2Security Objectives for the Operational Environment

The following table contains security objectives specific to the operational environments for WLAN Access Systems. These security objectives are in addition to those defined in the NDcPP, all of which apply to the operational environments for WLAN Access Systems.

Security Objective Name	Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

Table 6: Security Objectives for the OE

A.2.3Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.

Appendix B – Optional Requirements

As indicated in the introduction to this EP, the baseline requirements are contained in the body of this EP. There are additional requirements that can be included in the ST, but do not have to be in order for a TOE to claim conformance to this EP. It is not mandated that all WLAN Access Systems be implemented as distributed systems, as such, the requirements in this Appendix are not included in the body of this EP. In the case where the TOE is physically distributed among several components, communications between those components must be protected and the below requirements must be included in the ST.

Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix B, Appendix C, and/or Appendix D but are not listed (e.g., FMT-type requirements) are also included in the ST.

B.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 **Refinement:** The TSF shall **use** [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] **with security strength commensurate with all other trusted communications to** protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

Application Note: This requirement ensures all communications between components of a distributed TOE is protected through the use of an encrypted communications channel. The data passed in this trusted communication channel are encrypted as defined in the protocol chosen in the selection. The ST author chooses the mechanisms supported by the TOE, and then ensures the appropriate requirements from the NDcPP corresponding to their selection are copied to the ST if not already present.
For the purposes of this requirement, security strength is defined by NIST SP 800-57, "commensurate" means that the strengths must, at a minimum, meet the requirements for the cryptographic primitives listed in the EP, and "other trusted communications" refers to the mechanisms specified in FPT_ITC.

Assurance Activity:

TSS

The evaluator shall examine the TSS to determine that the methods and protocols used to protect distributed TOE components are described. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The evaluator shall examine all methods and ensure that the strengths meet the requirements described in the FCS_CKM, FCS_COP, and selected protocol requirements. The evaluator shall ensure that the TSS clearly identified the various strengths for the keys/algorithms used by each protocol and indicates that the overall strength of the channels is the lowest strength used.

Guidance

The evaluator shall confirm that the operational guidance contains instructions for establishing the communication paths for each supported method.

Test

The evaluator shall also perform the following tests:

Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) communications method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

Test 2: The evaluator shall ensure, for each method of communication, the channel data is not sent in plaintext.

Further assurance activities are associated with the specific protocols.

B.2 FCS_CKM.2(4) Cryptographic Key Distribution

FCS_CKM.2.1(4) **Refinement:** The TSF shall distribute **the IEEE 802.11 keys** in accordance with a specified key distribution method: [**FPT_ITT**] that meets the following: [**FCS_COP security strength**] **and does not expose the cryptographic keys**.

Application Note: This requirement applies to any key necessary for successful IEEE 802.11 connections (not covered by FCS_CKM.2.1(3). In cases where a key must be distributed to other access points, this communication must be performed via a mechanism of commensurate cryptographic strength. Because communications with any component of a distributed TOE are required to be performed over a trusted connection, the transfer of these keys will be protected.

Assurance Activity:

TSS

The evaluator shall examine the TSS to determine that it describes which keys are distributed outside the TOE, where they are sent, and the purpose for this transfer.

Guidance

If this is dependent on configuration of the System, the evaluator shall confirm that the operational guidance contains instructions for how to configure that the keys are adequately protected.

Test

This requirement will be tested in conjunction with the tests for the cryptographic primitives, the secure protocols, and FPT_ITT.

Appendix C – Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

At this time no selection-based requirements have been identified that are not inherited directly from the NDcPP Selection-Based requirements (e.g., FCS_HTTPS_EXT).

Appendix D – Objective Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements that specify security functionality that is desirable and these requirements are contained in this Appendix. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this EP.

At this time no objective requirements specific to WLAN AS TOEs have been identified.