PP-Module for Wireless Local Area Network (WLAN) Access System

Version: 1.0

2019-11-14

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2019-11-14	Initial Release

Contents

1 Introduction

1.1 Overview

This Protection Profile Module (PP-Module) describes security requirements for a Wireless Local Area Network (WLAN) Access System. A WLAN Access System is defined to be a device or system at the edge of a private network that establishes an encrypted IEEE 802.11 link that protects wireless data in transit from disclosure and modification. This PP-Module is intended to provide a minimal baseline set of requirements that are targeted at mitigating well-defined and described threats. This PP-Module extends the collaborative Protection Profile for Network Devices (NDcPP).

1.2 Terms

The following sections list Common Criteria and technology terms used in this document. The following sections provide both Common Criteria and technology terms used in this Protection Profile.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of theTOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in a ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Access Point (AP)	A device that provides the network interface that enables wireless client hosts to access a wired network.
Service Set Identifier (SSID)	The primary name associated with an 802.11 wireless local area network (WLAN).
Wireless Local Area Network (WLAN)	A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

This PP-Module 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 PP-Module extends the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this PP-Module in response to the threat environment discussed subsequently herein.

1.4 Use Cases

[USE CASE 1] Standalone Device

The TOE is a standalone network device that serves as a single network endpoint that provides connectivity to wireless clients.

[USE CASE 2] Distributed System

The TOE is a distributed system consisting of multiple network devices that collectively serve as the wireless network endpoint. In addition to claiming the relevant "Distributed TOE" requirement in the NDcPP, this use case also requires the TOE to claim the optional SFR FCS_CKM.2/DISTRIB to describe the key distribution method between distributed TOE components.

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module.

- Network Device cPP, version 2.1

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claims

This PP-Module does not claim conformance to any packages.

3 Security Problem Description

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

3.1 Threats

T.NETWORK_DISCLOSURE
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_ACCESS
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.TSF_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.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.REPLAY_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.

3.2 Assumptions

These assumptions are made on the Operational Environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

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

3.3 Organizational Security Policies

This PP-Module defines no additional organizational security policies beyond those specified in the NDcPP.

4 Security Objectives

4.1 Security Objectives for the TOE

O.CRYPTOGRAPHIC_FUNCTIONS
The TOE will provide means to encrypt and decrypt data to maintain confidentiality and allow for detection of modification of TSF data that is transmitted outside the TOE.

Addressed by: FCS_COP.1/DATAENCRYPTION (modified from Base-PP), FCS_IPSEC_EXT.1 (from Base-PP), FCS_TLSC_EXT.1 (from Base-PP), FCS_TLSC_EXT.2 (from Base-PP), FCS_CKM.1/WPA, FCS_CKM.2/GTK, FCS_CKM.2/PMK, FCS_CKM.2/DISTRIB (optional)

O.AUTHENTICATION
The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.

Addressed by: FCS_IPSEC_EXT.1 (from Base-PP), FCS_TLSC_EXT.1 (from Base-PP), FCS_TLSC_EXT.2 (from Base-PP), FIA_X509_EXT.1/Rev (from Base-PP), FTP_ITC.1 (modified from Base-PP), FIA_8021X_EXT.1, FIA_UAU.6, FTA_TSE.1, FCS_RADSEC_EXT.1 (selection-based), FCS_RADSEC_EXT.2 (selection-based), FIA_PSK_EXT.1 (selection-based)

O.FAIL_SECURE
Upon a self-test failure, the TOE will shut down to ensure that data cannot be passed without adhering to the TOE's security policies.

Addressed by: FPT_TST_EXT.1 (modified from Base-PP), FPT_FLS.1

O.SYSTEM_MONITORING
The TOE will provide a means to audit events specific to WLAN functionailty and security.

Addressed by: FAU_GEN.1 (modified from Base-PP)

O.TOE_ADMINISTRATION
The TOE will provide the functions necessary to address failed authentication attempts by a remote administrator.

Addressed by: FIA_AFL.1 (from Base-PP), FMT_SMR_EXT.1

4.2 Security Objectives for the Operational Environment

The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. 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 are incorporated as security objectives for the environment. The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track the assumptions about the environment.

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 the network traffic of monitored networks.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.NETWORK_DISCLOSURE	O.AUTHENTICATION, O.CRYPTOGRAPHIC_FUNCTIONS	Proper authentication of external entities ensures that network data is not disclosed to an unauthorized subject. Implementation of cryptogpraphic functions ensure that network data is not subject to unauthorized disclosure in transit.
T.NETWORK_ACCESS	O.AUTHENTICATION, O.TOE_ADMINISTRATION	Proper authentication methods ensure that subjects outside the protected network cannot access data inside the protected network until the TSF has authenticated them.

		The TOE's administration function does not permit execution of management functions that originate from wireless clients outside the protected network.
T.TSF_FAILURE	O.FAIL_SECURE, O.SYSTEM_MONITORING	The TOE responds to self-test failures that are significant enough to show a potential compromise of the TSF by making the TSF unavailable until the failure state has been cleared. The TOE generates audit records of unauthorized usage, communications outages, incorrect configuration, and other behaviors that may indicate a degraded ability to enforce its intended security functionality so that issues can be diagnosed and resolved appropriately.
T.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS	The TOE uses cryptographic functionality to enforce the integrity of protected data in transit.
T.REPLAY_ATTACK	O.AUTHENTICATION, O.CRYPTOGRAPHIC_FUNCTIONS	The TOE's use of authentication mechanisms prevent replay attacks because the source of the attack will not have the proper authentication data for the TSF to process the replayed traffic. The TOE's use of cryptographic functionality prevents impersonation attempts that use replayed traffic.
A.CONNECTIONS	OE.CONNECTIONS	The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following notations are used:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1".

5.1 NDc PP Security Functional Requirements Direction

In a PP-Configuration that includes NDc PP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDc PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDc PP in addition to what is mandated by Section 5.2 TOE Security Functional Requirements.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDc Protection Profile and relevant to the secure operation of the TOE.

5.1.1.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

5.1.1.2 Cryptographic Support (FCS)

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

FCS_COP.1.1/DATAENCRYPTION The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **CBC, CCMP** and [**selection**: *CTR*, *GCM*, ***GCMP***, ***no other***] **modes** and cryptographic key sizes **128 bits and** [**selection**: *192 bits*, *256 bits*, ***no other key sizes***] that meet the following: AES as specified in ISO 18033-3, **CBC as specified in ISO 10116, CCMP as specified in NIST SP 800-38C and IEEE 802.11-2012,** [**selection**: *CTR as specified in ISO 10116*, *GCM as specified in ISO 19772*, ***GCMP as specified in NIST SP 800-38D and IEEE 802.11ac-2013***, ***no other standards***].

Application Note: This SFR is defined in the Base-PP as FCS_COP.1/DataEncryption.

This requirement is modified from its definition in the NDcPP by mandating the selection of CBC mode and 128 bit key sizes while also defining additional AES mode and key size selections not present in the original definition.

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_EXT.1 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/DATAENCRYPTION, 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/WPA. 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.

CTR mode is not used for WLAN AS capabilities but remains selectable since it may be required by another part of the TSF.

Evaluation Activity

TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
In addition to the tests required by theNDcPP, the evaluator shall perform the following testing:

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.

5.1.1.3 Protection of the TSF (FPT)

FPT_TST_EXT.1 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 authorised user*, *at the conditions [**assignment**: conditions under which self-tests should occur]*, ***in no other circumstances***] to demonstrate the correct operation of theTSF: **integrity verification 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/SigGen, [selection: *[assignment: list of additional self-tests run by the TSF]*, *no other self-tests*].

Application Note: This SFR is modified from its definition in the NDcPP by mandating that self-testing occur at power on, and that the self-testing must include, at minimum, an integrity test using a digital signature. FCS_COP.1/SigGen is defined in the NDcPP.

Evaluation Activity

The evaluator shall perform the following activities in addition to those required by the NDcPP:

TSS
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.

The evaluator shall also ensure that the TSS or operational guidance describes the actions that take place for successful and unsuccessful exection of the integrity test.

Guidance
The evaluator shall ensure that the TSS or operational guidance describes the actions that take place for successful and unsuccessful exection of the integrity test.

Tests
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).*

5.1.1.4 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using **IEEE 802.11-2012 (WPA2), IEEE 802.1X, [selection: *IPsec*, *RADIUS over TLS*], and** [**selection**: *SSH*, *TLS*, *DTLS*, *HTTPS*, ***no other protocols***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **WLAN client, 802.1x authentication server,** audit server, [**selection**: *authentication server*, ***[assignment**: other capabilities]*, *no 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: This requirement has been modified from its definition in the NDcPP to mandate the communications protocols and environmental components that a WLAN Access System must use. IEEE 802.11-2012 (WPA2) with IEEE 802.1X is required for communications with wireless clients; IPsec or RADIUS over TLS (commonly known as "RadSec") is required at least for communications with the 802.1X authentication server. Other selections may be made if needed by other parts of the TSF. The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage.

The IT entity of "802.1X authentication server" is distinct from "authentication server" because the latter may be used for administrator authentication rather than authorization of WLAN clients.

If "IPsec" is selected in FTP_ITC.1.1, then FCS_IPSEC_EXT.1 from the NDcPP must be claimed. If RADIUS over TLS is selected in FTP_ITC.1.1, then FCS_RADSEC_EXT.1 in this PP-Module must be claimed, as well as FCS_TLSC_EXT.1 from the NDcPP.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**assignment**: *list of services for which the TSF is able to initiate communications*].

Evaluation Activity

The evaluator shall perform the following activities in addition to those required by the NDcPP:

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.

Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator 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 evaluator 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).*

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Cryptographic Support (FCS)

FCS_CKM.1/WPA Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)

FCS_CKM.1.1/WPA The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRF-384 and [**selection**: PRF-704, no other algorithm]*] and specified 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 PP-Module) 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 PP-Module, the HMAC function as specified in this PP-Module, as well as other information. This is specified in IEEE 802.11-2012 primarily in chapter 11. FCS_RBG_EXT.1 is defined in the NDcPP.

Evaluation Activity

TSS
The cryptographic primitives will be verified through evaluation activities specified elsewhere in this PP-Module. The evaluator shall verify that the TSS describes how the primitives defined and implemented by this PP-Module 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.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall 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.

Additionally, the evaluator shall test the PRF function using the test vectors from:

- *Section 2.4 "The PRF Function – PRF(key, prefix, data, length)" of the IEEE 802.11-02/362r6 document "Proposed Test vectors for IEEE 802.11 TGi" dated September 10, 2002, and*
- *Annex M.3 "PRF reference implementation and test vectors" of IEEE 802.11-2012.*

FCS_CKM.2/GTK Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/GTK The TSF shall distribute **Group Temporal Key (GTK)** in accordance with a specified cryptographic key distribution method: [**selection**: *AES Key Wrap in an EAPOL-Key frame*, *AES Key Wrap with Padding 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 is 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.

Evaluation Activity

TSS

The evaluator shall check the TSS to ensure that it describes how theGTK is wrapped prior to being distributed using the AES implementation specified in thisPP-Module, and also how the GTKs are distributed when multiple clients connect to the TOE.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall 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 evaluation activity for FCS_CKM.1/PMK.

To fully test the broadcast/multicast functionality, these steps shall be performed as the evaluator connects multiple clients to the TOE.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.

The evaluator shall also perform the following testing based on the supported GTK distribution method(s):

AES Key Wrap (AES-KW Tests)

- ***Test 1:** The evaluator shall test the authenticated encryption functionality ofAES-KW for EACH combination of the following input parameter lengths:*

  128 and 256 bit key encryption keys (KEKs)

  Three plaintext lengths. One of the plaintext lengths shall be two semi-blocks (128 bits). One of the plaintext lengths shall be three semi-blocks (192 bits). The third data unit length shall be the longest supported plaintext length less than or equal to 64 semi-blocks (4096 bits).

  using a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KW authenticated encryption. To determine correctness, the evaluator shall use the AES-KW authenticated-encryption function of a known good implementation.
- ***Test 2:** The evaluator shall test the authenticated-decryption functionality ofAES-KW using the same test as for authenticated-encryption, replacing plaintext values with ciphertext values and AES-KW authenticated-encryption withAES-KW authenticated-decryption. Additionally, the evaluator shall modify one byte of the ciphertext, attempt to decrypt the modified ciphertext, and ensure that a failure is returned rather than plaintext.*

AES Key Wrap with Padding (AES-KWP Tests)

- ***Test 1:** The evaluator shall test the authenticated-encryption functionality ofAES-KWP for EACH combination of the following input parameter lengths:*

  128 and 256 bit key encryption keys (KEKs)

  Three plaintext lengths. One plaintext length shall be one octet. One plaintext length shall be 20 octets (160 bits). One plaintext length shall be the longest

supported plaintext length less than or equal to 512 octets (4096 bits).

using a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KWP authenticated encryption. To determine correctness, the evaluator shall use the AES-KWP authenticated-encryption function of a known good implementation.

- ***Test 2:*** *The evaluator shall test the authenticated-decryption functionality of AES-KWP using the same test as for AES-KWP authenticated-encryption, replacing plaintext values with ciphertext values and AES-KWP authenticated-encryption with AES-KWP authenticated-decryption. Additionally, the evaluator shall modify one byte of the ciphertext, attempt to decrypt the modified ciphertext, and ensure that a failure is returned rather than plaintext.*

FCS_CKM.2/PMK Cryptographic Key Distribution (PMK)

FCS_CKM.2.1/PMK 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 PP-Module 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 a protected connection, the transfer of the PMK will be protected.

Evaluation 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 TOE.

Guidance
There are no guidance evaluation activities for this component.

Tests
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.

5.2.2 Identification and Authentication (FIA)

FIA_8021X_EXT.1 802.1X 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 protected either by IPsec or RadSec (TLS) 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 PP-Module. 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.

Evaluation 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 or RadSec (TLS) tunnel, 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.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following tests:

- ***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 demonstrates the enforcement of FIA_8021X_EXT.1.3.*

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 session locking, [**assignment**: other conditions], no other conditions]*].

Evaluation Activity

TSS
There are no TSS evaluation activities for this component.

Guidance
There are no guidance evaluation activities for this component.

Tests
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.

If other re-authentication conditions are specified, the evaluator shall cause those conditions to occur and verify that the TSF re-authenticates the authenticated user.

5.2.3 Security Management (FMT)

FMT_SMR_EXT.1 No Administration from Client

FMT_SMR_EXT.1.1 The TSF shall ensure that the ability to remotely administer theTOE from a wireless client shall be disabled by default.

Evaluation Activity

TSS
There are no TSS evaluation activities for this component.

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. The evaluator shall confirm that the TOE does not permit remote administration from a wireless client by default.

Tests
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.

5.2.4 Protection of the TSF (FPT)

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 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 occur.

Evaluation Activity

TSS
The evaluator shall examine the TSS to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall examine the TSS to ensure that it describes all failure conditions and how a secure state is preserved if any of these failures occur. The evaluator shall ensure that the definition of a secure state is suitable to ensure the continued protection of any key material and user data.

Guidance
The evaluator shall examine the operational guidance to verify that it describes applicable recovery instructions for each TSF failure state.

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

5.2.5 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny establishment **of a wireless client session** based on [*TOE interface, time, day, [**selection**: [**assignment**: other attributes], no other attributes]*].

Application Note: The "TOE interface" can be specified in terms of the device in theTOE 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.

Evaluation 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

Guidance

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

Tests

For each supported attribute, the evaluator shall perform the following test:

- ***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.*

6 Consistency Rationale

6.1 Network Device Protection Profile

6.1.1 Consistency of TOE Type

When this PP-Module extends the Network Device cPP, the TOE type for the overall TOE is still a network device. This PP-Module just defines the TOE as a specific type of network device with functional capabilities distinct to that type.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDc PP as follows:

PP-Module Threat	Consistency Rationale
T.NETWORK_DISCLOSURE	This threat extends the security problem defined by the Base-PP to include the threat of a malicious entity in an untrusted network interacting with a protected entity in a trusted network. This is not addressed in the Base-PP because not all network devices are responsible for facilitating communications between separate networks. This threat is also consistent with the T.UNTRUSTED_COMMUNICATION_CHANNELS threat defined by the Base-PP because compromise of data in transit is one potential way this threat may be exploited.
T.NETWORK_ACCESS	This threat extends the security problem defined by the Base-PP to include the threat of a malicious entity in an untrusted network interacting with a protected entity in a trusted network. This is not addressed in the Base-PP because not all network devices are responsible for facilitating communications between separate networks.
T.TSF_FAILURE	This threat is an extension of the T.SECURITY_FUNCTIONALITY_FAILURE threat defined by the Base-PP.
T.DATA_INTEGRITY	This threat is a specific type of failure that may result from successful exploitation of the T.WEAK_CRYPTOGRAPHY threat defined by the Base-PP. It is an extension of the Base-PP threat for communications that are specific to this PP-Module.
T.REPLAY_ATTACK	This threat is a specific type of failure that may result from successful exploitation of the T.UNAUTHORIZED_ADMINISTRATOR_ACCESS and T.UNTRUSTED_COMMUNICATIONS_CHANNELS threats defined by the Base-PP. It is an extension of the Base-PP threat for communications that are specific to this PP-Module.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the NDc PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.CRYPTOGRAPHIC_FUNCTIONS	The Base-PP does not define TOE objectives but it does define requirements for cryptographic functions. This objective is consistent with the functional behavior required by the Base-PP.
O.AUTHENTICATION	The Base-PP does not define TOE objectives but it does define requirements for authentication of both users and remote entities. This objective is consistent with the functional behavior required by the Base-PP.
O.FAIL_SECURE	The Base-PP does not define TOE objectives but it does define requirements for self-testing. This PP-Module is consistent with that by defining an objective to enter a secure state if a self-test does fail.
O.SYSTEM_MONITORING	The Base-PP does not define TOE objectives but it does define requirements for auditing. This PP-Module is consistent with that by ensuring that auditable events are appropriately defined for the WLAN AS capability.
O.TOE_ADMINISTRATION	The Base-PP does not define TOE objectives but it does define requirements for management. This PP-Module is consistent with that by applying security restrictions on how the TOE's management interface can be invoked.

The objectives for the TOE's Operational Environment are consistent with the NDcPP based on the following rationale:

PP-Module Operational Environment	Consistency Rationale

Objective	
OE.CONNECTIONS	The Base-PP does not define where in a particular network architecture a network device must be deployed since it is designed to be generic to various types of network devices. This PP-Module defines the expected architectural deployment specifically for WLAN AS network devices.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDc PP that are needed to support Wireless Local Area Network (WLAN) Access System functionality. This is considered to be consistent because the functionality provided by the NDc is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDc PP as well as new SFRs that are used entirely to provide functionality for Wireless Local Area Network (WLAN) Access System. The rationale for why this does not conflict with the claims defined by the NDc PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_GEN.1	This PP-Module modifies the Base-PP's definition of theSFR by defining additional auditable events for behavior described by this PP-Module. All auditable events required by the Base-PP are still required.
FCS_COP.1/DATAENCRYPTION	This PP-Module modifies the Base-PP's definition of theSFR by adding additional AES modes consistent with the standards referenced in the Base-PP, and by mandating specific selections that are relevant to the technology type of the PP-Module.
FPT_TST_EXT.1	This PP-Module modifies the Base-PP's definition of theSFR by defining a minimum baseline for what self-tests must be run. Additional self-tests may still be specified by the ST author.
FTP_ITC.1	This PP-Module modifies the Base-PP's definition of theSFR by specifying a minimum baseline of required communications protocols and also includes additional protocols not originally defined by the Base-PP. The original protocols specified in the Base-PP may still be selected by the ST author.
Mandatory SFRs	
FCS_CKM.1/WPA	This SFR defines additional cryptographic functionality not defined in the Base-PP but it implements this using the DRBG mechanism already defined in the Base-PP.
FCS_CKM.2/GTK	This SFR defines additional cryptographic functionality not defined in the Base-PP that is used for functionality outside the original scope of the Base-PP.
FCS_CKM.2/PMK	This SFR defines additional cryptographic functionality not defined in the Base-PP that is used for functionality outside the original scope of the Base-PP.
FIA_8021X_EXT.1	This SFR defines support for 802.1X communications, which is a logical interface that extends the scope of what the Base-PP originally defined.
FIA_UAU.6	This SFR defines support for re-authentication of wireless users, which are a type of subject beyond the scope of what the Base-PP originally defined.
FMT_SMR_EXT.1	This SFR applies restrictions on when the execution of management functions is authorized. It does not prevent proper administration of the TSF.
FPT_FLS.1	This SFR extends the functionality described byFPT_TST_EXT.1 in the Base-PP by defining the specific TSF reaction in the event of a failed self-test.
FTA_TSE.1	This SFR applies restrictions on establishment of wireless communications, which is a logical interface that extends the scope of what the Base-PP originally defined.
Optional SFRs	
FCS_CKM.2/DISTRIB	This SFR defines an additional use for the cryptographic and self-protection mechanisms defined in the Base-PP.
Selection-based SFRs	
FCS_RADSEC_EXT.1	ThiS SFR defines the implementation of RadSec and the peer authentication method that it uses. This relies on the TLS requirements defined by the Base-PP and may also use the X.509 certificate validation methods specified in the Base-PP, depending on the selected peer authentication method.
FCS_RADSEC_EXT.2	This SFR defines the implementation of RadSec when pre-shared key authentication is

	used. This functionality is outside the original scope of the Base-PP but it relies on the TLS client protocol implementation, cryptographic algorithms, and random bit generation functions defined by the Base-PP.
FIA_PSK_EXT.1	This SFR defines parameters for pre-shared key generation. The Base-PP supports pre-shared keys as a potential authentication method for IPsec. This PP-Module does not prevent this from being used but does define restrictions on how pre-shared keys may be generated and what constitutes an acceptable key. This may also be used for RadSec, which is outside the original scope of the Base-PP.
Objective SFRs	
This PP-Module does not define any objective requirements.	

Appendix A - Optional SFRs

FCS_CKM.2/DISTRIB Cryptographic Key Distribution (802.11 keys)

FCS_CKM.2.1/DISTRIB The TSF shall distribute **the IEEE 802.11** keys in accordance with a specified key distribution method: [*trusted channel protocol specified in FPT_ITT.1*] that meets the following: [*standards specified in the various iterations of FCS_COP.1*] **and does not expose the cryptographic keys**.

Application Note: This requirement is only applicable when theTOE is distributed (i.e., FPT_ITT.1 from the NDcPP is claimed).

This requirement applies to any key necessary for successful IEEE 802.11 connections not covered by FCS_CKM.2/GTK. 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.

FCS_COP.1 and FPT_ITT.1 are defined in the NDcPP.

Evaluation 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 function is dependent on TOE configuration, the evaluator shall confirm that the operational guidance contains instructions for how to configure that the keys are adequately protected.

Tests
This requirement will be tested in conjunction with the tests for the cryptographic primitives, the secure protocols, and FPT_ITT.1.

Appendix B - Selection-based SFRs

FCS_RADSEC_EXT.1 RadSec

FCS_RADSEC_EXT.1.1 The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

FCS_RADSEC_EXT.1.2 The TSF shall perform peer authentication using [**selection**: *X.509v3 certificates*, *pre-shared keys*].

Application Note: This SFR is applicable if "RADIUS over TLS" is selected in FTP_ITC.1.1.

If "X.509v3 certificates" is selected in FCS_RADSEC_EXT.1.2, then FCS_TLSC_EXT.2 from the NDcPP must be claimed. If "pre-shared keys" is selected in FCS_RADSEC_EXT.1.2, then FCS_RADSEC_EXT.2 in this PP-Module must be claimed.

Evaluation Activity

TSS
The evaluator shall verify that the TSS description includes the use of RADIUS over TLS, as described in RFC 6614.

If X.509v3 certificates is selected, the evaluator shall ensure that the TSS description includes the use of client-side certificates for TLS mutual authentication.

Guidance
The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the guidance.

Tests
The evaluator shall demonstrate the ability to successfully establish a RADIUS overTLS connection with a RADIUS server. This test shall be performed with X.509v3 certificates if selected and performed with pre-shared keys if selected.

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

FCS_RADSEC_EXT.2.1 The TSF shall implement [**selection**: *TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation shall support the following cipher suites for use when acting as a RADIUS over TLS client: [**selection**:

- *TLS_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_DHE_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_DHE_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_RSA_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_RSA_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_PSK_WITH_AES_256_GCM_SHA384*,
- *TLS_DHE_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_DHE_PSK_WITH_AES_256_GCM_SHA384*,
- *TLS_RSA_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_RSA_PSK_WITH_AES_256_GCM_SHA384*

].

Application Note: The above cipher suites are only for use when the TSF is acting as a RADIUS over TLS client, not for other uses of the TLS protocol. The cipher suites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the cipher suites that are supported. If "X.509v3 certificates" is selected in FCS_RADSEC_EXT.1.2, the cipher suites selected in (and tested by) FCS_TLSC_EXT.2.1 are also supported for RADIUS over TLS client use.

FCS_RADSEC_EXT.2.2 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.

FCS_RADSEC_EXT.2.3 If cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, the TSF shall, when any are used for a RADIUS overTLS connection, verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

Application Note: The rules for verification of identity are described in Section 6 of RFC 6125. The reference identifier is typically established by configuration (e.g. configuring the name of the authentication server). Based on a singular reference identifier's source domain and application service type (e.g. HTTP, SIP, LDAP), the client establishes all reference

identifiers which are acceptable, such as a Common Name for the Subject Name field of the certificate and a (case-insensitive) DNS name for the Subject Alternative Name field. The client then compares this list of all acceptable reference identifiers to the presented identifiers in the TLS server's certificate.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name is required for the purposes of backwards compatibility. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented. Finally, support for wildcards is discouraged but may be implemented. If the client supports wildcards, the client must follow the best practices regarding matching; these best practices are captured in the evaluation activity.

If no cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, then this requirement is satisfied by default.

FCS_RADSEC_EXT.2.4 If cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, the TSF shall, when any are used for a RADIUS overTLS connection, only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [**selection**: *not establish the connection*, *request authorization to establish the connection*, *[**assignment**: other action]*].

Application Note: This SFR must be claimed if "pre-shared keys" is selected in FCS_RADSEC_EXT.1.2.

Validity is determined by the identifier verification, certificate path, the expiration date, and the revocation status in accordance with RFC 5280. Certificate validity is tested in accordance with testing performed for FIA_X509_EXT.1/Rev in the NDcPP.

If no cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, then this requirement is satisfied by default.

Evaluation Activity

TSS
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified are identical to those listed for this component. The evaluator shall also verify that the TSS contains a description of the denial of old SSL and TLS versions.

The evaluator shall 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.

The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported (e.g., Common Name, DNS Name, URI Name, Service Name, or other application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator shall ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the TOE.

Guidance
The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the guidance.

The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that RADIUS over TLS conforms to the description in the TSS (for instance, the set of cipher suites advertised by the TOE may have to be restricted to meet the requirements).

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

The evaluator shall verify that the operational guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.

Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall establish a RADIUS over TLS connection using each of the cipher suites selected in FCS_RADSEC_EXT.2.1. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).*
- ***Test 2:*** *The evaluator shall set the pre-shared key to a value that does not match*

the server's pre-shared key and demonstrate that the TOE cannot successfully complete a protocol negotiation using this key.

- ***Test 3:*** *The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.*
- ***Test 4:*** *The evaluator shall perform the following modifications to the traffic:*
  - *Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection.*
  - *Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE cipher suite) or that the server denies the client's Finished handshake message.*
  - *Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.*
  - *Modify a byte in the Server Finished handshake message, and verify that the client rejects the connection and does not send any application data.*
  - *Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the client denies the connection.*
- ***Test 5:*** *[conditional] If any of the TLS_RSA_PSK cipher suites are selected:*
  - *The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.*
  - *The evaluator shall present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator shall verify that the connection fails.*
  - *The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type.*
  - *The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds.*
  - *If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.*
  - *If wildcards are supported by the TOE, the evaluator shall perform the following tests:*
    - *The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.*
    - *The evaluator shall present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com). The evaluator shall verify that the connection succeeds. The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.*
    - *The evaluator shall present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.*
  - *If wildcards are not supported by the TOE, the evaluator shall present a server certificate containing a wildcard and verify that the connection fails.*
  - *[conditional] If URI or Service name reference identifiers are supported, the evaluator shall configure the DNS name and the service identifier. The*

evaluator shall present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator shall repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.

- ***Test 6:*** *[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 7:*** *[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.*

FIA_PSK_EXT.1 Pre-Shared Key Composition

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

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: This requirement must be included if IPsec or another protocol that uses pre-shared keys is claimed, and pre-shared key authentication is selected (i.e. "Pre-shared Keys" is selected in FCS_IPSEC_EXT.1.13 or "pre-shared keys" is selected in FCS_RADSEC_EXT.1.2). In the second 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.

Evaluation 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 preshared 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 superset 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).

Tests

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.*

Appendix C - Objective SFRs

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

This PP-Module does not define any objective SFRs.

Appendix D - Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

D.1 Background and Scope

This appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Functional Class	Functional Components
Identification and Authentication (FIA)	FIA_8021X_EXT Cryptographic Key Management
Security Management (FMT)	FMT_SMR_EXT Security Management Restrictions
Cryptographic Support (FCS)	FCS_RADSEC_EXT RadSec
Identification and Authentication (FIA)	FIA_PSK_EXT Pre-Shared Key Composition

D.2 Extended Component Definitions

FIA_8021X_EXT Cryptographic Key Management

Family Behavior

Components in this family describe requirements for implementation of 802.1X port-based network access control.

Component Leveling

FIA_8021X_EXT.1, 802.1X Port Access Entity (Authenticator) Authentication, requires the TSF to securely implement IEEE 802.1X as an authenticator.

Management: FIA_8021X_EXT.1

No specific management functions are identified.

Audit: FIA_8021X_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Attempts to access the 802.1X controlled port prior to succesul completion of the authentication exchange.

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

Hierarchical to: No other components.

Dependencies to: No dependencies

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.

FMT_SMR_EXT Security Management Restrictions

Family Behavior

Components in this family describe architectural restrictions on security administration that are not defined in CC Part 2.

Component Leveling

FMT_SMR_EXT.1, No Administration from Client, requires the TSF to reject remote administration from a wireless client by default.

Management: FMT_SMR_EXT.1

No specific management functions are identified.

Audit: FMT_SMR_EXT.1

There are no auditable events foreseen.

FMT_SMR_EXT.1 No Administration from Client

Hierarchical to: No other components.

Dependencies to: FMT_SMF.1 Specification of Management Functions

FMT_SMR_EXT.1.1

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

FCS_RADSEC_EXT RadSec

Family Behavior

Components in this family describe requirements for implementation of the RadSec (RADIUS overTLS) protocol.

Component Leveling

FCS_RADSEC_EXT.1, RadSec, requires the TSF to implement RadSec using a specified peer authentication method.

Management: FCS_RADSEC_EXT.1

No specific management functions are identified.

Audit: FCS_RADSEC_EXT.1

There are no auditable events foreseen.

FCS_RADSEC_EXT.1 RadSec

Hierarchical to: No other components.

Dependencies to: FCS_TLSC_EXT.1 TLS Client Protocol

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_X509_EXT.1 X.509 Certificate Validation

FCS_RADSEC_EXT.1.1

The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

FCS_RADSEC_EXT.1.2

The TSF shall perform peer authentication using [**selection**: *X.509v3 certificates*, *pre-shared keys*].

Component Leveling

FCS_RADSEC_EXT.2, RadSec using Pre-Shared Keys, requires the TSF to implement RadSec using pre-shared key authentication in a manner that conforms to relevant TLS specifications.

Management: FCS_RADSEC_EXT.2

No specific management functions are identified.

Audit: FCS_RADSEC_EXT.2

There are no auditable events foreseen.

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

Hierarchical to: No other components.

Dependencies to: FCS_CKM.1 Cryptographic Key Generation

FCS_COP.1 Cryptographic Operation

FCS_RADSEC_EXT.1 RadSec

FCS_RBG_EXT.1 Random Bit Generation

FCS_RADSEC_EXT.2.1

The TSF shall implement [**selection**: *TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation shall support the following cipher suites for use when acting as a RADIUS over TLS client: [**selection**:

- *TLS_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_DHE_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_DHE_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_RSA_PSK_WITH_AES_128_CBC_SHA*,
- *TLS_RSA_PSK_WITH_AES_256_CBC_SHA*,
- *TLS_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_PSK_WITH_AES_256_GCM_SHA384*,
- *TLS_DHE_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_DHE_PSK_WITH_AES_256_GCM_SHA384*,
- *TLS_RSA_PSK_WITH_AES_128_GCM_SHA256*,
- *TLS_RSA_PSK_WITH_AES_256_GCM_SHA384*

].

FCS_RADSEC_EXT.2.2

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.

FCS_RADSEC_EXT.2.3

If cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, the TSF shall, when any are used for a RADIUS over TLS connection, verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_RADSEC_EXT.2.4

If cipher suites beginning with TLS_RSA_PSK are selected in FCS_RADSEC_EXT.2.1, the TSF shall, when any are used for a RADIUS over TLS connection, only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [**selection**: *not establish the connection*, *request authorization to establish the connection*, *[**assignment**: other action]*].

FIA_PSK_EXT Pre-Shared Key Composition

Family Behavior

Components in this family describe requirements for the creation and composition of pre-shared keys used to establish trusted communications channels.

Component Leveling

FIA_PSK_EXT.1, Pre-Shared Key Composition, requires the TSF to support pre-shared keys that meet various characteristics for specific communications usage.

Management: FIA_PSK_EXT.1

No specific management functions are identified.

Audit: FIA_PSK_EXT.1

There are no auditable events foreseen.

FIA_PSK_EXT.1 Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies to: FCS_RBG_EXT.1 Random Bit Generation

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for [**selection**: *RADIUS over TLS (RadSec)*, *IPsec*] and [**selection**: *IEEE 802.11 WPA2-PSK*, *[**assignment**: other protocols that use pre-shared keys]*, *no other protocols*].

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.

Appendix E - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.
[NDc PP]	collaborative Protection Profile for Network Devices, Version 2.1, March 2019
[SD]	Supporting Document Mandatory Technical Document, PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, November 2019

Appendix F - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AP	Access Point
AS	Access System
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter Mode with CBC-MAC
CCMP	CCM mode Protocol
CEM	Common Evaluation Methodology
CTR	Counter (encryption mode)
EAP	Extensible Authentication Protocol
GCM	Galois-Counter Mode
GTK	Group Temporal Key
IPsec	Internet Protocol Security
MAC	Media Access Control or Message Authentication Code
NDcPP	Network Device collaborative Protection Profile
PAE	Port Access Entity
PMK	Pairwise Master Key
PP	Protection Profile
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSID	Service Set Identifier
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access