PP-Module for WLAN Clients

Version: 1.0
2021-03-15
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2021-03-15	Initial Release

Contents

1 Introduction

1.1 Overview

The scope of the Wireless Local Area Network (WLAN) Client is to describe the security functionality of a WLAN Client in terms of [ ] and to define functional and assurance requirements for such products. This is intended for use with the following s:

- General Purpose Operating System (GPOS) Protection Profile, Version 4.2.1
- Mobile Device Fundamentals (MDF) Protection Profile, Version 3.2

These s are valid because a WLAN Client is a part of either a commercial operating system that can be installed on a general-purpose computer or an operating system that runs on a purpose-built mobile device.

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.
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	The security functionality of the product under evaluation.

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

1.2.2 Technical Terms

Access Point (AP)	A device that provides the network interface that enables wireless client hosts to access a wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between the wireless client and the radio frequency (RF) interface of the AP.
Administrator	A user that has administrative privilege to configure the TOE.
Authentication Credentials	The information the system uses to verify that the user or administrator is authorized to access the TOE or network. Credentials can exist in various forms, such as username/password or digital certificates.
Authentication Server (AS)	A server on the wired network that receives authentication credentials from wireless clients and determines their validity.
Critical Security Parameter (CSP)	Security related information, e.g. secret and private cryptographic keys, and authentication data such as passwords and Personal Identification Numbers (PINs), whose disclosure or modification can compromise the security of a cryptographic module.
Entropy Source	A cryptographic function that provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.
Extensible Authentication Protocol (EAP)	An authentication framework, used in wireless networks, that uses Public Key Infrastructure (PKI) to authenticate both the authentication server and the wireless client.
FIPS-Approved Cryptographic Function	A cryptographic operation that is specified for use by FIPS 140.
IEEE 802.1X	A standard for port-based network access control that defines an authentication mechanism for WLAN Clients to attach to a wired network.
Unauthorized User	A user that has not been granted the ability to use the TOE.

1.3 Compliant Targets of Evaluation

This document specifies SFRs for a WLAN Client. The TOE defined by this is the WLAN Client, a component executing on a client machine (often referred to as a "remote access client"). The TOE establishes a secure wireless tunnel between the client device and a WLAN Access System through which all data will traverse.

A WLAN Client allows remote users to use client machines to establish wireless communication with a private network through a WLAN Access System. IP packets passing between the private network and a WLAN Client are encrypted. The WLAN Client protects the confidentiality and integrity of data in transit between itself and the private network, even though it traverses a wireless connection. The focus of the SFRs in this is on the following fundamental aspects of a WLAN Client:

- Authentication of the WLAN Client
- Authentication of the Authentication Server
- Cryptographic protection of data in transit
- Implementation of services

The WLAN Client establishes an 802.11 tunnel between the client device and the network infrastructure using IEEE 802.1X with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for authentication. It performs mutual authentication to an AS in the private network as part of the EAP-TLS exchange. The EAP-TLS exchange uses certificates for mutual authentication. The WLAN Client examines the machine certificate transmitted from the AS, checks its validity, and ensures the certificate is signed by a trusted Certificate Authority (CA). The AS will authenticate the WLAN Client certificate at the same time. When the EAP-TLS exchange completes successfully, the network allows the WLAN Client to finish establishing a secure

communication tunnel to the private network. The WLAN Client sets up an encrypted, authenticated channel to the WLAN Access System using a 4-way handshake, as specified in IEEE 802.11. Once the channel is established, all communication between the WLAN Client to the WLAN Access System is encrypted with Advanced Encryption Standard (AES) in Cipher Block Chaining-Message Authentication Code Protocol (CCMP) mode and optionally AES in Galois/Counter Mode Protocol (GCMP) mode, as specified in [802.11-2016].

1.3.1 TOE Boundary

The WLAN Client (Figure 1), as defined by this , is a component executing on a remote access client machine. Note the client is depicted as just a small portion of the WLAN client "machine." As such, the TOE must rely heavily on the TOE's operational environment (host platform, network stack, and operating system) for its execution domain and its proper usage. The TOE will rely on the IT environment to address much of the security functionality related to administrative functions.

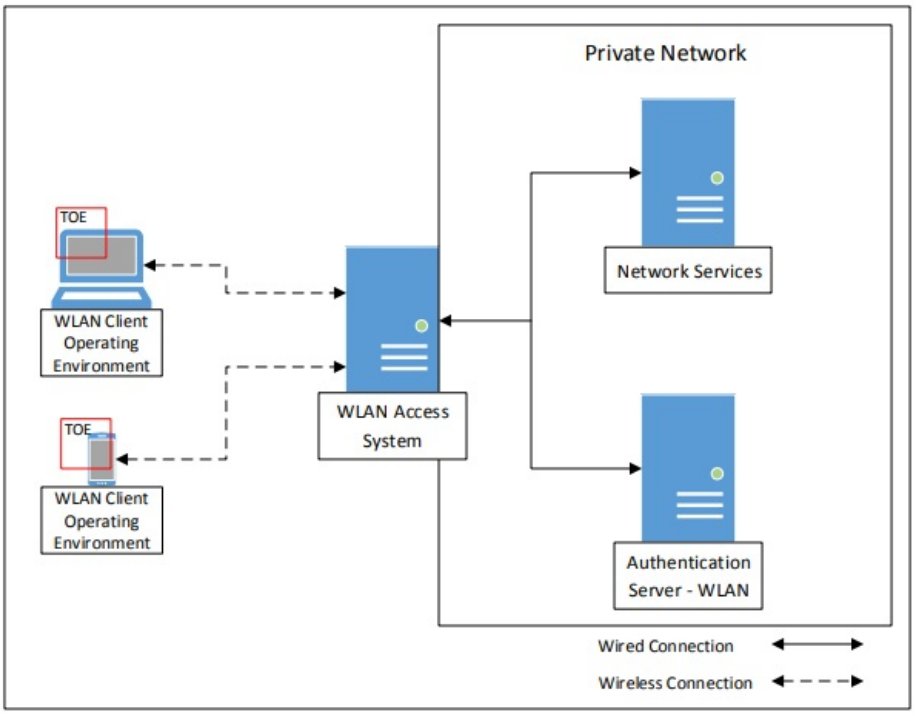


Figure 1: WLAN Client Operating Environment

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problems in at least the following use cases. These use cases are intentionally very broad, as many specific use cases exist within these larger categories.

[USE CASE 1] General-Purpose Operating System

This use case is for a WLAN Client TOE that is part of a general-purpose operating system. Specifically, the WLAN Client TOE is expected to be part of the operating system itself and not a standalone third-party application that is installed on top of it.

[USE CASE 2] Mobile Device

This use case is for a WLAN Client TOE that is part of a mobile operating system that runs on a mobile device. Specifically, the WLAN Client TOE is expected to be part of the mobile operating system itself and not a standalone third-party application that is acquired from the mobile vendor's application store.

2 Conformance Claims

Conformance Statement

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

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

- General Purpose Operating Systems, version 4.2.1
- Mobile Device Fundamentals, version 3.1

CC Conformance Claims

This is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5.

PP Claim

This does not claim conformance to any Protection Profile.

Package Claim

This does not claim conformance to any packages.

Conformance Statement

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

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

- PP-Module for VPN Client, Version 2.2
- PP-Module for MDM Agent, Version 1.0

CC Conformance Claims

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

Package Claims

There are no package claims for this PP-Module.

3 Security Problem Description

This PP-Module is written to address the situation when an entity desires wireless access to a private network. To allow access to the private network, the entity (machine) must be authenticated before a secure communications channel can be established. The TOE is the entity that seeks to be authenticated and be given access to services offered by the protected network and is the Supplicant in the IEEE 802.1X framework.

3.1 Threats

The following threats are specific to WLAN Clients, and represent an addition to those identified in the s.

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.UNAUTHORIZED_ACCESS
A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

T.UNDETECTED_ACTIONS
Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

3.2 Assumptions

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

A.NO_TOE_BYPASS
Information cannot flow between the wireless client and the internal wired network without passing through the .

A.TRUSTED_ADMIN
Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 PP-Module defines no additional Organizational Security Policies.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

O.AUTH_COMM
The will provide a means to ensure that it is communicating with an authorized Access Point and not some other entity pretending to be an authorized Access Point, and will provide assurance to the Access Point of its identity.

O.CRYPTOGRAPHIC_FUNCTIONS
The will provide or use cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the and its host environment.

O.SELF_TEST
The will provide the capability to test some subset of its security functionality to ensure it is operating properly.

O.SYSTEM_MONITORING
The will provide the capability to generate audit data.

O.TOE_ADMINISTRATION
The will provide mechanisms to allow administrators to be able to configure the .

O.WIRELESS_ACCESS_POINT_CONNECTION
The will provide the capability to restrict the wireless access points to which it will connect.

4.2 Security Objectives for the Operational Environment

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

OE.NO_TOE_BYPASS
Information cannot flow between external and internal networks located in different enclaves without passing through the .

OE.TRUSTED_ADMIN
administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.3 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.TSF_FAILURE	O.SELF_TEST	The threat T.TSF_FAILURE is mitigated by O.SELF_TEST as this defines a mechanism for ensuring the reliability of the TSF by detecting potential failure conditions.
T.UNAUTHORIZED_ACCESS	O.AUTH_COMM	The threat T.UNAUTHORIZED_ACCESS is mitigated in part by O.AUTH_COMM by ensuring the authenticity of any remote endpoint that the TSF connects to.
	O.CRYPTOGRAPHIC_FUNCTIONS	The threat T.UNAUTHORIZED_ACCESS is mitigated in part by O.CRYPTOGRAPHIC_FUNCTIONS by ensuring the confidentiality and integrity of data in transit to

		protect against man-in-the-middle attacks.
	O.TOE_ADMINISTRATION	The threat T.UNAUTHORIZED_ACCESS is mitigated in part by O.TOE_ADMINISTRATION by using the TOE platform's authentication mechanism to ensure that only authorized administrators can configure the TOE's behavior.
	O.WIRELESS_ACCESS_POINT_CONNECTION	The threat T.UNAUTHORIZED_ACCESS is mitigated in part by this objective because it provides a mechanism to restrict the remote entities that the TOE is permitted to communicate with.
T.UNDETECTED_ACTIONS	O.SYSTEM_MONITORING	The threat T.UNDETECTED_ACTIONS is mitigated by O.SYSTEM_MONITORING by enforcing an auditing mechanism that can be used to track security-relevant TOE behavior.
A.NO_TOE_BYPASS	OE.NO_TOE_BYPASS	The Operational Environment objective OE.NO_TOE_BYPASS is realized through A.NO_TOE_BYPASS.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	The Operational Environment objective OE.TRUSTED ADMIN is realized through A.TRUSTED_ADMIN.

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 GPOS PP Security Functional Requirements Direction

In a PP-Configuration that includes GPOS PP, the TOE is expected to rely on some of the security functions implemented by the Operating System as a whole and evaluated against the GPOS PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the GPOS PP in addition to what is mandated by Section 5.3 TOE Security Functional Requirements.

5.1.1 Modified SFRs

This PP-Module does not modify any SFRs defined by the GPOS PP.

5.1.2 Additional SFRs

This PP-Module does not define any additional SFRs for any PP-Configuration where the GPOS PP is claimed as the Base-PP.

5.2 MDF PP Security Functional Requirements Direction

In a PP-Configuration that includes MDF PP, the TOE is expected to rely on some of the security functions implemented by the Mobile Device as a whole and evaluated against the MDF PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the MDF PP in addition to what is mandated by Section 5.3 TOE Security Functional Requirements.

5.2.1 Modified SFRs

This PP-Module does not modify any SFRs defined by the MDF PP.

5.2.2 Additional SFRs

This PP-Module does not define any additional SFRs for any PP-Configuration where the MDF PP is claimed as the Base-PP.

5.3 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.

5.3.1 Security Audit (FAU)

FAU_GEN.1/WLAN Audit Data Generation (Wireless LAN)

FAU_GEN.1.1/WLAN

The TSF shall **[selection: *invoke platform-provided functionality, implement functionality*]** to generate an audit record of the following auditable events:

a. Startup and shutdown of the audit functions;
b. All auditable events for [*not specified*] level of audit; and

c. [*all auditable events specified in the Auditable Events table*].

Application Note: If auditing for the WLAN Client cannot be controlled separately from its underlying platform, the "Startup and shutdown of the audit functions" event defined in each Base-PP is sufficient to address that event for this iteration of the SFR.

The Auditable Events table includes auditable events for SFRs that are not mandatory. If the TOE does not claim a particular non-mandatory SFR, it is not expected to generate any corresponding audit records for that SFR.

The Auditable Events table includes auditable events for FPT_TST_EXT.1/WLAN. If the TOE does not perform its own self-tests (i.e., "TOE platform" is selected in FPT_TST_EXT.1.1/WLAN and FPT_TST_EXT.1.2/WLAN), the audit record for this event may also be generated by the TOE platform.

Table2 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/WLAN	None.	
FCS_CKM.1/WLAN	None.	
FCS_CKM.2/WLAN	None.	
FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session.	Reason for failure. Non-TOE endpoint of connection.
	Establishment/termination of an EAP-TLS session.	Non-TOE endpoint of connection.
FCS_TLSC_EXT.2/WLAN	None.	
FIA_PAE_EXT.1	None.	
FIA_X509_EXT.1/WLAN	Failure to validate X.509v3 certificate.	Reason for failure of validation.
FIA_X509_EXT.2/WLAN	None.	
FIA_X509_EXT.4	Attempts to load certificates.	None.
	Attempts to revoke certificates.	None.
FMT_SMF.1/WLAN	None.	
FPT_TST_EXT.1/WLAN	Execution of this set of TSF self-tests.	None.
	[**selection**: *Detected integrity violation.* , *None.*]	[**selection**: *The TSF binary file that caused the integrity violation.* , *None.*]
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to. Success and failures (including reason for failure).
FTP_ITC.1/WLAN	All attempts to establish a trusted channel.	Identification of the non-TOE endpoint of the channel.

FAU_GEN.1.2/WLAN

The **[selection: *TSF, TOE platform*]** shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, (if relevant) the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-**Module**/ST, [*Additional Audit Record Contents as specified in Auditable Events table*].

Evaluation Activities

FAU_GEN.1/WLAN:
TSS
The evaluator shall check the and ensure it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field.

If "invoke platform-provided functionality" is selected, the evaluator shall examine the to verify it describes (for each supported platform) how this functionality is invoked (it should be noted that this may be through a mechanism that is not implemented by the WLAN Client; however, that mechanism will be identified in the as part of this evaluation activity).

Guidance
The evaluator shall check the operational guidance and ensure it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP-Module is described and that the description of the fields contains the information required in FAU_GEN.1.2/WLAN, and the additional information specified in the Auditable Events table.

The evaluator shall in particular ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In the Auditable Events table, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP-Module. The TOE may contain functionality that is not evaluated in the context of this PP-Module because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP-Module, which thus form the set of "all administrative actions". The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.

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

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

5.3.2 Cryptographic Support (FCS)

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

FCS_CKM.1.1/WLAN

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] (as defined in IEEE 802.11-2016)***] 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**.

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 was first defined in IEEE 802.11ac-2014 (Section 11.4.5) but subsequently integrated into 802.11-2016. This protocol requires a key derivation function (KDF) KDF based on HMAC-SHA-256 (for 128-bit symmetric keys) or HMAC-SHA384 (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 Pairwise Temporal Key (PTK) from the PMK, which is done using a random value generated by the RBG specified in this PP-Module, the HMAC function using SHA-1 as specified in this PP-Module, as well as other information. This is specified in 802.11-2012 primarily in section 11.6.1.2.

Evaluation Activities

FCS_CKM.1/WLAN:

TSS

The evaluator shall verify that the TSS describes how the primitives defined and implemented by this PP-Module are used by the TOE in establishing and maintaining secure connectivity to the wireless clients. The TSS shall also provide a description of the developer's method(s) of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also any third-party testing that is performed.

Guidance

There are no guidance evaluation activities for this component.

Tests

The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall configure the access point so the cryptoperiod of the session key is 1 hour. The evaluator shall successfully connect the TOE to the access point and maintain the connection for a length of time that is greater than the configured cryptoperiod. The evaluator shall use a packet capture tool to determine that after the configured cryptoperiod, a re-negotiation is initiated to establish a new session key. Finally, the evaluator shall determine that the renegotiation has been successful and the client continues communication with the access point.*
- ***Test 2:*** *The evaluator shall perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless LAN access point:*

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

  Step 2: The evaluator shall configure the TOE to communicate with a WLAN access point using IEEE 802.11-2016 and a 256-bit (64 hex values 0-f) pre-shared key. The pre-shared key is only used for testing.

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

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

  Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK from the 4-way handshake frames and preshared key as specified in IEEE 802.11-2016.

  Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and access point after the 4-way handshake successfully completed, and without the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the PTK to decrypt the data portion of the packet as specified in IEEE 802.11-2016, and shall verify that the decrypted data contains ASCII-readable text.

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

FCS_CKM.2/WLAN Cryptographic Key Distribution (Group Temporal Key for WLAN)

FCS_CKM.2.1/WLAN

The TSF shall **decrypt Group Temporal Key** in accordance with a specified cryptographic key distribution method [*AES Key Wrap (as defined in RFC 3394) in an EAPOL-Key frame (as defined in IEEE 802.11-2016 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 received by the TOE for use in decrypting broadcast and multicast messages from the Access Point to which it's connected. 802.11-2016 specifies the format for the transfer as well as the fact that it must be wrapped by the AES Key Wrap method specified in RFC 3394; the TOE must be capable of

unwrapping such keys.

Evaluation Activities

FCS_CKM.2/WLAN:
TSS
The evaluator shall check the TSS to ensure that it describes how the GTK is unwrapped prior to being installed for use on the TOE using the AES implementation specified in this PP-Module.

Guidance
There are no guidance evaluation activities for this component.

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

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

Step 2: The evaluator shall configure the TOE to communicate with the access point using IEEE 802.11-2016 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

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

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

Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK and GTK from the 4-way handshake frames and preshared key as specified in IEEE 802.11-2016.

Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and access point after the 4-way handshake successfully completed, and with the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the GTK to decrypt the data portion of the selected packet as specified in IEEE 802.11-2016, and shall verify that the decrypted data contains ASCII-readable text.

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

FCS_TLSC_EXT.1/WLAN TLS Client Protocol (EAP-TLS for WLAN)

FCS_TLSC_EXT.1.1/WLAN

The TSF shall implement TLS 1.2 (RFC 5246) and [**selection**: *TLS 1.1 (RFC 4346), no other TLS version*] in support of the EAP-TLS protocol as specified in RFC 5216 supporting the following cipher suites: [**selection**:

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,*
- *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,*
- *TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246,*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,*
- *TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*

- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

].

Application Note: If any of the ECDHE cipher suites are selected by the ST author, it is necessary to claim the selection-based requirement FCS_TLSC_EXT.2/WLAN.

FCS_TLSC_EXT.1.2/WLAN
The TSF shall generate random values used in the EAP-TLS exchange using the RBG specified in FCS_RBG_EXT.1.

FCS_TLSC_EXT.1.3/WLAN
The TSF shall use X509 v3 certificates as specified in FIA_X509_EXT.1**/WLAN**.

FCS_TLSC_EXT.1.4/WLAN
The TSF shall verify that the server certificate presented includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

FCS_TLSC_EXT.1.5/WLAN
The TSF shall allow an authorized administrator to configure the list of CAs that are allowed to sign authentication server certificates that are accepted by the TOE.

FCS_TLSC_EXT.1.6/WLAN
The TSF shall allow an authorized administrator to configure the list of algorithm suites that may be proposed and accepted during the EAP-TLS exchanges.

Application Note: The cipher suites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the optional cipher suites that are supported. It is necessary to limit the cipher suites that can be used in an evaluated configuration administratively on the server in the test environment.

While FCS_TLSC_EXT.1.4/WLAN requires that the TOE perform certain checks on the certificate presented by the authentication server, there are corresponding checks that the authentication server will have to perform on the certificate presented by the client; namely that the extendedKeyUsage field of the client certificate includes "Client Authentication" and that the digital signature bit (for the Diffie-Hellman cipher suites) or the key encipherment bit (for RSA cipher suites) be set. Certificates obtained for use by the TOE will have to conform to these requirements in order to be used in the enterprise.

The FIA_X509_EXT.1 requirements defined in each of the possible Base-PPs define requirements that the underlying platform is expected to implement.

Evaluation Activities

FCS_TLSC_EXT.1/WLAN:
TSS
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator shall check the TSS to ensure that the cipher suites specified include those listed for this component.

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

The evaluator shall check that the guidance contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange, and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange.

Tests
The evaluator shall write, or the TOE developer shall provide, an application for the purposes of testing TLS.

The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not*

necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

- ***Test 2:*** *The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.*
- ***Test 3:*** *The evaluator shall send a server certificate in the TLS connection that does not match the server-selected cipher suite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite or send a RSA certificate while using one of the ECDSA cipher suites.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.*
- ***Test 4:*** *The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.*
- ***Test 5:*** *The evaluator shall perform the following modifications to the traffic:*
  - *Change the TLS version selected by the server in the Server Hello to a nonsupported TLS version (for example 1.5 represented by the two bytes 03 06) and verify that the client rejects the connection.*
  - *Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE cipher suite) or that the server denies the client's Finished handshake message.*
  - *Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.*
  - *[conditional: the TOE supports at least one cipher suite that uses DHE or ECDHE for key exchange] Modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message. This test does not apply to cipher suites using RSA key exchange.*
  - *Modify a byte in the Server Finished handshake message, and verify that the client sends an Encrypted Message followed by a FIN and ACK message. This is sufficient to deduce that the TOE responded with a Fatal Alert and no further data would be sent.*
  - *Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the client denies the connection.*

5.3.3 Identification and Authentication (FIA)

FIA_PAE_EXT.1 Port Access Entity Authentication

FIA_PAE_EXT.1.1

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

Application Note: This requirement covers the TOE's role as the supplicant in an 802.1X authentication exchange. If the exchange is completed successfully, the TOE will derive the PMK as a result of the EAP-TLS (or other appropriate EAP exchange) and perform the 4-way handshake with the wireless access system (authenticator) to begin 802.11 communications.

As indicated previously, there are at least two communication paths present during the exchange; one with the wireless access system and one with the authentication server that uses the wireless access system as a relay. The TOE establishes an EAP over LAN (EAPOL) connection with the wireless access system as specified in 802.1X-2010. The TOE and authentication server establish an EAP-TLS session (RFC 5216).

The point of performing 802.1X authentication is to gain 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 TOE will gain access to the "controlled port" maintained by the wireless access system.

Evaluation Activities

FIA_PAE_EXT.1:
TSS
There are no TSS evaluation activities for this component.

Guidance

There are no guidance evaluation activities for this component.

Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall demonstrate that the TOE has no access to the test network. After successfully authenticating with an authentication server through a wireless access system, the evaluator shall demonstrate that the TOE does have access to the test network.*
- ***Test 2:*** *The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.*
- ***Test 3:*** *The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid authentication server certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.*

FIA_X509_EXT.1/WLAN X.509 Certificate Validation

FIA_X509_EXT.1.1/WLAN

The TSF shall validate certificates for **EAP-TLS** in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a certificate in the Trust Anchor Database
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/WLAN

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Application Note: FIA_X509_EXT.1/WLAN lists the rules for validating certificates for EAP-TLS. In contrast to FIA_X509_EXT.1 in the Base-PPs, this iteration does not require revocation checking for the EAP-TLS connection used to establish a WiFi connection. The FIA_X509_EXT.1 requirements defined in each of the possible Base-PPs define requirements that the underlying platform is expected to implement in order to support compliance with RFC 5280.

Evaluation Activities

FIA_X509_EXT.1/WLAN:
TSS
The evaluator shall ensure the TSS describes where the check of validity of the EAP-TLS certificates takes place. The evaluator shall also ensure the TSS also provides a description of the certificate path validation algorithm.

Guidance
There are no guidance evaluation activities for this component.

Tests
The tests described must be performed in conjunction with the other Certificate Services assurance activities. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA.

- ***Test 1:*** *The evaluator shall then load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function (e.g. application validation), and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.*
- ***Test 2:*** *The evaluator shall demonstrate that validating an expired certificate results in the function failing.*
- ***Test 3:*** *The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.*
- ***Test 4:*** *The evaluator shall construct a certificate path, such that the certificate of the CA*

issuing the TOE's certificate has the cA flag in the basicConstraints extension not set. The validation of the certificate path fails.

- ***Test 5:*** *The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate (the certificate will fail to parse correctly).*
- ***Test 6:*** *The evaluator shall modify any bit in the last byte of the signature algorithm of the certificate and demonstrate that the certificate fails to validate (the signature on the certificate will not validate).*
- ***Test 7:*** *The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate (the signature on the certificate will not validate).*

FIA_X509_EXT.2/WLAN X.509 Certificate Authentication (EAP-TLS for WLAN)

FIA_X509_EXT.2.1/WLAN

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support [*[authentication for EAP-TLS exchanges]*].

Application Note: RFC 5280 defines certificate validation and certification path validation requirements that must be implemented by the TSF. The FIA_X509_EXT.1 requirements defined in each of the supported Base-PPs define requirements that the underlying platform is expected to implement in order to support compliance with this RFC.

Evaluation Activities

FIA_X509_EXT.2/WLAN:
TSS
The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operational environment so that the TOE can use the certificates.

The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.

Guidance
The evaluator shall check the administrative guidance to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions for configuring the operating environment so that the TOE can use the certificates.

Tests
The evaluator shall perform the following test:

- ***Test 1:*** *The evaluator shall demonstrate using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.*

5.3.4 Security Management (FMT)

FMT_SMF.1/WLAN Specification of Management Functions (WLAN Client)

FMT_SMF.1.1/WLAN

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

- configure security policy for each wireless network:
  - [**selection**: *specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s),, specify the Fully Qualified Domain Names (FQDNs) of acceptable WLAN authentication server certificate(s),*],
  - security type,
  - authentication protocol,
  - client credentials to be used for authentication
- specify wireless networks (SSIDs) to which the TSF may connect

[**selection**:

- *enable/disable certificate revocation list checking,*
- *disable ad hoc wireless client-to-client connection capability,*

- *disable wireless network bridging capability (for example, bridging a connection between the WLAN and cellular radios on a smartphone so it can function as a hotspot),*
- *disable roaming capability,*
- *enable/disable IEEE 802.1X pre-authentication,*
- *loading X.509 certificates into the TOE,*
- *revoke X.509 certificates loaded into the TOE,*
- *enable/disable and configure PMK caching:*
  - *set the amount of time (in minutes) for which PMK entries are cached,*
  - *set the maximum number of PMK entries that can be cached*

  ,
- *no other management functions*

].

Application Note: For installation, the WLAN Client relies on the underlying platform to authenticate the administrator to the client machine on which the TOE is installed.

For the function "configure the cryptoperiod for the established session keys," the unit of measure for configuring the cryptoperiod shall be no greater than an hour. For example: units of measure in seconds, minutes and hours are acceptable and units of measure in days or greater are not acceptable.

Items in the selection are equivalent to ‘OO’ in the GPOS PP and ‘OOOO’ in MDF PP.

Evaluation Activities

FMT_SMF.1/WLAN:
TSS
There are no TSS evaluation activities for this component.

Guidance
The evaluator shall check the operational guidance to verify that every management function claimed by the TOE is described there. The evaluator shall also verify that these descriptions include the information required to perform the management duties associated with the function.

Tests
The evaluator shall test the TOE’s ability to provide the management functions by configuring the TOE and performing the management activities associated with each function claimed in the SFR.

Note that this may be accomplished in conjunction with the testing of other requirements, such as FCS_TLSC_EXT.1/WLAN and FTA_WSE_EXT.1.

5.3.5 Protection of the TSF (FPT)

FPT_TST_EXT.1/WLAN TSF Cryptographic Functionality Testing (WLAN Client)

FPT_TST_EXT.1.1/WLAN

The [**selection**: *TOE*, *TOE platform*] shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2/WLAN

The [**selection**: *TOE*, *TOE platform*] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

Application Note: While the TOE is defined as a software package running on a platform defined by the claimed Base-PP, it is still capable of performing the self-test activities required above. However, if the cryptographic algorithm implementation is provided by the underlying platform, it may be the case where the TSF self-testing is a check to verify that the underlying platform has successfully completed its own self-tests prior to the TSF attempting to use the implementation. It should be understood that there is a significant dependency on the host platform in assessing the assurance provided by these self-tests since a compromise of the underlying platform could potentially result in the self-tests functioning incorrectly.

Evaluation Activities

FPT_TST_EXT.1/WLAN:
TSS
The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.

Guidance
The evaluator shall ensure that the operational guidance describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.

Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall perform the integrity check on a known good TSF executable and verify that the check is successful.*
- ***Test 2:*** *The evaluator shall modify the TSF executable, perform the integrity check on the modified TSF executable, and verify that the check fails.*

5.3.6 TOE Access (FTA)

FTA_WSE_EXT.1 Wireless Network Access

FTA_WSE_EXT.1.1

The TSF shall be able to attempt connections only to wireless networks specified as acceptable networks as configured by the administrator in FMT_SMF.1.1/WLAN.

Application Note: The intent of this requirement is to allow the administrator to limit the wireless networks to which the TOE is allowed to connect.

Evaluation Activities

FTA_WSE_EXT.1:
TSS
The evaluator shall examine the TSS to determine it defines SSIDs as the attribute used to specify acceptable networks.

Guidance
The evaluator shall examine the operational guidance to determine that it contains guidance for configuring the list of SSIDs that the WLAN Client is able to connect to.

Tests
The evaluator shall perform the following tests for each attribute:

- ***Test 1:*** *The evaluator shall configure the TOE to allow a connection to a wireless network with a specific SSID. The evaluator shall also configure the test environment such that the allowed SSID and an SSID that is not allowed are both "visible" to the TOE. The evaluator shall demonstrate that they can successfully establish a connection with the allowed SSID. The evaluator shall then attempt to establish a session with the disallowed SSID and observe that the attempt fails.*

5.3.7 Trusted Path/Channels (FTP)

FTP_ITC.1/WLAN Trusted Channel Communication (Wireless LAN)

FTP_ITC.1.1/WLAN

The TSF shall **use 802.11-2016, 802.1X, and EAP-TLS** to provide a **trusted** communication channel between itself and **a wireless access point** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/WLAN

The TSF shall permit [*the TSF*] to initiate communication via the trusted

channel.

FTP_ITC.1.3/WLAN

The TSF shall initiate communication via the trusted channel for [*wireless access point connections*].

Application Note: The intent of the above requirement is to use the cryptographic protocols identified in the requirement to protect communications between the TOE and the Access Point.

The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage. It may be the case that some part of the TOE setup involves manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to re-establish the communication automatically with (the necessary) manual intervention, there may be a window created where an attacker might be able to gain critical information or compromise a connection. The following tests are only intended to cover the WLAN communication channel (not other communication channels that may be available on the TOE such as mobile broadband).

Evaluation Activities

FTP_ITC.1/WLAN:
TSS
The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to an access point in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Guidance
The evaluator shall confirm that the operational guidance includes instructions for establishing the connection to the access point and that it includes recovery instructions should a connection be unintentionally broken.

Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall ensure that the TOE is able to initiate communications with an access point using the protocols specified in the requirement by setting up the connections as described in the operational guidance and ensuring that communications are successful.*
- ***Test 2:*** *The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- ***Test 3:*** *The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.*
- ***Test 4:*** *The evaluators shall physically interrupt the connection from the TOE to the access point (e.g., moving the TOE host out of range of the access point, turning the access point off). The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.*

Further evaluation activities are associated with the specific protocols.

5.4 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.AUTH_COMM	FCS_TLSC_EXT.1/WLAN, FIA_PAE_EXT.1, FIA_X509_EXT.1/WLAN, FIA_X509_EXT.2/WLAN, FTP_ITC.1/WLAN, FCS_TLSC_EXT.2/WLAN (selection-based)	FCS_TLSC_EXT.1/WLAN supports the objective by requiring the TSF to use EAP-TLS to establish a secure connection to a wireless access point, including authentication of the access point. FIA_PAE_EXT.1 supports the objective by requiring the TSF to act as the supplicant for 802.1X authentication.

		FIA_X509_EXT.1/WLAN supports the objective by defining how the TSF determines the validity of presented X.509 certificates. FIA_X509_EXT.2/WLAN supports the objective by requiring the TSF to implement X.509 certificate authentication as the mechanism for authentication EAP-TLS connections. FTP_ITC.1/WLAN supports the objective by requiring the TSF to implement trusted protocols that include authentication of the remote endpoints. FCS_TLSC_EXT.2/WLAN supports the objective by optionally requiring the TSF to support only certain elliptic curves if the TOE implements any EAP-TLS cipher suites that rely on ECDHE as the key establishment method.
O.CRYPTOGRAPHIC_FUNCTIONS	FCS_CKM.1/WLAN, FCS_CKM.2/WLAN	FCS_CKM.1/WLAN supports the objective by requiring the TSF to generate symmetric keys used for WPA2 in a specified manner. FCS_CKM.2/WLAN supports the objective by requiring the TSF to decrypt group temporal keys used for IEEE 802.11.
O.SELF_TEST	FPT_TST_EXT.1/WLAN	FPT_TST_EXT.1/WLAN supports the objective by requiring the TSF to perform self-tests to ensure that it is operating in a known state.
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	FMT_SMF.1/WLAN, FIA_X509_EXT.4 (optional)	FMT_SMF.1/WLAN supports the objective by requiring the TSF to implement management functionality for security-relevant WLAN behavior. FIA_X509_EXT.4 supports the objective by optionally requiring the TSF to securely store certificates in a repository that an administrator can interact with.
O.WIRELESS_ACCESS_POINT_CONNECTION	FTA_WSE_EXT.1	FTA_WSE_EXT.1 supports the objective by requiring the TSF to restrict connectivity to allowed wireless networks.

a

6 Consistency Rationale

6.1 Protection Profile for General Purpose Operating Systemss

6.1.1 Consistency of TOE Type

When this is used to extend the GPOS PP, the TOE type for the overall TOE is still a general-purpose operating system. The TOE boundary is simply extended to include the WLAN Client functionality that runs on the operating system.

6.1.2 Consistency of Security Problem Definition

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

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_FAILURE	The Base-PP defines threats for local attacks and remote attacks, both of which could cause a failure of the TSF. This PP-Module adds a generic TSF failure threat in the event that the WLAN Client fails through unintended system behavior rather than a direct malicious attack.
T.UNAUTHORIZED_ACCESS	The Base-PP defines threats for local attacks and remote attacks. The threat of unauthorized access to the WLAN Client is a specific threat that results from successful exploitation of one of these Base-PP threats.
T.UNDETECTED_ACTIONS	The Base-PP defines threats for local attacks and remote attacks. It does not define a threat specifically for undetected actions but it does map the local attack and remote attack threats to a TOE objective for accountability. Therefore, the threat of undetected actions is consistent with the Base-PP because this is a subset of the threats defined in the Base-PP, or a mechanism to increase the likelihood that these threats will successfully be exploited.
A.NO_TOE_BYPASS	This assumption relates to the deployment of the TOE in relation to the network resources that it interacts with. It does not enforce any restrictions on the TOE's deployment that are contrary to what the Base-PP requires.
A.TRUSTED_ADMIN	The Base-PP defines A.PROPER_USER and A.PROPER_ADMIN objectives that serve the same purpose as OE.TRUSTED_ADMIN in this PP-Module.

6.1.3 Consistency of Objectives

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

PP-Module TOE Objective	Consistency Rationale
O.AUTH_COMM	This objective is specifically for a communications interface that is defined by the PP-Module, but it is consistent with the general O.PROTECTED_COMMS objective specified in the Base-PP.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE implements this objective in part by relying on the cryptographic functionality specified in the Base-PP to address the Base-PP's O.PROTECTED_COMMS objective. The PP-Module uses these cryptographic functions for the same purpose as the Base-PP.
O.SELF_TEST	The Base-PP defines a general O.INTEGRITY objective; this PP-Module defines O.SELF_TEST as a specific method of guaranteeing the integrity of the TOE.
O.SYSTEM_MONITORING	The Base-PP defines an O.ACCOUNTABILITY objective for system auditing. The O.SYSTEM_MONITORING objective in this PP-Module serves the same purpose.
O.TOE_ADMINISTRATION	The Base-PP defines an O.MANAGEMENT objective for TOE administration. The O.TOE_ADMINISTRTION objective in this PP-Module serves the same purpose.
O.WIRELESS_ACCESS_POINT_CONNECTION	This objective relates to behavior that applies to a communications interface defined in this PP-Module and therefore does not relate to the Base-PP's functionality.

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

PP-Module Operational Environment Objective	Consistency Rationale
OE.NO_TOE_BYPASS	This objective relates to the deployment of the TOE in relation to the network resources that it interacts with. It does not enforce any restrictions on the TOE's deployment that are contrary to what the Base-PP requires.
OE.TRUSTED_ADMIN	The Base-PP defines OE.PROPER_USER and OE.PROPER_ADMIN objectives that serve the same purpose as OE.TRUSTED_ADMIN in this PP-Module.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the GPOS PP that are needed to support WLAN Clients functionality. This is considered to be consistent because the functionality provided by the GPOS PP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the GPOS PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
This PP-Module does not modify any requirements when the GPOS PP is the base.	
Mandatory SFRs	
FAU_GEN.1/WLAN	The Base-PP defines its own auditing mechanism; this PP-Module can use that mechanism or implement its own to generate audit records for security-relevant events that are specific to this PP-Module.
FCS_CKM.1/WLAN	This SFR requires the TOE to generate cryptographic keys that are only used by the PP-Module's functionality. It invokes Base-PP functionality to do this in a manner that the Base-PP permits.
FCS_CKM.2/WLAN	This SFR requires the TOE to perform a decryption operation using AES Key Wrap, which is a function that the Base-PP provides.
FCS_TLSC_EXT.1/WLAN	This SFR requires the TOE to implement EAP-TLS; this protocol relies on the same cryptographic functionality that the Base-PP uses to implement TLS.
FIA_PAE_EXT.1	This SFR defines the ability of the TOE to implement IEEE 802.1X. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FIA_X509_EXT.1/WLAN	This SFR defines the TOE's X.509 certificate validation specifically when validating EAP-TLS certificates. The Base-PP also defines an iteration of this SFR but the PP-Module requires a separate iteration because EAP-TLS certificates have specific handling requirements that are not present in the Base-PP because the Base-PP does not define implementation of the EAP-TLS protocol.
FIA_X509_EXT.2/WLAN	This SFR defines the TOE's use of X.509 certificates in EAP-TLS. This function uses the same certificate validation functionality that the Base-PP defines.
FMT_SMF.1/WLAN	This SFR defines the management activities that are specific to this PP-Module. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FPT_TST_EXT.1/WLAN	This SFR defines self-test behavior for the WLAN Client. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FTA_WSE_EXT.1	This SFR requires the TOE to restrict the wireless networks that it can connect to. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FTP_ITC.1/WLAN	This SFR defines the protocols that the TOE uses for secure wireless communications. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
Optional SFRs	

FIA_X509_EXT.4	This SFR defines behavior for implementing certificate storage. As this function is optional, it does not interfere with any certificate storage mechanism enforced by the Base-PP.
Selection-based SFRs	
FCS_TLSC_EXT.2/WLAN	This SFR requires the TOE to validate a specific TLS extension when establishing EAP-TLS communications. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-Dependent SFRs	
This PP-Module does not define any Implementation-Dependent requirements.	

6.2 Protection Profile for Mobile Device Fundamentalss

6.2.1 Consistency of TOE Type

When this is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. The TOE boundary is simply extended to include the WLAN Client functionality that runs on the mobile device's Rich OS.

6.2.2 Consistency of Security Problem Definition

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

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_FAILURE	The Base-PP defines the T.FLAWAPP threat for the threat that application failures may pose to the device as a whole. The T.TSF_FAILURE threat from this PP-Module is a specific example of the T.FLAWAPP threat, though it relates to the WLAN Client as an intrinsic part of the mobile device rather than a third-party application installed on top of it. The Base-PP also defines the T.PERSISTENT threat, which is another specific case of TSF failure.
T.UNAUTHORIZED_ACCESS	The Base-PP defines threats for network eavesdropping and network attacks. Exploiting either threat could allow an attacker to exploit the T.UNAUTHORIZED_ACCESS threat defined by this PP-Module.
T.UNDETECTED_ACTIONS	The Base-PP defines threats for persistent access to the TOE and flawed applications on the TOE. It does not define a threat specifically for undetected actions but the threat of undetected actions defined by this PP-Module could increase the likelihood that the Base-PP threats can be successfully exploited.
A.NO_TOE_BYPASS	This assumption relates to the deployment of the TOE in relation to the network resources that it interacts with. It does not enforce any restrictions on the TOE's deployment that are contrary to what the Base-PP requires.
A.TRUSTED_ADMIN	The Base-PP defines the OE.CONFIG objective that expects administrators will configure the TOE correctly, which also implies they are non-malicious.

6.2.3 Consistency of Objectives

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

PP-Module TOE Objective	Consistency Rationale
O.AUTH_COMM	This objective is specifically for a communications interface that is defined by the PP-Module, but it is consistent with the general O.COMMS objective specified in the Base-PP.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE implements this objective in part by relying on the cryptographic functionality specified in the Base-PP to address the Base-PP's O.COMMS objective. The PP-Module uses these cryptographic functions for the same purpose as the Base-PP.
O.SELF_TEST	The Base-PP defines a general O.INTEGRITY objective; this PP-Module defines O.SELF_TEST as a specific method of

	guaranteeing the integrity of the TOE.
O.SYSTEM_MONITORING	The Base-PP defines an O.INTEGRITY objective that includes system auditing as a method of asserting the TOE's integrity. The O.SYSTEM_MONITORING objective in this PP-Module serves the same purpose.
O.TOE_ADMINISTRATION	The Base-PP defines an O.CONFIG objective for TOE administration. The O.TOE_ADMINISTRTION objective in this PP-Module serves the same purpose.
O.WIRELESS_ACCESS_POINT_CONNECTION	This objective relates to behavior that applies to a communications interface defined in this PP-Module and therefore does not relate to the Base-PP's functionality.

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

PP-Module Operational Environment Objective	Consistency Rationale
OE.NO_TOE_BYPASS	This objective relates to the deployment of the TOE in relation to the network resources that it interacts with. It does not enforce any restrictions on the TOE's deployment that are contrary to what the Base-PP requires.
OE.TRUSTED_ADMIN	The Base-PP defines the OE.CONFIG objective that expects administrators will configure the TOE correctly, which also implies they are non-malicious.

6.2.4 Consistency of Requirements

This PP-Module identifies several SFRs from the MDF PP that are needed to support WLAN Clients functionality. This is considered to be consistent because the functionality provided by the MDF PP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the MDF PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
This PP-Module does not modify any requirements when the MDF PP is the base.	
Mandatory SFRs	
FAU_GEN.1/WLAN	The Base-PP defines its own auditing mechanism; this PP-Module can use that mechanism or implement its own to generate audit records for security-relevant events that are specific to this PP-Module.
FCS_CKM.1/WLAN	This SFR requires the TOE to generate cryptographic keys that are only used by the PP-Module's functionality. It invokes Base-PP functionality to do this in a manner that the Base-PP permits.
FCS_CKM.2/WLAN	This SFR requires the TOE to perform a decryption operation using AES Key Wrap, which is a function that the Base-PP provides.
FCS_TLSC_EXT.1/WLAN	This SFR requires the TOE to implement EAP-TLS; this protocol relies on the same cryptographic functionality that the Base-PP uses to implement TLS.
FIA_PAE_EXT.1	This SFR defines the ability of the TOE to implement IEEE 802.1X. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FIA_X509_EXT.1/WLAN	This SFR defines the TOE's X.509 certificate validation specifically when validating EAP-TLS certificates. The Base-PP also defines an iteration of this SFR but the PP-Module requires a separate iteration because EAP-TLS certificates have specific handling requirements that are not present in the Base-PP because the Base-PP does not define implementation of the EAP-TLS protocol.
FIA_X509_EXT.2/WLAN	This SFR defines the TOE's use of X.509 certificates in EAP-TLS. This function uses the same certificate validation functionality that the Base-PP defines.
FMT_SMF.1/WLAN	This SFR defines the management activities that are specific to this PP-Module. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.

FPT_TST_EXT.1/WLAN	This SFR defines self-test behavior for the WLAN Client. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FTA_WSE_EXT.1	This SFR requires the TOE to restrict the wireless networks that it can connect to. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
FTP_ITC.1/WLAN	This SFR defines the protocols that the TOE uses for secure wireless communications. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
Optional SFRs	
FIA_X509_EXT.4	This SFR defines behavior for implementing certificate storage. As this function is optional, it does not interfere with any certificate storage mechanism enforced by the Base-PP.
Selection-based SFRs	
FCS_TLSC_EXT.2/WLAN	This SFR requires the TOE to validate a specific TLS extension when establishing EAP-TLS communications. This behavior relates entirely to the PP-Module and does not affect the ability of the Base-PP to implement its security functionality.
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

A.1.1 Identification and Authentication (FIA)

FIA_X509_EXT.4 X.509 Certificate Storage and Management

FIA_X509_EXT.4.1

The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.4.2

The TSF shall provide the capability for authorized administrators to load X.509v3 certificates into the TOE for use by the TSF.

Application Note: This SFR may be included if the TOE includes the capability to store and manage certificates. Note that this is intended to be used if the certificate storage capability is actually provided by the TOE and not in cases where the TSF is relying on a storage mechanism that is part of the underlying platform.

Evaluation Activities

FIA_X509_EXT.4:
TSS
The evaluator shall examine the TSS to determine that it describes all certificate stores implemented that contain certificates used to meet the requirements of this PP-Module. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access.

Guidance
The evaluator shall check the administrative guidance to ensure that it describes how to load X.509 certificates into the TOE's certificate store.

Tests
The evaluator shall perform the following test for each TOE function that requires the use of certificates:

- ***Test 1:*** *The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. The evaluator shall then load any certificates needed to validate the certificate to be used in the function and demonstrate that the function succeeds. The evaluator then shall delete one of these dependent certificates and show that the function fails.*

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

Appendix B - Selection-based Requirements

B.1 Cryptographic Support (FCS)

FCS_TLSC_EXT.2/WLAN TLS Client Support for Supported Groups Extension (EAP-TLS for WLAN)

FCS_TLSC_EXT.2.1/WLAN

The TSF shall present the Supported Groups extension in the Client Hello with the following NIST curves: [**selection**: *secp256r1*, *secp384r1*, *secp521r1*].

Application Note: This requirement must be claimed if any cipher suites beginning with 'TLS_ECDHE' are selected in FCS_TLSC_EXT.1.1/WLAN.

This requirement does not limit the elliptic curves the client may propose for authentication and key agreement. Rather, it asks the ST author to define which of the NIST curves from FCS_COP.1(3) (defined in each supported Base-PP) and FCS_CKM.1/WLAN and FCS_CKM.2/WLAN (each defined in this PP-Module) can be used for TLS key establishment.

Evaluation Activities

FCS_TLSC_EXT.2/WLAN:

TSS

The evaluator shall verify that the TSS describes the Supported Groups extension and whether the required behavior is performed by default or may be configured.

Guidance

If the TSS indicates that the Supported Groups extension must be configured to meet the requirement, the evaluator shall verify that the operational guidance includes instructions for configuration of this extension.

Tests

The evaluator shall perform the following test:

- ***Test 1:*** *The evaluator shall configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.*

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

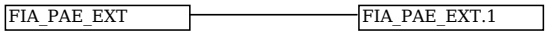
Functional Class	Functional Components

C.2 Extended Component Definitions

FIA_PAE_EXT Port Access Entity Authentication

Family Behavior

Components in this family define requirements for TOE support of IEEE 802.1X authentication.



Component Leveling

FIA_PAE_EXT.1, Port Access Entity Authentication, describes the ability of the TOE to act as a supplicant for 802.1X authentication.

Management: FIA_PAE_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable IEEE 802.1X pre-authentication.
- Enable/disable PMK caching.
- Set the amount of time (in minutes) for which PMK entries are cached.
- Set the maximum number of PMK entries that can be cached.

Audit: FIA_PAE_EXT.1

There are no auditable events foreseen.

FIA_PAE_EXT.1 Port Access Entity Authentication

Hierarchical to: No other components.

Dependencies to: No dependencies.

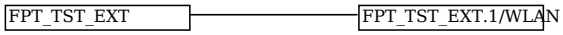
FIA_PAE_EXT.1.1

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

FPT_TST_EXT TSF Self-Test

Family Behavior

Components in this family define requirements for self-testing to verify the functionality and integrity of the TOE.



Component Leveling

FPT_TST_EXT.1/WLAN, TSF Cryptographic Functionality Testing (WLAN Client), requires the TOE to perform power on self-tests to verify its functionality and the integrity of its stored executable code.

Management: FPT_TST_EXT.1/WLAN

The following actions could be considered for the management functions in FMT:

- Specification of CAs that are authorized to sign authentication server certificates.
- Specification of proposed and accepted algorithm suites.

Audit: FPT_TST_EXT.1/WLAN

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Execution of TSF self-tests.
- Basic: Detected integrity violation.

FPT_TST_EXT.1/WLAN TSF Cryptographic Functionality Testing (WLAN Client)

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FPT_TST_EXT.1.1/WLAN

The [**selection**: *TOE*, *TOE platform*] shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

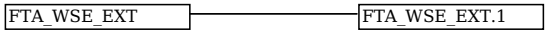
FPT_TST_EXT.1.2/WLAN

The [**selection**: *TOE*, *TOE platform*] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

FTA_WSE_EXT Wireless Network Access

Family Behavior

Components in this family define requirements for specifying wireless networks that the TOE can connect to.



Component Leveling

FTA_WSE_EXT.1, Wireless Network Access, describes the ability of the TOE to apply administrative limits on the wireless networks that it can connect to.

Management: FTA_WSE_EXT.1

The following actions could be considered for the management functions in FMT:

- Specify allowed wireless networks based on MAC Access, Service Set Identifier (SSID), or other attributes.

Audit: FTA_WSE_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: All attempts to connect to access points.

FTA_WSE_EXT.1 Wireless Network Access

Hierarchical to: No other components.

Dependencies to: FMT_SMF.1 Specification of Management Functions

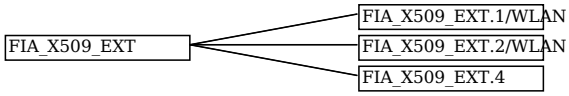
FTA_WSE_EXT.1.1

The TSF shall be able to attempt connections only to wireless networks specified as acceptable networks as configured by the administrator in FMT_SMF.1.1/WLAN.

FIA_X509_EXT X.509 Certificate Use and Management

Family Behavior

Components in this family define requirements for the use of X.509 certificates.



Component Leveling

FIA_X509_EXT.1/WLAN, X.509 Certificate Validation,

Management: FIA_X509_EXT.1/WLAN

There are no management functions foreseen.

Audit: FIA_X509_EXT.1/WLAN

There are no audit events foreseen.

FIA_X509_EXT.1/WLAN X.509 Certificate Validation

Hierarchical to: No other components.

Dependencies to: No dependencies.

FIA_X509_EXT.1.1/WLAN

The TSF shall validate certificates for **EAP-TLS** in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a certificate in the Trust Anchor Database
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/WLAN

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Component Leveling

FIA_X509_EXT.2/WLAN, X.509 Certificate Authentication (EAP-TLS for WLAN),

Management: FIA_X509_EXT.2/WLAN

There are no management functions foreseen.

Audit: FIA_X509_EXT.2/WLAN

There are no audit events foreseen.

FIA_X509_EXT.2/WLAN X.509 Certificate Authentication (EAP-TLS for WLAN)

Hierarchical to: No other components.

Dependencies to: No dependencies.

FIA_X509_EXT.2.1/WLAN

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support [*[authentication for EAP-TLS exchanges]*].

Component Leveling

FIA_X509_EXT.4, X.509 Certificate Storage and Management, requires the TOE to implement the ability to store X.509 certificates.

Management: FIA_X509_EXT.4

The following actions could be considered for the management functions in FMT:

- Loading of X.509 certificates into the TOE.
- Revocation of loaded X.509 certificates.

Audit: FIA_X509_EXT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Attempts to load certificates.
- Basic: Attempts to revoke certificates.

FIA_X509_EXT.4 X.509 Certificate Storage and Management

Hierarchical to: No other components.

Dependencies to: No dependencies.

FIA_X509_EXT.4.1

The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

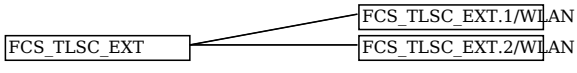
FIA_X509_EXT.4.2

The TSF shall provide the capability for authorized administrators to load X.509v3 certificates into the TOE for use by the TSF.

FCS_TLSC_EXT TLS Client Protocol

Family Behavior

Components in this family define requirements for the implementation of the TLS protocol when the TOE is acting as a client.



Component Leveling

FCS_TLSC_EXT.1/WLAN, TLS Client Protocol (EAP-TLS for WLAN), describes the ability of the TOE to implement the EAP-TLS protocol as a client.

Management: FCS_TLSC_EXT.1/WLAN

There are no specific management functions identified.

Audit: FCS_TLSC_EXT.1/WLAN

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: All attempts to establish a trusted channel.
- Basic: Detection of modification of channel data.

FCS_TLSC_EXT.1/WLAN TLS Client Protocol (EAP-TLS for WLAN)

Hierarchical to: No other components.

Dependencies to: FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Distribution

FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation

FIA_X509_EXT.1 X.509 Certificate Validation

FMT_SMR.1 Security Roles

FCS_TLSC_EXT.1.1/WLAN

The TSF shall implement TLS 1.2 (RFC 5246) and [**selection**: *TLS 1.1 (RFC 4346), no other TLS version*] in support of the EAP-TLS protocol as specified in RFC 5216 supporting the following cipher suites: [**assignment**: *list of supported cipher suites*].

FCS_TLSC_EXT.1.2/WLAN

The TSF shall generate random values used in the EAP-TLS exchange using the RBG specified in FCS_RBG_EXT.1.

FCS_TLSC_EXT.1.3/WLAN

The TSF shall use X509 v3 certificates as specified in FIA_X509_EXT.1.

FCS_TLSC_EXT.1.4/WLAN

The TSF shall verify that the server certificate presented includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

FCS_TLSC_EXT.1.5/WLAN

The TSF shall allow an authorized administrator to configure the list of CAs that are allowed to sign authentication server certificates that are accepted by the TOE.

FCS_TLSC_EXT.1.6/WLAN

The TSF shall allow an authorized administrator to configure the list of algorithm suites that may be proposed and accepted during the EAP-TLS exchanges.

Component Leveling

FCS_TLSC_EXT.2/WLAN, TLS Client Support for Supported Groups Extension (EAP-TLS for WLAN), describes the ability of the TOE to present certain values in the Supported Groups extension when attempting to establish a TLS connection as a client.

Management: FCS_TLSC_EXT.2/WLAN

There are no specific management functions identified.

Audit: FCS_TLSC_EXT.2/WLAN

There are no auditable events foreseen.

FCS_TLSC_EXT.2/WLAN TLS Client Support for Supported Groups Extension (EAP-TLS for WLAN)

Hierarchical to: No other components.

Dependencies to: FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.2.1/WLAN

The TSF shall present the Supported Groups extension in the Client Hello with the following NIST curves: [**assignment**: *list of supported groups*].

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, SFRs inherited from the Base-PPs, or SFRs that are hierarchical to the listed dependency.

Appendix E - 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-PPs.

Appendix F - 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.
[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.
[CEM]	Common Evaluation Methodology for Information Technology Security - Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017.
[GPOS]	Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
[MDF]	Protection Profile for Mobile Device Fundamentals, Version 3.2, March 4, 2021
[802.11-2016]	802.11-2016 - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[802.11-2016]	802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control
[RFC 3394]	RFC 3394 - Advanced Encryption Standard (AES) Key Wrap Algorithm
[RFC 4346]	RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1
[RFC 5216]	RFC 5216 - The EAP-TLS Authentication Protocol
[RFC 5246]	RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2
[RFC 5280]	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Appendix G - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AP	Access Point
AS	Authentication Server
Base-PP	Base Protection Profile
CA	Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMP	Counter mode CBC-MAC Protocol
CCTL	Common Criteria Test Laboratory
CEM	Common Evaluation Methodology
CSP	Critical Security Parameter
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GPOS	General-Purpose Operating System
GTK	Group Temporal Key
HMAC	Hash-Based Message Authentication Code
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
KDF	Key Derivation Function
LAN	Local Area Network
MAC	Message Authentication Code (cryptography) or Media Control Address (system property)
MDF	Mobile Device Fundamentals
NIAP	National Information Assurance Partnership
NVLAP	National Voluntary Laboratory Accreditation Program
OE	Operational Environment
OSP	Organizational Security Policy
PAE	Port Access Entity
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PP	Protection Profile
PP	Protection Profile

PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
PRF	Pseudo-Random Function
PTK	Pairwise Temporal Key
RBG	Random Bit Generator
RF	Radio Frequency
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
ST	Security Target
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TOE	Target of Evaluation
TSF	TOE Security Function
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
TSS	TOE Summary Specification
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access