Supporting Document
Mandatory Technical Document

PP-Module for WLAN Clients
Version: 1.0
2021-03-15
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2021-03-15	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of WLAN Clients products.

Acknowledgments:
This SD was developed with support from NIAP WLAN Clients Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for WLAN Clients is to describe the security functionality of WLAN Clients products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PPs:

- Protection Profile for General Purpose Operating Systemss, Version 4.2.1
- Protection Profile for Mobile Device Fundamentalss, Version 3.1

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- WLAN Clients, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.

Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 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.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for General Purpose Operating Systemss

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the GPOS PP.

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the GPOS PP is the base.

2.2 Protection Profile for Mobile Device Fundamentalss

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the MDF PP.

2.2.1 Modified SFRs

The PP-Module does not modify any requirements when the MDF PP is the base.

2.3 TOE SFR Evaluation Activities

2.3.1 Security Audit (FAU)

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

FAU_GEN.1/WLAN
TSS
The evaluator shall check the TSS 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 TSS 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 TSS 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.

2.3.2 Cryptographic Support (FCS)

FCS_CKM.1/WPA3 Cryptographic Key Generation (Symmetric Keys for WPA3 Connections)

FCS_CKM.1/WPA3
TSS
Placeholder

Guidance
Placeholder

Tests
Placeholder

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

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 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and 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 pre-shared key as specified in IEEE 802.11-2012.

Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and 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 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text.

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

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

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 unsupported 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: if 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.

FCS_WPA_EXT.1 Supported WPA Versions

FCS_WPA_EXT.1

2.3.3 Identification and Authentication (FIA)

FIA_PAE_EXT.1 Port Access Entity Authentication

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/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/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.

Guidance
If not already present in the TSS, 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.

If the administrator is able to specify the action to be performed in this situation, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.

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.

FIA_X509_EXT.4 X.509 Certificate Storage and Management

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.

If the TOE relies on a platform mechanism for certificate loading and storage, the evaluator shall verify that the TSS identifies this mechanism and describes how use of this mechanism is protected against 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, regardless of whether the TSF provides this mechanism itself or the TOE relies on a platform-provided mechanism for this.

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 shall then delete one of these dependent certificates and show that the function fails.
- **Test 2:** The evaluator shall demonstrate that the mechanism used to load or configure X.509 certificates cannot be accessed without appropriate authorization.

2.3.4 Security Management (FMT)

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

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.

2.3.5 Protection of the TSF (FPT)

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

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.

2.3.6 TOE Access (FTA)

FTA_WSE_EXT.1 Wireless Network Access

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.

2.3.7 Trusted Path/Channels (FTP)

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

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.

2.4 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.5 Evaluation Activities for Selection-Based SFRs

2.5.1 Cryptographic Support (FCS)

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

FCS_CKM.1/WPA2
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 802.11-2012 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 pre-shared key as specified in IEEE 802.11-2012.

Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and 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 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text.

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

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

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.

2.6 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base-PP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against the Base-PP as well. The Base-PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

Identifier	Title
[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
[802.11-2012]	802.11-2012 - 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
[802.1X-2020]	802.1X-2020 - 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