PP-Module for Authentication Servers

Version: 1.0
2022-08-12
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-08-12	Initial Release

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
1.4 TOE Boundary
1.5 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 Cryptographic Support (FCS)
C.2.1.1 FCS_RADSEC_EXT RadSec
C.2.2 Identification and Authentication (FIA)
C.2.2.1 FIA_8021X_EXT 802.1X Port Access Entity (Authenticator) Authentication
C.2.2.2 FIA_PSK_EXT Pre-Shared Key Composition
C.2.3 Security Management (FMT)
C.2.3.1 FMT_SMR_EXT Security Management Restrictions
Appendix D - Implicitly Satisfied Requirements
Appendix E - Allocation of Requirements in Distributed TOEs
Appendix F - Entropy Documentation and Assessment
Appendix G - Acronyms

1 Introduction

1.1 Overview

An authentication server provides assertions to a relying party that a particular request for access is from an authentic digital identity associated with various identity attributes, such as a registered account within an information system, or a certified identity as validated by a trusted certification authority or both. The digital identities can represent people, devices or processes. Authentication servers validate various authenticators controlled by the entities represented by the presented digital identity. When the entity is a person, authenticators can provide indications of what the entity knows (e.g., a password, pin or passphrase), what the entity has (e.g., a registered device in the control of the user), or what the entity is (a biometric). NIST SP 800-63-3 Part B provides recommendations about how these authenticators can be leveraged individually or in combinations to provide assurance that the entity is authentic and describes requirements for validation of the authenticators to various assurance levels. A relying party may delegate verification of authenticator(s) to an authentication server; such delegation creates a relationship between the relying party and the authentication server that is referred to as an identity federation. Assertions to a federated relying party can be via bearer assertions or via direct communication with the relying party. The latter mechanism is modeled after that used by Authentication, Access and Accounting (AAA) servers, which used the RADIUS protocol. RADIUS has been largely replaced by DIAMETER, a protocol that addresses many of the security issues with RADIUS. These provide direct, back-end assertions protected by an authenticated and encrypted channel to a Network Access Server that further governs accesses to resources on a network.

This PP-module describes the security functionality of authentication servers supporting RADIUS/DIAMETER and other messaging protocols intended for direct communications with relying parties via authenticated, real-time protected channels. The scope of this PP-Module is to describe the security functionality of an Authorization Server 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-PP:

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

This Base-PP is valid because an authentication server can be deployed as a dedicated network appliance. The use case of deploying the authentication server as an application on a general-purpose computer is outside the scope of this PP-Module. Authentication server products allow enterprises to provide a centralized and standardized method of evaluating user authentication requests made throughout the enterprise. This enables centralized definition of user identity and credential data and allows for uniform application of authentication policies that define what credentials and user attributes are necessary to gain access to various systems and applications in the enterprise environment.

Note that the NDcPP defines an optional architecture for a “distributed TOE” that allows for security functionality to be spread across multiple distinct components. This PP-Module does not require or prohibit the TOE from being a distributed system when the TOE conforms to the NDcPP; the TOE may be standalone or distributed in this case.

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	A TOE composed of multiple components operating as a logical whole.

TOE	
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 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.
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

Assertion	A statement from the TOE to an RP that contains information about a subscriber. Assertions may also contain verified attributes. For the purposes of this PP-Module, Assertions containing authentication status and identity attributes are made by EAP response messages in accordance with EAP-TLS or EAP-TTLS.
Authentication Policy	A policy that specifies which authenticator types are required for a particular entity. The policy may be implicit for all entities, or configurable.
Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant’s identity.
Authenticator Output	The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.
Claimant	A subject whose identity is to be verified using one or more authentication protocols.
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.
Federation Protocol	A protocol to establish a trusted relationship with a relying party, and for the purposes of this PP module, to communicate authentication status for entities requesting access to resources managed by the relying party. In this PP-module, Federation Protocols include RADIUS, DIAMETER, and other standard protocols used in direct communication between the relying party and the TOE. Federation protocols that only support bearer assertions are out of scope for this PP-Module.
Relying Party	An entity that relies upon the subscriber’s authenticator(s) and credentials or a verifier’s

(RP)	assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

1.3 Compliant Targets of Evaluation

This PP-Module specifically addresses a dedicated network device that performs entity (device or user) authentication via direct, back-end connections with a relying party. The entity to be authenticated is referred to as the claimant, though different terms have been used for specific protocols (e.g., peer for RADIUS/DIAMETER). The relying party can manage a single resource or provide access control for resources within a network. For example, a Wireless Local Area Network (WLAN) Access System may use the services of a dedicated authentication server during tunnel establishment. In this use case, an authentication server must support IEEE 802.1X Port-Based Network Access Control and must fulfill the IEEE 802.11 authentication server role using Extensible Authentication Protocol (EAP) messaging.

Similarly, the authentication server may be used during Virtual Private Network (VPN) tunnel establishment. The relying party in this case is a VPN Gateway acting as a Network Access Server using passthrough between the VPN client and authentication server (the TOE), also using EAP messaging.

In general, any relying party using a direct authentication federation protocol that supports EAP-TLS or EAP-TTLS messaging is addressed by this PP-Module. The combination of the NDcPP and this PP-Module is a network device that provides authentication server functionality in addition to all of the security functionality expected of a network device as mandated by the NDcPP. This PP-Module describes the functional requirements and threats specific to authentication servers. A TOE that conforms to this PP-Module must also conform to the Base-PP.

1.4 TOE Boundary

This document specifies SFRs for an authentication server. An authentication server is designed to authenticate a claimant that attempts to access a relying party – an access gateway to a protected network, or individual resources and services – and provide assertions to one or more relying parties about the authentication state of the claimant. A claimant forwards one or more authenticator outputs to the authentication server; the authentication server verifies the authenticator outputs and may also provide additional identity attributes to allow the relying party to determine whether the claimant meets its authentication policy. The authentication server defined by this PP-Module is one or more dedicated network appliances; the TOE is not intended to run as an application on a general-purpose computer. The authentication server can be co-located with an access management or privilege management system, or it may be separate from such services. Regardless of the deployment, access control functions and management of non-identity attributes are outside the scope of this PP-Module.

An authentication server may be part of a larger system that also provides authorization information, either as part of an AAA (authentication, authorization, and accounting) server, as an Authorization server, or domain controller. This PP-Module specifies the functional requirements for authentication services only; as in the case where the TOE may be co-located with the relying party, the TOE's logical boundary only includes the authentication server functionality. However, the TOE boundary includes the ability to generate audit events that are specific to the authentication functionality but may be used to support other functions (e.g. AAA servers).

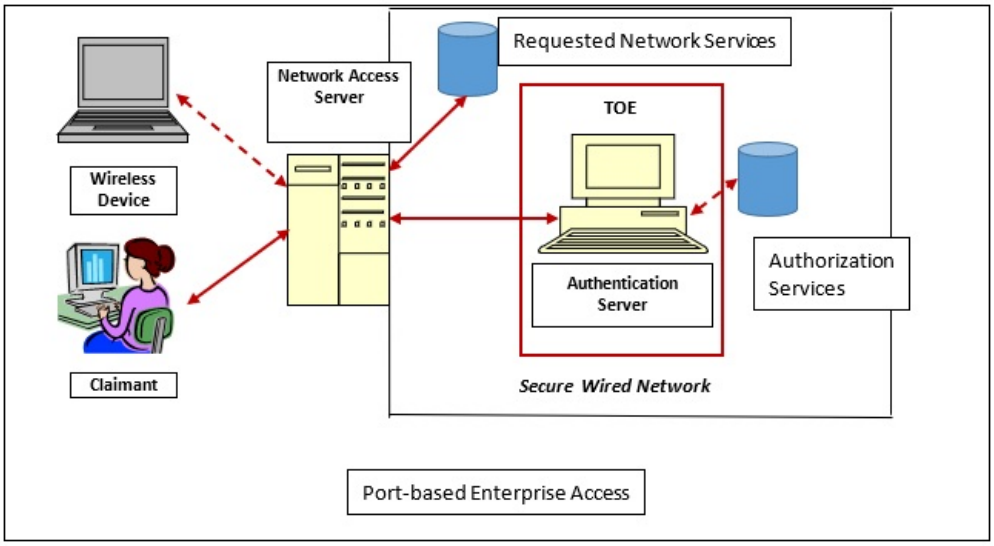


Figure 1: NAS with an Authentication Server

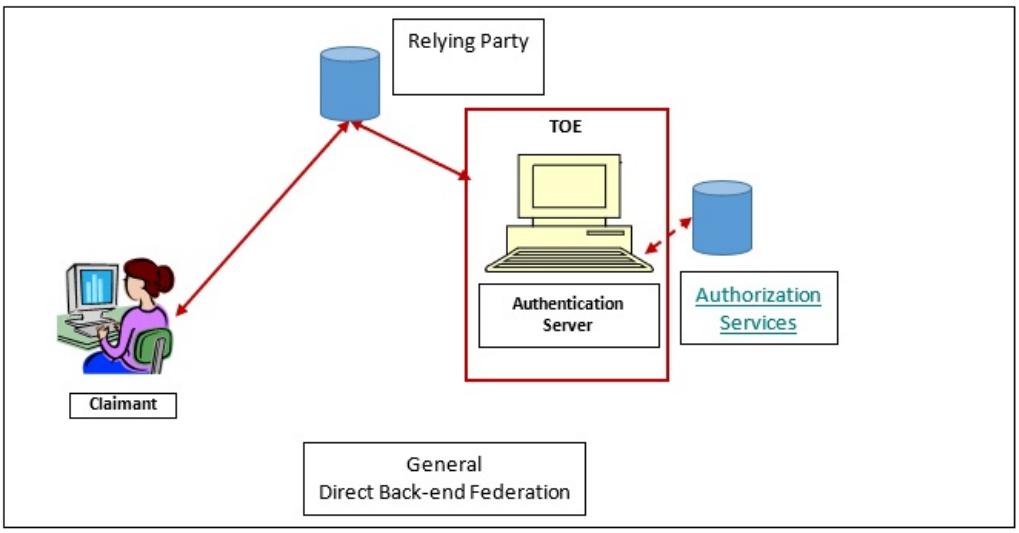


Figure 2: Generic Authentication Server User Case

1.5 Use Cases

[USE CASE 1] Dedicated Appliance

The authentication server is integrated on a standalone network appliance. In this use case, conformance to the NDcPP and this PP-Module is sufficient to ensure security. This PP-Module does not cover the use case where the authentication server is an application that is installed on a general-purpose computer.

[USE CASE 2] Standalone Server

The system on which the authentication server is deployed is solely responsible for acting as an authenticator. In this deployment, the authentication server's only network infrastructure role is to communicate with the relying party for receiving challenges and issuing responses.

[USE CASE 3] Relying Party Co-Location

The system on which the authentication server is deployed acts as both the relying party or its proxy and the authentication server. In this deployment, the authentication server's interactions with the relying party are internal-only. Regardless of whether the relying party is a standalone component or whether the authentication server executable code also provides relying party functionality, the TOE's logical boundary still only includes the authentication server component. Additionally, if the authentication server is a software application that can be deployed independently of the relying party, the required external trusted communications must still be supported; an authentication server cannot use the fact that it can be deployed on the same physical server as the relying party as a way to exempt itself from implementation of IPsec, RadSec or mutually authenticated (D)TLS with an external relying party.

[USE CASE 4] Integrated as an Authorization Server Component

The system on which the authentication server is deployed acts as an authorization server (e.g., as part of an AAA server) that provides authorization services in addition to the authentication server. Assertions made via the direct connection can also include authorization information, and an unauthorized, but authenticated user may result in a negative response to the relying party. Regardless of whether these are all standalone components or whether the authentication server executable code also provides authorization functionality, the TOE's logical boundary still only includes the authentication server component. As in the case where the authentication server is co-located with the relying party, this deployment does not exempt the TOE from being able to implement all the functionality that this PP-Module requires.

2 Conformance Claims

Conformance Statement

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

No 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 TSF.

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

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

3.2 Assumptions

These assumptions are made on the Operational Environment (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 the NDcPP, the TOE is expected to rely on some of the security functions implemented by the Authentication Server 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.

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.

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.

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.

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 AES used in **CBC, CCMP,** and [**selection**: *CTR*, *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 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.

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.

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: *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: **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*].

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	Protocol failures.	Reason for failure.

(selection-based)		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 [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 establish a trusted channel (including IEEE 802.11).	Identification of the 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.

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.

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 802.11-2020 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. 802.11-2020 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.

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 802.11-2020*] **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.

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.

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]*].

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
  - SSID
  - If the SSID is broadcasted
  - Frequency band set to [**selection**: *2.4 GHz*, *5 GHz*, *6 GHz*]
  - Transmit power level

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.

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.

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.

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*].

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 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 Authentication Servers 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 Authentication Servers 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.

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.

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.

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.

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.

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
Cryptographic Support (FCS)	FCS_RADSEC_EXT RadSec
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

C.2 Extended Component Definitions

C.2.1 Cryptographic Support (FCS)

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

C.2.1.1 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.

C.2.2 Identification and Authentication (FIA)

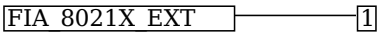
This Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.2.1 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, 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 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

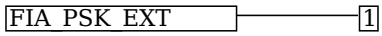
The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

C.2.2.2 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.2.3 Security Management (FMT)

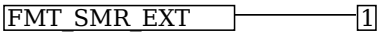
This Module defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.3.1 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.

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
AAA	Authentication, Authorization, and Accounting
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
EAP	Extensible Authentication Protocol
IPsec	Internet Protocol Security
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
RADIUS	Remote Authentication Dial In User Service
RP	Relying Party
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
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

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