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

Version: 1.0
2020-10-28
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-10-28	Initial Release

Contents

1 Overview

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

- Collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e

This Base-PP is valid because a WLAN Access System 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. This is functionality that typically will be implemented by a network device.

A TOE that conforms to a PP-Configuration containing this PP-Module may be a 'Distributed TOE' as defined in the NDcPP. The TOE functionality may reside entirely within a single device or be spread across multiple distributed physical components.

1.1 Terms

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

1.1.1 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.
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 Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.

TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.1.2 Technical Terms

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

2 Compliant Targets of Evaluation

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

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

3 Use Cases

[USE CASE 1] Standalone Device

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

[USE CASE 2] Distributed System

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

Conformance Statement

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

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

- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1

CC Conformance Claims

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

Package Claims

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

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

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

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

4 Threats

T.NETWORK_DISCLOSURE

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

T.NETWORK_ACCESS

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

T.TSF_FAILURE

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

T.DATA_INTEGRITY

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

T.REPLAY_ATTACK

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

5 Assumptions

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

All assumptions for the operational environment 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.

6 Organizational Security Policies

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

7 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 functionailty and security.

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

8 Security Objectives for the Operational Environment

The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment.

All objectives for the operational environment 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.

8.1 Security Objectives Rationale

This section describes how the assumptions, threats, and organization 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 cryptogpraphic 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 operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.

9 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."

9.1 NDc PP Security Functional Requirements Direction

In a PP-Configuration that includes NDc PP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDc PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDc PP in addition to what is mandated by Section 9.2 TOE Security Functional Requirements.

9.1.1 Modified SFRs

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

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

FCS_COP.1.1/DataEncryption

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

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

This requirement mandates two modes for AES with key size of 128 bits be implemented. It is not expected that these modes will both be used for all encryption/decryption functionality. Rather, the mandates serve particular purposes: to comply with the FCS_IPSEC_EXT.1 requirements, CBC mode is mandated, and to comply with IEEE 802.11-2012, AES-CCMP (which uses AES in CCM as specified in SP 800-38C) must be implemented.

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

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

Evaluation Activities

FCS_COP.1/DataEncryption:

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests **during initial start-up (on power on) and** [**selection**: *periodically during normal operation, at the request of the authorised user, at the conditions [**assignment**: conditions under which self-tests should occur], **in no other circumstances***] to demonstrate the correct operation of 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:

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

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

Application Note: This requirement has been modified from its definition in the NDcPP to mandate the communications protocols and environmental components that a WLAN Access System must use. IEEE 802.11-2012 (WPA2) with IEEE 802.1X is required for communications with wireless clients; IPsec or RADIUS over TLS (commonly known as "RadSec") is required at least for communications with the 802.1X authentication server. Other selections may be made if needed by other parts of the TSF. The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage.

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

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

FTP_ITC.1.2

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

FTP_ITC.1.3

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

Evaluation Activities

FTP_ITC.1:

9.2 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.

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;
c. [*Auditable events listed in the Auditable Events table ();*
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_IPSEC_EXT.1 (selection-based)	Protocol failures.	Reason for failure. Non-TOE endpoint of connection.
	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection.
	Negotiation "down" from an IKEv2 to IKEv1 exchange.	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 (MAC address).
FIA_PSK_EXT.1 (selection-based)	None.	
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
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 establish a trusted channel (including IEEE 802.11).	Identification of the initiator and target of channel.
	Detection of modification of channel data.	

Table2: Auditable Events

Application Note: The auditable events defined in 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 () 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:

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

FCS_CKM.1.1/WPA

The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRF-384 and [**selection**: PRF-704, no other algorithm]*] and specified key sizes [*128 bits and [**selection**: 256 bits, no other key sizes]*] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: [*IEEE 802.11-2012 and [**selection**: IEEE 802.11ac-2013, no other standards]*].

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

This requirement applies only to the keys that are generated/derived for the communications between the access point and the client once the client has been authenticated. It refers to the derivation of the GTK (through the RBG specified in this PP-Module) as well as the derivation of the PTK from the PMK, which is done using a random value generated by the RBG specified in this PP-Module, the HMAC function as specified in this PP-Module, as well as other information. This is specified in IEEE 802.11-2012 primarily in chapter 11. FCS_RBG_EXT.1 is defined in the NDcPP.

Evaluation Activities

FCS_CKM.1/WPA:

FCS_CKM.2/GTK Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/GTK

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

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

Evaluation Activities

FCS_CKM.2/GTK:

FCS_CKM.2/PMK Cryptographic Key Distribution (PMK)

FCS_CKM.2.1/PMK

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

Application Note: This requirement applies to the Pairwise Master Key that is

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

Evaluation Activities

FCS_CKM.2/PMK:

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

FIA_8021X_EXT.1.1

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

FIA_8021X_EXT.1.2

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

FIA_8021X_EXT.1.3

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

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

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

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

Evaluation Activities

FIA_8021X_EXT.1:

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:

FMT_SMR_EXT.1 No Administration from Client

FMT_SMR_EXT.1.1

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

Evaluation Activities

FMT_SMR_EXT.1:

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:

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 access point(s)). “Time” and “day” refer to time-of-day and day-of-week respectively.

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

Evaluation Activities

FTA_TSE.1:

9.3 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_IPSEC_EXT.1 (from Base-PP), FCS_TLSC_EXT.1 (from Base-PP), FCS_TLSC_EXT.2 (from Base-PP), FCS_CKM.1/WPA, FCS_CKM.2/GTK, FCS_CKM.2/PMK, FCS_CKM.2/DISTRIB (optional)	FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions. FCS_IPSEC_EXT.1 supports the objective by requiring the TSF to use IPsec to implement a trusted communications channel if selected in FTP_ITC.1. FCS_TLSC_EXT.1 supports the objective by requiring the TSF to use RADIUS over TLS (RadSec) to implement a trusted communications

		channel if selected in FTP_ITC.1. FCS_TLSC_EXT.2 supports the objective by requiring the TSF to use X.509 certificates as the authentication method used for RadSec. FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2. 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 supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11. 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	FCS_IPSEC_EXT.1 (from Base-PP), FCS_TLSC_EXT.1 (from Base-PP), FCS_TLSC_EXT.2 (from Base-PP), FIA_X509_EXT.1/Rev (from Base-PP), FTP_ITC.1 (modified from Base-PP), FIA_8021X_EXT.1, FIA_UAU.6, FTA_TSE.1, FCS_RADSEC_EXT.1 (selection-based), FCS_RADSEC_EXT.2 (selection-based), FIA_PSK_EXT.1 (selection-based)	FCS_IPSEC_EXT.1 supports the objective by optionally requiring the TSF to use IPsec to implement a trusted communications channel if selected in FTP_ITC.1. IPsec includes authenticating using X.509 certificates or pre-shared keys. FCS_TLSC_EXT.1 supports the objective by optionally requiring the TSF to use RADIUS over TLS (RadSec) to implement a trusted communications channel if selected in FTP_ITC.1. TLS includes authenticating using X.509 certificates or pre-shared keys. FCS_TLSC_EXT.2 supports the objective by optionally requiring the TSF to use X.509 certificates as the authentication method used for RadSec. FIA_X509_EXT.1/Rev supports the objective by optionally requiring the TSF to implement X.509 certificate validation if certificates are used for authentication. FTP_ITC.1 supports the objective by requiring the TSF to identify the trusted communications channels it implements, each of which is able to support authentication. FIA_8021X_EXT.1 supports

		the objective by requiring the TSF to act as the authenticator for 802.1X authentication. FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances. FTA_TSE.1 supports the objective by requiring the TSF to deny the establishment of a wirless client session for reasons unrelated to the correctness of an authentication credential. 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 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 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_FLS.1	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 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.
O.TOE_ADMINISTRATION	FIA_AFL.1 (from Base-PP), FMT_SMR_EXT.1	FIA_AFL.1 supports the objective by requiring the TSF to block authentication if there is evidence of an attempt to compromise an administrator account through brute force. FMT_SMR_EXT.1 supports the objective by requiring the TSF to prevent any administrative actions that originate from the 'external' network.

10 Consistency Rationale

10.1 Protection Profile for Network Devices

10.1.1 Consistency of TOE Type

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

10.1.2 Consistency of Security Problem Definition

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

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.

10.1.3 Consistency of Objectives

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

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

O.TOE_ADMINISTRATION	The Base-PP does not define TOE objectives but it does define requirements for management. This PP-Module is consistent with that by applying security restrictions on how the TOE's management interface can be invoked.

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

PP-Module Operational Environment 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.

10.1.4 Consistency of Requirements

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

PP-Module Requirement	Consistency Rationale
Modified SFRs	
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.
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_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.
Optional SFRs	
FCS_CKM.2/DISTRIB	This SFR defines an additional use for the cryptographic and self-protection mechanisms defined in the Base-PP.
Selection-based SFRs	
FCS_RADSEC_EXT.1	This SFR defines the implementation of RadSec and the peer authentication method that it uses. This relies on the TLS requirements defined by the Base-PP and may also use the X.509 certificate validation methods specified in the Base-PP, depending on the selected peer authentication method.
FCS_RADSEC_EXT.2	This SFR defines the implementation of RadSec when pre-shared key authentication is used. This functionality is outside the original scope of the Base-PP but it relies on the TLS client protocol implementation, cryptographic algorithms, and random bit generation functions defined by the Base-PP.
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-Dependent SFRs	
This PP-Module does not define any Implementation-Dependent requirements.	

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

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

FCS_CKM.2.1/DISTRIB

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

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

This requirement applies to any key necessary for successful IEEE 802.11 connections not covered by FCS_CKM.2/GTK. In cases where a key must be distributed to other access points, this communication must be performed via a mechanism of commensurate cryptographic strength. Because communications with any component of a distributed TOE are required to be performed over a trusted connection, the transfer of these keys will be protected.

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

Evaluation Activities

FCS_CKM.2/DISTRIB:

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 SFRs

FCS_RADSEC_EXT.1 RadSec

FCS_RADSEC_EXT.1.1

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

FCS_RADSEC_EXT.1.2

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

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

If "X.509v3 certificates" is selected in FCS_RADSEC_EXT.1.2, then FCS_TLSC_EXT.2 from the NDcPP must be claimed. If "pre-shared keys" is selected in FCS_RADSEC_EXT.1.2, then FCS_RADSEC_EXT.2 and FIA_PSK_EXT.1 in this PP-Module must be claimed.

Evaluation Activities

FCS_RADSEC_EXT.1:

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

FCS_RADSEC_EXT.2.1

The TSF shall implement [**selection**: *TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] and no earlier TLS versions when acting as a RADIUS over TLS client that supports the following cipher suites: [**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 cipher suites are selected by the ST author, it is necessary to claim the selection-based requirement FCS_RADSEC_EXT.3.

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

FCS_RADSEC_EXT.2.2

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

Evaluation Activities

FCS_RADSEC_EXT.2:

FCS_RADSEC_EXT.3 RadSec using Pre-Shared Keys and RSA

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 cipher suites 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 cipher suites 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:

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for [**selection**: *RADIUS over TLS (RadSec)*, *IPsec*, *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:

Appendix C - Extended Component Definitions

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

C.1 Extended Components Table

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

Table 4: Extended Component Definitions

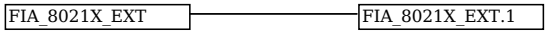
Functional Class	Functional Components

C.2 Extended Component Definitions

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

Management: FIA_8021X_EXT.1

No specific management functions are identified.

Audit: FIA_8021X_EXT.1

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

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

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

Hierarchical to: No other components.

Dependencies to: No dependencies

FIA_8021X_EXT.1.1

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

FIA_8021X_EXT.1.2

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

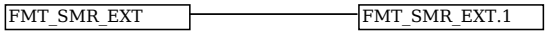
FIA_8021X_EXT.1.3

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

FMT_SMR_EXT Security Management Restrictions

Family Behavior

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



Component Leveling

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

Management: FMT_SMR_EXT.1

No specific management functions are identified.

Audit: FMT_SMR_EXT.1

There are no auditable events foreseen.

FMT_SMR_EXT.1 No Administration from Client

Hierarchical to: No other components.

Dependencies to: FMT_SMF.1 Specification of Management Functions

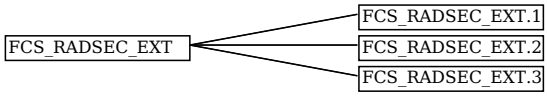
FMT_SMR_EXT.1.1

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

FCS_RADSEC_EXT RadSec

Family Behavior

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



Component Leveling

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

Management: FCS_RADSEC_EXT.1

No specific management functions are identified.

Audit: FCS_RADSEC_EXT.1

There are no auditable events foreseen.

FCS_RADSEC_EXT.1 RadSec

Hierarchical to: No other components.

Dependencies to: FCS_TLSC_EXT.1 TLS Client Protocol

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_X509_EXT.1 X.509 Certificate Validation

FCS_RADSEC_EXT.1.1

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

FCS_RADSEC_EXT.1.2

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

Component Leveling

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

Management: FCS_RADSEC_EXT.2

No specific management functions are identified.

Audit: FCS_RADSEC_EXT.2

There are no auditable events foreseen.

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

Hierarchical to: No other components.

Dependencies to: FCS_CKM.1 Cryptographic Key Generation

FCS_COP.1 Cryptographic Operation

FCS_RADSEC_EXT.1 RadSec

FCS_RBG_EXT.1 Random Bit Generation

FCS_RADSEC_EXT.2.1

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

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.

Component Leveling

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.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.509 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.

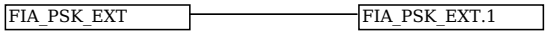
FCS_RADSEC_EXT.3.2

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.

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, 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.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this Protection Profile. However, 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 Protection Profile 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
FCS_CKM.1/WPA	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	All
FCS_CKM.2/GTK	Cryptographic Key Distribution (GTK)	All
FCS_CKM.2/PMK	Cryptographic Key Distribution (PMK)	All
FIA_8021X_EXT.1	802.1X Port Access Entity (Authentictaor) Authentication	All
FIA_UAU.6	Re-Authenticating	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
FCS_CKM.2/DISTRIB	Cryptographic Key Distribution (802.11 Keys)	Feature Dependent
FCS_RADSEC_EXT.1	RadSec	Feature Dependent
FCS_RADSEC_EXT.1	RadSec using Pre-Shared Keys	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 - 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

Appendix H - 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-MAC
CCMP	CCM mode Protocol
CEM	Common Evaluation Methodology
CTR	Counter (encryption mode)
EAP	Extensible Authentication Protocol
GCM	Galois-Counter Mode
GTK	Group Temporal Key
IPsec	Internet Protocol Security
MAC	Media Access Control or Message Authentication Code
NDcPP	Network Device collaborative Protection Profile
OE	Operational Environment
PAE	Port Access Entity
PMK	Pairwise Master Key
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSID	Service Set Identifier
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access