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

Version: 1.0
2022-03-31
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-03-31	Initial Release
0.5	2022-01-20	Conversion to Protection Profile Module (PP-Module); Updated to include Wi-Fi Protected Access (WPA) 3 and Wi-Fi 6. WPA 3 is required. WPA 2 can additionally be included in the Security Target (ST). 256 bit keys are required. 128 and 192 bit keys can additionally be included in the ST. Mandated Distributed Target of Evaluation (TOE)

Contents

1 Introduction
1.1 Overview
1.2 Terms
1.2.1 Common Criteria Terms
1.2.2 Technical Terms
1.3 Compliant Targets of Evaluation
1.3.1 TOE Boundary
1.4 Use Cases
2 Conformance Claims
3 Security Problem Description
3.1 Threats
3.2 Assumptions
3.3 Organizational Security Policies
4 Security Objectives
4.1 Security Objectives for the TOE
4.2 Security Objectives for the Operational Environment
4.3 Security Objectives Rationale
5 Security Requirements
5.1 NDcPP Security Functional Requirements Direction
5.1.1 Modified SFRs
5.1.1.1 Security Audit (FAU)
5.1.1.2 Communication (FCO)
5.1.1.3 Cryptographic Support (FCS)
5.1.1.4 Protection of the TSF (FPT)
5.1.1.5 Trusted Path/Channels (FTP)
5.2 TOE Security Functional Requirements
5.2.1 Security Audit (FAU)
5.2.2 Cryptographic Support (FCS)
5.2.3 Identification and Authentication (FIA)
5.2.4 Security Management (FMT)
5.2.5 Protection of the TSF (FPT)
5.2.6 TOE Access (FTA)
5.2.7 Trusted Path/Channels (FTP)
5.3 TOE Security Functional Requirements Rationale
5.4 TOE Security Assurance Requirements
6 Consistency Rationale
6.1 Collaborative Protection Profile for NDs
6.1.1 Consistency of TOE Type
6.1.2 Consistency of Security Problem Definition
6.1.3 Consistency of Objectives
6.1.4 Consistency of Requirements
Appendix A - Optional SFRs
A.1 Strictly Optional Requirements
A.1.1 Cryptographic Support (FCS)
A.2 Objective Requirements
A.3 Implementation-dependent Requirements
Appendix B - Selection-based Requirements
B.1 Cryptographic Support (FCS)
B.2 Identification and Authentication (FIA)
Appendix C - Extended Component Definitions
C.1 Extended Components Table
C.2 Extended Component Definitions
C.2.1 Identification and Authentication (FIA)
C.2.1.1 FIA_8021X_EXT 802.1X Port Access Entity (Authenticator) Authentication
C.2.1.2 FIA_PSK_EXT Pre-Shared Key Composition
C.2.2 Security Management (FMT)

C.2.2.1 FMT_SMR_EXT Security Management Restrictions
C.2.3 Cryptographic Support (FCS)
C.2.3.1 FCS_RADSEC_EXT RadSec
Appendix D - Implicitly Satisfied Requirements
Appendix E - Allocation of Requirements in Distributed TOEs
Appendix F - Entropy Documentation and Assessment
Appendix G - Acronyms
Appendix H - Bibliography

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of a Wireless Local Area Network (WLAN) Access System (AS) in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base Protection Profile (Base-PP):

- Network Device collaborative Protection Profile (NDcPP) Version 2.2e

This Base-PP is valid because a WLAN AS is a device 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. A network device typically implements this functionality.

A TOE that conforms to a Protection Profile Configuration (PP-Configuration) containing this PP-Module must be a 'Distributed TOE' as defined in the NDcPP. The expectation for this PP-Module is that a WLAN AS must include a controller and one or more access points (APs).

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
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 (OE)	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 (PP-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-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security	A requirement for security enforcement by the TOE.

Functional Requirement (SFR)	
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
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 an ST.

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 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) ASes. A compliant WLAN AS 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 AS 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] 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 Security Functional Requirement (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 Common Criteria (CC) and Common Evaluation Methodology (CEM) addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

No Protection Profiles (PPs) or PP-Modules may be specified in a PP-Configuration with this PP-Module other than the Base-PP specified in Section 1.1 Overview.

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 AS. 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 AS is used to establish secure communications. The WLAN AS provides one end of the secure cryptographic tunnel and performs encryption and decryption of network packets in accordance with a WLAN AS 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 AS 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 (OE). Together the threats of the NDcPP and those defined in this PP-Module define the comprehensive set of security threats addressed by a WLAN AS 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 or 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 be only 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 TOE Security Functionality (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 OE 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 OE that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality. All assumptions for the OE of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

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

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

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.

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 shut down to ensure that data cannot be passed without adhering to the TOE's security policies.

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 failed authentication attempts by a remote administrator.

4.2 Security Objectives for the Operational Environment

All objectives for the OE of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

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 organizational security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.NETWORK_DISCLOSURE	O.AUTHENTICATION	The threat T.NETWORK_DISCLOSURE is countered by O.AUTHENTICATION as proper authentication of external entities ensures that network data is not disclosed to an unauthorized subject.
	O.CRYPTOGRAPHIC_FUNCTIONS	The threat T.NETWORK_DISCLOSURE is countered by O.CRYPTOGRAPHIC_FUNCTIONS as implementation of cryptographic functions ensures that network data is not subject to unauthorized disclosure in transit.
T.NETWORK_ACCESS	O.AUTHENTICATION	The threat T.NETWORK_ACCESS is countered by O.AUTHENTICATION as proper authentication methods ensure that subjects outside the protected network cannot access data inside the protected network until the TSF has authenticated them.
	O.TOE_ADMINISTRATION	The threat T.NETWORK_DISCLOSURE is countered by O.TOE_ADMINISTRATION as 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	The threat T.TSF_FAILURE is countered by O.FAIL_SECURE as 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.
	O.SYSTEM_MONITORING	The threat T.TSF_FAILURE is countered by O.SYSTEM_MONITORING as 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 threat T.DATA_INTEGRITY is countered by O.CRYPTOGRAPHIC_FUNCTIONS as the TOE uses cryptographic functionality to enforce the integrity of protected data in transit.
T.REPLAY_ATTACK	O.AUTHENTICATION	The threat T.REPLAY_ATTACK is countered by O.AUTHENTICATION as 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.
	O.CRYPTOGRAPHIC_FUNCTIONS	The threat T.REPLAY_ATTACK is countered by O.CRYPTOGRAPHIC_FUNCTIONS as the TOE's use of cryptographic functionality prevents impersonation attempts that use replayed traffic.
A.CONNECTIONS	OE.CONNECTIONS	The OE 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 conventions are used for the completion of operations:

- **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 NDcPP Security Functional Requirements Direction

In a PP-Configuration that includes NDcPP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDcPP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDcPP 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 NDcPP and relevant to the secure operation of the TOE.

5.1.1.1 Security Audit (FAU)

FAU_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1.1

This is specified as a selection-based SFR in the Base-PP but is mandatory for any TOE that claims conformance to this PP-Module because a conformant TOE will always be distributed. Therefore, it will always be required for each TOE component to generate its own audit records.

Evaluation Activities

FAU_GEN_EXT.1
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

FAU_STG_EXT.1 Protected Audit Event Storage

Application Note: This SFR is modified to restrict selections in FAU_STG_EXT.1.2 to a subset of the available options to account for the TOE being distributed.

FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition [**selection**: *The TOE shall be a distributed TOE that stores audit data on the following TOE components: [**assignment**: identification of TOE components], The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [**assignment**: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data]*].

FAU_STG_EXT.1.3

The TSF shall [**selection**: *drop new audit data, overwrite previous audit records according to the following rule: [**assignment**: rule for overwriting previous audit records], [**assignment**: other action]*] when the local storage space for audit data is full.

Evaluation Activities

FAU_STG_EXT.1
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to restricts selections in FAU_STG_EXT.1.2 to a subset of the available options to account for the TOE being distributed.

FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1

This is specified as a selection-based SFR in the Base-PP but is mandatory for any TOE that claims conformance to this PP-Module because a conformant TOE will always be distributed. Therefore, it will always be required for each TOE component to appropriately protect its own audit records.

Evaluation Activities

FAU_STG_EXT.4
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

5.1.1.2 Communication (FCO)

FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1

This is specified as a selection-based SFR in the Base-PP but is mandatory for any TOE that claims conformance to this PP-Module because a conformant TOE will always be distributed. Therefore, it will always be required for a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2

This is specified as a selection-based SFR in the Base-PP but is mandatory for any TOE that claims conformance to this PP-Module because a conformant TOE will always be distributed. Therefore, it will always be required that each component establish and use a communications channel that uses a secure channel requirement or no channel.

Evaluation Activities

FCO_CPC_EXT.1
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

5.1.1.3 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 Advanced Encryption Standard (AES) used in **Cipher Block Chaining (CBC), CCM mode Protocol (CCMP),** and [**selection**: *Counter (encryption mode) (CTR)*, *Galois-Counter Mode (GCM)*, ***GCMP***, ***no other***] **modes** and cryptographic key sizes **256 bits and** [**selection**: *128 bits*, *192 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 802.11-2020,** [**selection**: *CTR as specified in ISO 10116*, *GCM as specified in ISO 19772*, ***GCMP as specified in NIST SP 800-38D and IEEE 802.11ax-2021***, ***no other standards***].

Application Note: This requirement is modified from its definition in the NDcPP by mandating the selection of CBC mode and 256 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 a key size of 256 bits being implemented. It is not expected that these modes will both be used for all encryption and 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 802.11-2020, AES-CCMP (which uses AES in Counter Mode with CBC-Message Authentication Code (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. 256-bit CCMP is required in order to comply with FCS_CKM.1/WPA. Note that optionally AES-CCMP-192, AES-CCMP-128, AES-GCMP-192, and AES-GCMP-128 with cryptographic key size of 256 bits, may be implemented for IEEE 802.11ax-2021 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 Activities

FCS_COP.1/DataEncryption
TOE Summary Specification (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 the NDcPP, the evaluator will perform the following testing:
AES-CCM Tests

The evaluator will 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 will be the shortest supported payload length, greater than or equal to zero bytes. The other payload length will 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 will be 0, if supported. One associated data length will be the shortest supported payload length, greater than or equal to zero bytes. One associated data length will 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 will be tested.*

***Nonce lengths**. All supported nonce lengths between 7 and 13 bytes, inclusive, will be tested.*

***Tag lengths**. All supported tag lengths of 4, 6, 8, 10, 12, 14, and 16 bytes will 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 will ensure that these are the only supported lengths. To test the generation-encryption functionality of AES-CCM, the evaluator will 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 will 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 will 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 will 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 will 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 will 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 will 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 will supply 10 tuples that should fail and 5 that should pass per set of 15.

Additionally, the evaluator will 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 verify further the IEEE 802.11-2020 implementation of AES-CCMP.

5.1.1.4 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 authorized user, at the conditions [**assignment**: conditions under which self-tests should occur], **in no other circumstances***] to demonstrate the correct operation of the TSF: **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 Activities

FPT_TST_EXT.1
The evaluator will perform the following activities in addition to those required by the NDcPP:

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

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

Tests
The evaluator will perform the following tests:

- ***Test 1:*** *Following the operational guidance, the evaluator will initialize the integrity protection system. The evaluator will 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 will modify the TSF executable and cause that executable to be loaded by the TSF. The evaluator will 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).*

5.1.1.5 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

The TSF shall be capable of using **IEEE 802.1X, [selection: *Internet Protocol Security (IPsec), Remote Authentication Dial In User Service (RADIUS) over Transport Layer Security (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: **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 AS must use for infrastructure communications (802.11 support is also required for wireless client communications, but this is covered by the FTP_ITC.1/Client). 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 Activities

FTP_ITC.1
The evaluator will perform the following activities in addition to those required by the NDcPP:

TSS
The evaluator will 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 will also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Guidance
The evaluator will 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 will perform the following tests:

- ***Test 1:*** *The evaluator will 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 will follow the guidance documentation to ensure that the communication channel can be initiated from the TOE.*
- ***Test 3:*** *The evaluator will ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- ***Test 4:*** *The evaluator will, for each protocol associated with each authorized IT entity tested during test 1, physically interrupt an established connection. The evaluator will ensure that when physical connectivity is restored, communications are appropriately protected.*

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 Security Audit (FAU)

FAU_GEN.1/WLAN Audit Data Generation

FAU_GEN.1.1/WLAN

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [not specified] level of audit; and
c. [*Auditable events listed in the Auditable Events table (Table 2)*
d. *Failure of wireless sensor communication*]

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1/WPA	None.	
FCS_CKM.2/DISTRIB (optional)	None.	
FCS_CKM.2/GTK	None.	
FCS_CKM.2/PMK	None.	
FCS_RADSEC_EXT.1 (selection-based)	None.	
FCS_RADSEC_EXT.2 (selection-based)	None.	
FCS_RADSEC_EXT.3 (selection-based)	None.	
FCS_IPSEC_EXT.1 (selection-based)	Protocol failures.	Reason for failure. Non-TOE endpoint of connection.
	Establishment or Termination of an IPsec SA.	Non-TOE endpoint of connection.
FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (e.g. Media Access Control [Media Access Control (MAC)] address).
	Failed authentication attempt.	Provided client identity (e.g. MAC address).
FIA_PSK_EXT.1 (selection-based)	None.	
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FMT_SMF.1/AccessSystem	None.	
FMT_SMR_EXT.1	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 TSF self-test.	None.
	Detected integrity violations.	The TSF code file that caused the integrity violation.
FTA_TSE.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FTP_ITC.1	Failed attempts to	Identification of the

	establish a trusted channel (including IEEE 802.11).	initiator and target of channel.
	Detection of modification of channel data.	

Table 2: Auditable Events

Application Note: The auditable events defined in Table 2 are for the SFRs that are explicitly defined in this PP-Module and are intended to extend FAU_GEN.1 in the Base-PP.
The events in the Auditable Events table should be combined with those of the NDcPP in the context of a conforming Security Target.

The Auditable Events (Table 2) includes optional and objective SFRs. The auditing of optional and objective SFRs is only required if that SFR is included in the ST.

Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel.

Evaluation Activities

FAU_GEN.1/WLAN
TSS
There are no TSS evaluation activities for this SFR.

Guidance
There are no operational guidance activities for this SFR.

Tests
The evaluator will test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the evaluation activities associated with the functional requirements in this PP-Module. When verifying the test results, the evaluator will ensure the audit records generated during testing match the format specified in the administrative guide and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

5.2.2 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-512, PRF-704, no other algorithm]*] and specified cryptographic key sizes [*256 bits and [**selection**: 128 bits, 192 bits, no other key sizes]*] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: [*IEEE 802.11-2020 and [**selection**: IEEE 802.11ax-2021, no other standards]*].

Application Note: The cryptographic key derivation algorithm required by IEEE 802.11-2020 (Section 12.7.1.2) 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 802.11ax-2021 (Section 12.5.5) and requires a Key Derivation Function (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 or derived for the communications between the AP and the client once the client has been authenticated. It refers to the derivation of the Group Temporal Key (GTK), through the Random Bit Generator (RBG) specified in this PP-Module, as well as the derivation of the Pairwise Transient Key (PTK) from the Pairwise Master Key (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 802.11-2020, primarily in chapter 12. FCS_RBG_EXT.1 is defined in the NDcPP.

Evaluation Activities

FCS_CKM.1/WPA
TSS
The cryptographic primitives will be verified through evaluation activities specified elsewhere in this PP-Module. The evaluator will 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 will include how the GTK and PTK are generated or derived. The TSS will also provide a description of the developer's methods 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 will 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 will perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless client:

Step 1: The evaluator will configure the AP 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 client.

Step 2: The evaluator will configure the TOE to communicate with a WLAN client using IEEE 802.11-2020 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 will start the sniffing tool, initiate a connection between the TOE and WLAN client, and allow the TOE to authenticate, associate, and successfully complete the four-way handshake with the client.

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

Step 5: The evaluator will identify the four-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK from the four-way handshake frames and pre-shared key as specified in IEEE 802.11-2020.

Step 6: The evaluator will select the first data frame from the captured packets that was sent between the client and TOE after the four-way handshake successfully completed and without the frame control value 0x4208 (the first two bytes are 08 42). The evaluator will use the PTK to decrypt the data portion of the packet as specified in IEEE 802.11-2020 and verify that the decrypted data contains ASCII-readable text.

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

Additionally, the evaluator will 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*
- *Annex J.3 "PRF reference implementation and test vectors" of IEEE 802.11-2020*

FCS_CKM.2/GTK Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/GTK

The TSF shall distribute **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 802.11-2020 for the packet format and timing considerations*] **and does not expose the cryptographic keys**.

Application Note: This requirement applies to the GTK that is generated by the TOE for use in broadcast and multicast messages to clients to which it is connected. 802.11-2020 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 Activities

FCS_CKM.2/GTK
TSS
The evaluator will check the TSS to ensure that it describes how the GTK is wrapped prior to being distributed using the AES implementation specified in this PP-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 will 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 and multicast functionality, these steps will be performed as the evaluator connects multiple clients to the TOE. The evaluator will ensure that GTKs established are sent to the appropriate participating clients.

Step 1: The evaluator will configure the AP 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 client.

Step 2: The evaluator will configure the TOE to communicate with the client using IEEE 802.11-2020 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 will start the sniffing tool, initiate a connection between the TOE and client, and allow the client to authenticate, associate and successfully complete the four-way handshake with the TOE.

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

Step 5: The evaluator will identify the four-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK and GTK from the four-way handshake frames and pre-shared key as specified in IEEE 802.11-2020.

Step 6: The evaluator will select the first data frame from the captured packets that was sent between the TOE and client after the four-way handshake successfully completed, and with the frame control value 0x4208 (the first two bytes are 08 42). The evaluator will use the GTK to decrypt the data portion of the selected packet as specified in IEEE 802.11-2020 and verify that the decrypted data contains ASCII-readable text.

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

The evaluator will also perform the following testing based on the supported GTK distribution methods:

AES Key Wrap (AES-KW Tests)

- ***Test 1:*** *The evaluator will test the authenticated encryption functionality of AES-KW for each combination of the following input parameter lengths:*
  - *128 and 256 bit key encryption keys (KEKs)*
  - *Three plaintext lengths:*
    1. *One of the plaintext lengths will be two semi-blocks (128 bits).*
    2. *One of the plaintext lengths will be three semi-blocks (192 bits).*
    3. *The third data unit length will be the longest supported plaintext length less than or equal to 64 semi-blocks (4096 bits).*

  For each combination, generate a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KW authenticated encryption. To determine correctness, the evaluator will use the same key and plaintext values and encrypt them using a known good implementation of AES-KW authenticated-encryption, and ensure that the resulting respective ciphertext values are identical.
- ***Test 2:*** *The evaluator will test the authenticated-decryption functionality of AES-KW using the same test as for authenticated-encryption, replacing plaintext values with ciphertext values and AES-KW authenticated-encryption with AES-KW authenticated-decryption. Additionally, the evaluator will 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 will test the authenticated-encryption functionality of AES-KWP for each combination of the following input parameter lengths:

  128 and 256 bit key encryption keys (KEKs)

  Three plaintext lengths. One plaintext length will be one octet. One plaintext length will be 20 octets (160 bits). One plaintext length will 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 will use the AES-KWP authenticated-encryption function of a known good implementation.

- ***Test 2:*** *The evaluator will 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 will 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 PMK** in accordance with a specified cryptographic key distribution method: [*from 802.1X Authorization Server*] that meets the following: [*IEEE 802.11-2020*] **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 both WPA2-Enterprise and WPA3-Enterprise at a minimum 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 Activities

FCS_CKM.2/PMK
TSS
The evaluator will examine the TSS to determine that it describes how the PMK is transferred (that is, through what Extensible Authentication Protocol (EAP) attribute) to the TOE.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will establish a session between the TOE and a RADIUS server according to the configuration guidance provided. The evaluator will 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.

5.2.3 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 four-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 the TOE acting as a transfer point only. The TOE establishes an EAP over Local Area Network (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 evaluation 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 Activities

FIA_8021X_EXT.1
TSS
In order to show that the TSF implements the 802.1X-2010 standard correctly, the evaluator will 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*
- *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 will 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 will perform the following tests:

- ***Test 1:*** *The evaluator will demonstrate that a wireless client has no access to the test network. After successfully authenticating with a RADIUS server through the TOE, the evaluator will demonstrate that the wireless client does have access to the test network.*
- ***Test 2:*** *The evaluator will demonstrate that a wireless client has no access to the test network. The evaluator will 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 will demonstrate that a wireless client has no access to the test network. The evaluator will 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 is 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 Activities

FIA_UAU.6
TSS
There are no TSS evaluation activities for this component.

Guidance
There are no guidance evaluation activities for this component.

Tests

The evaluator will attempt to change their password as directed by the operational guidance. While making this attempt, the evaluator will verify that re-authentication is required.
If other re-authentication conditions are specified, the evaluator will cause those conditions to occur and verify that the TSF re-authenticates the authenticated user.

5.2.4 Security Management (FMT)

FMT_SMF.1/AccessSystem Specification of Management Functions (WLAN Access Systems)

FMT_SMF.1.1/AccessSystem

The TSF shall be capable of performing the following management functions:

- Configure the security policy for each wireless network, including:
  - Security type
  - Authentication protocol
  - Client credentials to be used for authentication
  - Service Set Identifier (SSID)
  - If the SSID is broadcasted
  - Frequency band set to [**selection**: *2.4 GHz*, *5 GHz*, *6 GHz*]
  - Transmit power level

Evaluation Activities

FMT_SMF.1/AccessSystem
TSS
The evaluator will confirm that the TSS includes which security types (e.g., WPA3), authentication protocol (e.g., SAE), and frequency bands the WLAN AS supports. The evaluator will confirm that the TSS includes how connection attempts from clients that are not operating on an approved security type are handled.

Guidance
The evaluator will confirm that the operational guidance includes instructions for configuring the WLAN AS for each feature listed.

Tests

- ***Test 1:*** *For each security type specified in the TSS, configure the network to the approved security type and verify that the client can establish a connection. Maintaining the same SSID, change the security type of the client to a non-approved security type and attempt to establish a connection. Verify that the connection was unsuccessful.*
- ***Test 2:*** *For each authentication protocol specified in the TSS, configure the network accordingly per the AGD. Verify that the client connection attempt is successful when using the correct client credentials and that the connection is unsuccessful when incorrect authentication credentials are used.*
- ***Test 3:*** *Configure the SSID to be broadcasted. Using a network sniffing tool, capture a beacon frame and confirm that the SSID is included. Configure the SSID to be hidden. Using a network sniffing tool, capture a beacon frame and confirm that the SSID is not listed.*
- ***Test 4:*** *The evaluator will configure the AS to operate in each of the selected frequency bands and verify using a network sniffing tool.*
- ***Test 5:*** *The evaluator will demonstrate that the client can establish a connection to the AS on the default power level. After disconnecting, the power level should be adjusted and then the client should be able to successfully connect to the AS again.*

FMT_SMR_EXT.1 No Administration from Client

FMT_SMR_EXT.1.1

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

Evaluation Activities

FMT_SMR_EXT.1
TSS
There are no TSS evaluation activities for this component.

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

Tests
The evaluator will 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 will then demonstrate that an identically configured wireless client that can successfully connect to the TOE cannot be used to perform administration.

5.2.5 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 Activities

FPT_FLS.1
TSS
The evaluator will examine the TSS to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator will 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 will 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 will 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 will ensure that the TOE attains a secure state (e.g., shutdown) after initiating each failure mode type.

5.2.6 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1

The TSF shall be able to deny session 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 the TOE that the WLAN client is connecting to (e.g. specific WLAN APs). "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 Activities

FTA_TSE.1
TSS
The evaluator will examine the TSS to determine that all of the attributes on which a client session can be denied are specifically defined.

Guidance
The evaluator will 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 will 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 the client's access is denied based on a specific value of the attribute. The evaluator will 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 AP) it is connecting to, or that the client is denied access based upon the time-of-day or day-of-week it is attempting connection on). The evaluator will observe that the access attempt fails.*

5.2.7 Trusted Path/Channels (FTP)

FTP_ITC.1/Client Inter-TSF Trusted Channel (WLAN Client Communications)

FTP_ITC.1.1/Client

The TSF shall be capable of using WPA3-Enterprise, WPA2-Enterprise and [**selection**: *WPA3-SAE*, *WPA3-SAE-PK*, *WPA2-PSK*, *no other mode*] as defined by IEEE 802.11-2020 to provide a trusted communication channel between itself and WLAN clients 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.

FTP_ITC.1.2/Client

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

FTP_ITC.1.3/Client

The TSF shall initiate communication via the trusted channel for [*no services*].

Evaluation Activities

FTP_ITC.1/Client
This component is adequately evaluated when performing the evaluation activities for FTP_ITC.1 in the Network Device, version 2.2e base-PP.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 3: SFR Rationale

Objective	Addressed by	Rationale
O.CRYPTOGRAPHIC_FUNCTIONS	FCS_COP.1/DataEncryption (modified from Base-PP)	FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions.
	FCS_CKM.1/WPA	FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2.
	FCS_CKM.2/GTK	FCS_CKM.2/GTK supports the objective by requiring the TSF to distribute group temporal keys used for IEEE 802.11.
	FCS_CKM.2/PMK	FCS_CKM.2/PMK supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11.
	FCS_CKM.2/DISTRIB (optional)	FCS_CKM.2/DISTRIB supports the objective by optionally requiring the TSF to distribute IEEE 802.11 keys to any distributed TOE components using a secured method.
O.AUTHENTICATION	FCO_CPC_EXT.1 (from Base-PP)	FCO_CPC_EXT.1 supports the objective by requiring the TSF to implement a mechanism that authenticates its distributed components to each other.
	FIA_8021X_EXT.1	FIA_8021X_EXT.1 supports the objective by requiring the TSF to act as the authenticator for 802.1X authentication.

	FIA_UAU.6	FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances.
	FTA_TSE.1	FTA_TSE.1 supports the objective by requiring the TSF to deny the establishment of a wireless client session for reasons unrelated to the correctness of an authentication credential.
	FCS_RADSEC_EXT.1 (selection-based)	FCS_RADSEC_EXT.1 supports the objective by optionally requiring the TSF to implement RadSec in accordance with a defined specification.
	FCS_RADSEC_EXT.2 (selection-based)	FCS_RADSEC_EXT.2 supports the objective by optionally requiring the TSF to implement RadSec using pre-shared keys if that is the method chosen for peer authentication.
	FIA_PSK_EXT.1 (selection-based)	FIA_PSK_EXT.1 supports the objective by optionally requiring the TSF to implement pre-shared key authentication if any trusted protocols require its use.
O.FAIL_SECURE	FPT_TST_EXT.1 (modified from Base-PP)	FPT_TST_EXT.1 supports the objective by requiring the TSF to perform self-tests that may aid in the detection of a TSF failure.
	FPT_FLS.1	FPT_FLS.1 supports the objective by requiring the TSF to preserve a secure state in the event of a self-test failure.
O.SYSTEM_MONITORING	FAU_GEN.1/WLAN	FAU_GEN.1/WLAN supports the objective by requiring the TSF to generate audit records for security-relevant WLAN behavior.
	FAU_GEN_EXT.1 (modified from Base-PP)	FAU_GEN_EXT.1 supports the objective by requiring the TSF to generate appropriate security-relevant auditable events on each of its distributed components.
	FAU_STG_EXT.1 (modified from Base-PP)	FAU_STG_EXT.1 supports the objective by defining how distributed TOE components store their generated audit records.
O.TOE_ADMINISTRATION	FMT_SMR_EXT.1	FMT_SMR_EXT.1 supports the objective by requiring the TSF to prevent any administrative actions that originate from the 'external' network.
	FMT_SMF.1/AccessSystem	FMT_SMF.1/AccessSystem supports the objective by defining management functionality that is specific to WLAN AS devices.

5.4 TOE Security Assurance Requirements

This PP-Module does not define any Security Assurance Requirements (SARs) beyond those defined within the Base-PP to which it can claim conformance. It is important to note that a TOE that is evaluated against this PP-Module is inherently evaluated against the NDcPP as well. This PP includes a number of EAs associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this PP-Module includes a number of SFR-based EAs that similarly refine the SARs of the Base-PP. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from this PP-Module.

6 Consistency Rationale

6.1 Collaborative Protection Profile for NDs

6.1.1 Consistency of TOE Type

When this PP-Module extends the NDcPP, 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

PP-Module Threat, Assumption, OSP	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.
A.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.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the NDcPP 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 OE are consistent with the NDcPP based on the following rationale:

PP-Module OE Objective	Consistency Rationale
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 NDcPP that are needed to support WLAN Access System functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDcPP that are used entirely to provide functionality for WLAN Access System. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_GEN_EXT.1	This PP-Module does not modify the Base-PP SFR; it only mandates the inclusion of the SFR because a conformant TOE will always require this functionality that is only conditional in the Base-PP.
FAU_STG_EXT.1	This PP-Module modifies a Base-PP SFR by restricting the selection options to a subset of those defined in the Base-PP. .
FAU_STG_EXT.4	This PP-Module does not modify the Base-PP SFR; it only mandates the inclusion of the SFR because a conformant TOE will always require this functionality that is only conditional in the Base-PP.
FCO_CPC_EXT.1	This PP-Module does not modify the Base-PP SFR; it only mandates the inclusion of the SFR because a conformant TOE will always require this functionality that is only conditional in the Base-PP.
FCS_COP.1/DataEncryption	This PP-Module modifies the Base-PP's definition of the SFR 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 the SFR 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 the SFR 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.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
FAU_GEN.1/WLAN	This SFR iterates the FAU_GEN.1 SFR defined in the Base-PP to define auditable events for the functionality that is specific to this PP-Module.
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_SMF.1/AccessSystem	This SFR defines additional management functionality that is specific to the Module's product type and would therefore not be expected to be present in the Base-PP.
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 by FPT_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.
FTP_ITC.1/Client	This SFR iterates the FTP_ITC.1 SFR defined in the Base-PP to define trusted communication channels for the functionality that is specific to this PP-Module.
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.509v3 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.
FCS_RADSEC_EXT.3	This SFR defines the implementation of RadSec when pre-shared key authentication with RSA 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.	
Implementation-based SFRs	
This PP-Module does not define any Implementation-based requirements.	

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 Cryptographic Support (FCS)

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(Base-PP)*] 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 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 APs, 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 Activities

FCS_CKM.2/DISTRIB
TSS
The evaluator will 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 will 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 (Base-PP).

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

This PP-Module does not define any Implementation-dependent SFRs.

Appendix B - Selection-based Requirements

B.1 Cryptographic Support (FCS)

FCS_RADSEC_EXT.1 RadSec

The inclusion of this selection-based component depends upon selection in FTP_ITC.1.1.

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 and FIA_PSK_EXT.1 in this PP-Module must be claimed.

Evaluation Activities

FCS_RADSEC_EXT.1
TSS
The evaluator will 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 will ensure that the TSS description includes the use of client-side certificates for TLS mutual authentication.

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

Tests
The evaluator will demonstrate the ability to successfully establish a RADIUS over TLS connection with a RADIUS server. This test will 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

The inclusion of this selection-based component depends upon selection in FCS_RADSEC_EXT.1.2.

FCS_RADSEC_EXT.2.1

The TSF shall implement [**selection**: *TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] and no earlier TLS versions when acting as a RADIUS over TLS client that supports the following ciphersuites: [**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: If any of the TLS_RSA_PSK ciphersuites are selected by the ST author, it is necessary to claim the selection-based requirement

FCS_RADSEC_EXT.3.

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

Evaluation Activities

FCS_RADSEC_EXT.2

TSS

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

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

The evaluator will 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 ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

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

Tests

The evaluator will perform the following tests:

- ***Test 1:*** *The evaluator will establish a RADIUS over TLS connection using each of the ciphersuites 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 will 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 will 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 will 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 will 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 the TOE does not generate bit-based pre-shared keys, the evaluator will obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.*
- ***Test 6:*** *[conditional] If the TOE does generate bit-based pre-shared keys, the evaluator will generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.*

FCS_RADSEC_EXT.3 RadSec using Pre-Shared Keys and RSA

The inclusion of this selection-based component depends upon selection in FCS_RADSEC_EXT.2.1.

FCS_RADSEC_EXT.3.1

When the TSF negotiates a TLS_RSA_PSK cipher suite, the TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

Application Note: This requirement must be claimed if any ciphersuites beginning with 'TLS_RSA_PSK' are selected in FCS_RADSEC_EXT.2.1.
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.

FCS_RADSEC_EXT.3.2

When the TSF negotiates a TLS_RSA_PSK cipher suite, the TSF shall [**selection**: *not establish the connection*, *request authorization to establish the connection*, *[**assignment**: other action]*] if the presented server certificate is deemed invalid.

Application Note: This requirement must be claimed if any ciphersuites beginning with 'TLS_RSA_PSK' are selected in FCS_RADSEC_EXT.2.1.
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.

Evaluation Activities

FCS_RADSEC_EXT.3
TSS
The evaluator will ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator and 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 will ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the TOE.

Guidance
The evaluator will 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 will perform the following tests:

- ***Test 1:*** *The evaluator will 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.*
- ***Test 2:*** *The evaluator will 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 will verify that the connection fails.*
- ***Test 3:*** *The evaluator will 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 will verify that the connection fails. The evaluator will repeat this test for each supported SAN type.

- ***Test 4:*** *The evaluator will 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 will verify that the connection succeeds.*
- ***Test 5:*** *[conditional] If the TOE does not mandate the presence of the SAN extension, the evaluator will present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator will verify that the connection succeeds. If the TOE does mandate the presence of the SAN extension, this test will be omitted.*
- ***Test 6:*** *[conditional] If wildcards are supported by the TOE, the evaluator will perform the following tests:*
  - *The evaluator will 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 will present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g. *.example.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.example.com). The evaluator will verify that the connection succeeds. The evaluator will 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 will configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.*
  - *The evaluator will present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.*
- ***Test 7:*** *[conditional] If wildcards are not supported by the TOE, the evaluator will present a server certificate containing a wildcard and verify that the connection fails.*
- ***Test 8:*** *[conditional] If URI or Service name reference identifiers are supported, the evaluator will configure the DNS name and the service identifier. The evaluator will 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 will repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.*

B.2 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

The inclusion of this selection-based component depends upon selection in FCS_RADSEC_EXT.1.2.

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for [**selection**: *RADIUS over TLS (RadSec), IPsec, WPA3-SAE, WPA3-SAE-PK, IEEE 802.11 WPA2-PSK, [**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: This requirement must be included if IPsec or another protocol that uses pre-shared keys is claimed, and pre-shared key authentication is selected (e.g., "Pre-shared Keys" is selected in FCS_IPSEC_EXT.1.13 or "pre-shared keys" is selected in FCS_RADSEC_EXT.1.2). 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 Activities

FIA_PSK_EXT.1
TSS
The evaluator will verify that the TSS describes

1. *the protocols that can use pre-shared keys and that these are consistent with the selections made in FIA_PSK_EXT.1.1.*
2. *the allowable values for pre-shared keys and that they are consistent with the selections made in FIA_PSK_EXT.1.2.*
3. *the way bit-based pre-shared keys are procured and that it is consistent with the selections made in FIA_PSK_EXT.1.3.*

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

Tests
The evaluator will 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 will 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 will 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 will obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator will 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 will generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.*

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the Module.

C.1 Extended Components Table

All extended components specified in the Module are listed in this table:

Table 4: Extended Component Definitions

Functional Class	Functional Components
Identification and Authentication (FIA)	FIA_8021X_EXT 802.1X Port Access Entity (Authenticator) Authentication FIA_PSK_EXT Pre-Shared Key Composition
Security Management (FMT)	FMT_SMR_EXT Security Management Restrictions
Cryptographic Support (FCS)	FCS_RADSEC_EXT RadSec

C.2 Extended Component Definitions

C.2.1 Identification and Authentication (FIA)

This Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.1.1 FIA_8021X_EXT 802.1X Port Access Entity (Authenticator) Authentication

Family Behavior

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

Component Leveling

FIA_8021X_EXT ——— 1

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 ST:

- Attempts to access the 802.1X controlled port prior to successful 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 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

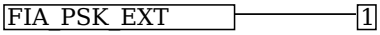
The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

C.2.1.2 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*, *WPA3-SAE*, *WPA3-SAE-PK*, *IEEE 802.11 WPA2-PSK*, *[**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.

C.2.2 Security Management (FMT)

This Module defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.2.1 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 administer remotely the TOE from a wireless client shall be

disabled by default.

C.2.3 Cryptographic Support (FCS)

This Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.3.1 FCS_RADSEC_EXT RadSec

Family Behavior

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

Component Leveling

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

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.

FCS_RADSEC_EXT.3, RadSec using Pre-Shared Keys and RSA, requires the TSF to validate the external entity used for trusted communications.

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.509v3 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 [**assignment**: *some authentication method*].

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 [**assignment**: *list of allowed TLS versions*] and reject all other TLS and SSL versions. The TLS implementation shall support the following ciphersuites for use when acting as a RADIUS over TLS client: [**assignment**: *list of supported ciphersuites*].

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.

Management: FCS_RADSEC_EXT.3

No specific management functions are identified.

Audit: FCS_RADSEC_EXT.3

There are no auditable events foreseen.

FCS_RADSEC_EXT.3 RadSec using Pre-Shared Keys and RSA

Hierarchical to: No other components.

Dependencies to: FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys
FIA_X509_EXT.1 X.509v3 Certificate Validation

FCS_RADSEC_EXT.3.1

When the TSF negotiates a TLS_RSA_PSK cipher suite, the TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_RADSEC_EXT.3.2

When the TSF negotiates a TLS_RSA_PSK cipher suite, the TSF shall [**selection**: *not establish the connection, request authorization to establish the connection, [**assignment**: other action]*] if the presented server certificate is deemed invalid.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this Module. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP provides evidence that these controls are present and have been evaluated.

This PP-Module has no implicitly satisfied requirements. All SFR dependencies are explicitly met either through SFRs defined by the PP-Module or inherited from the Base-PP.

Appendix E - Allocation of Requirements in Distributed TOEs

For a distributed TOE, the security functional requirements in this PP-Module need to be met by the TOE as a whole, but not all SFRs will necessarily be implemented by all components. The following categories are defined in order to specify when each SFR must be implemented by a component:

- **All Components ("All")** —All components that comprise the distributed TOE must independently satisfy the requirement.
- **At least one Component ("One")** —This requirement must be fulfilled by at least one component within the distributed TOE.
- **Feature Dependent ("Feature Dependent")** — These requirements will only be fulfilled where the feature is implemented by the distributed TOE component (note that the requirement to meet the PP-Module as a whole requires that at least one component implements these requirements if they are claimed by the TOE).

The table below specifies how each of the SFRs in this PP-Module must be met, using the categories above.

Requirement	Description	Distributed TOE SFR Allocation
FAU_GEN.1/WLAN	Audit Data Generation	All
FCS_CKM.1/WPA	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	One
FCS_CKM.2/GTK	Cryptographic Key Distribution (GTK)	Feature Dependent
FCS_CKM.2/PMK	Cryptographic Key Distribution (PMK)	Feature Dependent
FIA_8021X_EXT.1	802.1X Port Access Entity (Authenticator) Authentication	One
FIA_UAU.6	Re-Authenticating	Feature Dependent
FMT_SMF.1/AccessSystem	Specification of Management Functions	Feature Dependent
FMT_SMR_EXT.1	No Administration from Client	All
FPT_FLS.1	Failure with Preservation of Secure State	All
FTA_TSE.1	TOE Session Establishment	All
FTP_ITC.1/Client	Inter-TSF Trusted Channel (WLAN Client Communications)	All
FCS_CKM.2/DISTRIB	Cryptographic Key Distribution (802.11 Keys)	Feature Dependent
FCS_RADSEC_EXT.1	RadSec	Feature Dependent
FCS_RADSEC_EXT.2	RadSec using Pre-Shared Keys	Feature Dependent
FCS_RADSEC_EXT.3	RadSec using Pre-Shared Keys and RSA	Feature Dependent
FIA_PSK_EXT.1	Pre-Shared Key Composition	Feature Dependent

Appendix F - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PP.

Appendix G - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AP	Access Point
AS	Access System
Base-PP	Base Protection Profile
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter Mode with CBC-Message Authentication Code
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
NDcPP	Network Device collaborative Protection Profile
OE	Operational Environment
PAE	Port Access Entity
PMK	Pairwise Master Key
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
RBG	Random Bit Generator
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
TSF Interface (TSFI)	TSF Interface
TSS	TOE Summary Specification
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
Collaborative Protection Profile (cPP)	Collaborative Protection Profile

Appendix H - 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.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019