Supporting Document
Mandatory Technical Document

PP-Module for Wireless Local Area Network (WLAN) Access System
Version: 1.0
2022-03-11
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	2022-03-11	Initial Release
0.5	2022-01-20	Conversion to PP-Module; Updated to include WPA 3 and Wi-Fi 6. WPA 3 is required. WPA 2 can additionally be included in the ST. 256 bit keys are required. 128 and 192 bit keys can additionally be included in the ST. Mandated Distributed TOE

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Wireless Local Area Network (WLAN) Access System products.

Acknowledgments:
This SD was developed with support from NIAP Wireless Local Area Network (WLAN) Access System 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
1.2 Structure of the Document
1.3 Terms
1.3.1 Common Criteria Terms
1.3.2 Technical Terms
2 Evaluation Activities for SFRs

2.1 Collaborative Protection Profile for NDs
2.1.1 Modified SFRs
2.1.1.1 Cryptographic Support (FCS)
2.1.1.2 Protection of the TSF (FPT)
2.1.1.3 Trusted Path/Channels (FTP)
2.1.1.4 Security Audit (FAU)
2.1.1.5 Communication (FCO)
2.2 TOE SFR Evaluation Activities
2.2.1 Security Audit (FAU)
2.2.2 Cryptographic Support (FCS)
2.2.3 Identification and Authentication (FIA)
2.2.4 Security Management (FMT)
2.2.5 Protection of the TSF (FPT)
2.2.6 TOE Access (FTA)
2.2.7 Trusted Path/Channels (FTP)
2.3 Evaluation Activities for Optional SFRs
2.3.1 Cryptographic Support (FCS)
2.4 Evaluation Activities for Selection-Based SFRs
2.4.1 Cryptographic Support (FCS)
2.4.2 Identification and Authentication (FIA)
2.5 Evaluation Activities for Objective SFRs
3 Evaluation Activities for SARs
4 Required Supplementary Information
Appendix A - References

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Wireless Local Area Network (WLAN) Access System is to describe the security functionality of Wireless Local Area Network (WLAN) Access System 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-PP:

- Network Device, version 2.2e

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

- Wireless Local Area Network (WLAN) Access System, 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.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Technical Terms

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

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 Collaborative Protection Profile for NDs

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

2.1.1 Modified SFRs

2.1.1.1 Cryptographic Support (FCS)

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

FCS_COP.1/DataEncryption
TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
In addition to the tests required by the NDcPP, the evaluator will perform the following testing:

AES-CCM Tests

The evaluator will test the generation-encryption and decryption-verification functionality of AES-CCM for the following input parameter and tag lengths:

128 bit and 256 bit keys

Two payload lengths. One payload length will be the shortest supported payload length, greater than or equal to zero bytes. The other payload length will be the longest supported payload length, less than or equal to 32 bytes (256 bits).

Two or three associated data lengths. One associated data length will be 0, if supported. One associated

data length will be the shortest supported payload length, greater than or equal to zero bytes. One associated data length will be the longest supported payload length, less than or equal to 32 bytes (256 bits). If the implementation supports an associated data length of 216 bytes, an associated data length of 216 bytes will be tested.

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

Tag lengths. All supported tag lengths of 4, 6, 8, 10, 12, 14, and 16 bytes will be tested.

Due to the restrictions that IEEE 802.11 specifies for this mode (nonce length of 13 and tag length of 8), it is acceptable to test a subset of the supported lengths as long as the selections fall into the ranges specified above. In this case, the evaluator will ensure that these are the only supported lengths. To test the generation-encryption functionality of AES-CCM, the evaluator will perform the following four tests:

- **Test 1:** For each supported key and associated data length and any supported payload, nonce and tag length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.
- **Test 2:** For each supported key and payload length and any supported associated data, nonce and tag length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.
- **Test 3:** For each supported key and nonce length and any supported associated data, payload, and tag length, the evaluator will supply one key value and 10 associated data, payload and nonce value 3-tuples, and obtain the resulting ciphertext.
- **Test 4:** For each supported key and tag length and any supported associated data, payload, and nonce length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values and, obtain the resulting ciphertext

To determine correctness in each of the above tests, the evaluator will compare the ciphertext with the result of generation-encryption of the same inputs with a known good implementation.

To test the decryption-verification functionality of AES-CCM, for each combination of supported associated data length, payload length, nonce length, and tag length, the evaluator will supply a key value and 15 nonce, associated data and ciphertext 3-tuples, and obtain either a fail result or a pass result with the decrypted payload. The evaluator will supply 10 tuples that should fail and 5 that should pass per set of 15.

Additionally, the evaluator will use tests from the IEEE 802.11-02/362r6 document “Proposed Test vectors for IEEE 802.11 TGi”, dated September 10, 2002, Section 2.1 AES-CCMP Encapsulation Example and Section 2.2 Additional AES-CCMP Test Vectors to verify further the IEEE 802.11-2020 implementation of AES-CCMP.

2.1.1.2 Protection of the TSF (FPT)

FPT_TST_EXT.1 TSF Testing

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

TSS
The evaluator will examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution, which includes the generation and protection of the “check value” used to ensure integrity as well as the verification step. This description will also cover the digital signature service used in performing these functions. The evaluator also checks the operational guidance to ensure that any actions required by the administrator to initialize or operate this functionality are present.

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

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

Tests
The evaluator will perform the following tests:

- **Test 1:** Following the operational guidance, the evaluator will initialize the integrity protection system. The evaluator will perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors.
- **Test 2:** The evaluator will modify the TSF executable and cause that executable to be loaded by the TSF. The evaluator will observe that an integrity violation is triggered (care must be taken so that the integrity violation is determined to be the cause of the failure to load the module and not the fact that the module was modified so that it was rendered unable to run because its format was corrupt).

2.1.1.3 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

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

TSS
The evaluator will examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator will also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Guidance
The evaluator will confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity and that it contains recovery instructions should a connection be unintentionally broken.

Tests
The evaluator will perform the following tests:

- **Test 1:** The evaluator will ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
- **Test 2:** For each protocol that the TOE can initiate as defined in the requirement, the evaluator will follow the guidance documentation to ensure that the communication channel can be initiated from the TOE.
- **Test 3:** The evaluator will ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
- **Test 4:** The evaluator will, for each protocol associated with each authorized IT entity tested during test 1, physically interrupt an established connection. The evaluator will ensure that when physical connectivity is restored, communications are appropriately protected.

2.1.1.4 Security Audit (FAU)

FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1
TSS

The evaluator will examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.

The evaluator will examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.

The evaluator will examine the TSS to ensure it it contains a list of TOE components that store audit data locally. The evaluator will examine the TSS to ensure that for TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.

The evaluator will examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option overwrite previous audit records is selected this description should include an outline of the rule for overwriting audit data. If [**assignment**: *other action*] are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.

The evaluator will examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in real- time or periodically. In case the TOE does not perform transmission in real- time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.

The evaluator will examine the TSS to ensure it describes to which TOE components this SFR applies and how audit data transfer to the external audit server is implemented among the different TOE components (e.g. every TOE components does its own transfer or the data is sent to another TOE component for central transfer of all audit events to the external audit server).

The evaluator will examine the TSS to ensure it describes which TOE components are storing audit information locally and which components are buffering audit information and forwarding the information to another TOE component for local storage. For every component the TSS shall describe the behavior when local storage space or buffer space is exhausted.

Guidance

The evaluator will also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

The evaluator will also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.

The evaluator will also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

Tests

Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement:

a. Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator’s choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
b. Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that
    1. The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option ‘drop new audit data’ in FAU_STG_EXT.1.3).
    2. The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option ‘overwrite previous audit records’ in FAU_STG_EXT.1.3)
    3. The TOE behaves as specified (for the option ‘other action’ in FAU_STG_EXT.1.3).
c. Test 3: If the TOE complies with FAU_STG_EXT.2/LocSpace (in the base) the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3.
d. Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.

FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4
TSS

The evaluator will examine the TSS to confirm that it describes which TOE components store their security audit events locally and which send their security audit events to other TOE components for local storage. For the latter, the target TOE component(s) which store security audit events for other TOE components will be identified. For every sending TOE component, the corresponding receiving TOE component(s) need to be identified. For every transfer of audit information between TOE components it will be described how the data is secured during transfer according to FTP_ITC.1 or FPT_ITT.1 (Base-PP).

For each TOE component which does not store audit events locally by itself, the evaluator will then confirm that the TSS describes how the audit information is buffered before sending to another TOE component for local storage.

Guidance

The evaluator will examine the guidance documentation to ensure that it describes how the link between different TOE components is established if audit data is exchanged between TOE components for local storage. The guidance documentation will describe all possible configuration options for local storage of audit data and provide all instructions how to perform the related configuration of the TOE components.

The evaluator will also ensure that the guidance documentation describes for every TOE component which does not store audit information locally how audit information is buffered before transmission to other TOE components.

Tests
For at least one of each type of distributed TOE components (sensors, central nodes, etc.), the following tests will be performed using distributed TOEs.

- **Test 1:** For each type of TOE component, the evaluator will perform a representative subset of auditable actions and ensure that these actions cause the generation of appropriately formed audit records. Generation of such records can be observed directly on the distributed TOE component (if there is appropriate interface), or indirectly after transmission to a central location.
- **Test 2:** For each type of TOE component that, in the evaluated configuration, is capable of transmitting audit information to the external audit server (as specified in FTP_ITC.1), the evaluator will configure a trusted channel and confirm that audit records generated as a result of actions taken by the evaluator are securely transmitted. It is sufficient to observe negotiation and establishment of the secure channel with the TOE component and the subsequent transmission of encrypted data to confirm this functionality. Alternatively, the following steps will be performed: The evaluator induces audit record transmission, then reviews the packet capture around the time of transmission and verifies that no audit data is transmitted in the clear.
- **Test 3:** For each type of TOE component that, in the evaluated configuration, is capable of transmitting audit information to another TOE component (as specified in FTP_ITT.1 (Base-PP) or FTP_ITC.1, respectively), the evaluator will configure a secure channel and confirm that audit records generated as a result of actions taken by the evaluator are securely transmitted. It is sufficient to observe negotiation and establishment of the secure channel with the TOE component and the subsequent transmission of encrypted data to confirm this functionality. Alternatively, the following steps will be performed: The evaluator induces audit record transmission, then reviews the packet capture around the time of transmission and verifies that no audit data is transmitted in the clear.
- **Test 4:** While performing these tests, the evaluator will verify that the TOE behavior observed during testing is consistent with the descriptions provided in the TSS and the Guidance Documentation. Depending on the TOE configuration, there might be a large number of different possible configurations. In such cases, it is acceptable to perform subset testing, accompanied by an equivalency argument describing the evaluator’s sampling methodology.

FAU_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1
TSS

The evaluator will examine the TSS to confirm that it describes which TOE components store their security audit events locally and which send their security audit events to other TOE components for local storage. For the latter, the target TOE components which store security audit events for other TOE components will be identified. For each sending TOE component, the corresponding receiving TOE component(s) need to be identified. For each transfer of audit information between TOE components, the evaluator will ensure that the TSS contains a description of how the data is secured during transfer according to FTP_ITC.1 or FPT_ITT.1 (Base-PP).

For each TOE component which does not store audit events locally by itself, the evaluator will confirm that the TSS describes how the audit information is buffered before sending to another TOE component for local storage.

Guidance

The evaluator will examine the guidance documentation to ensure that it describes how the link between different TOE components is established if audit data is exchanged between TOE components for local storage. The evaluator will ensure that the guidance documentation describes all possible configuration options for local storage of audit data and provide all instructions how to perform the related configuration of the TOE components.

The evaluator will also ensure that the guidance documentation describes for each TOE component that does not store audit information locally how audit information is buffered before transmission to other TOE components.

Tests

For at least one of each type of distributed TOE components (sensors, central nodes, etc.), the following tests will be performed using distributed TOEs.

1. Test 1: For each type of TOE component, the evaluator will perform a representative subset of auditable actions and ensure that these actions cause the generation of appropriately formed audit records. Generation of such records can be observed directly on the distributed TOE component (if there is appropriate interface), or indirectly after transmission to a central location.
2. Test 2: For each type of TOE component that, in the evaluated configuration, is capable of transmitting audit information to the external audit server (as specified in FTP_ITC.1), the evaluator will configure a trusted channel and confirm that audit records generated as a result of actions taken by the evaluator are securely transmitted. It is sufficient to observe negotiation and establishment of the secure channel with the TOE component and the subsequent transmission of encrypted data to confirm this functionality. Alternatively, the following steps will be performed: The evaluator induces audit record transmission, then reviews the packet capture around the time of transmission and verifies that no audit data is transmitted in the clear.
3. Test 3: For each type of TOE component that, in the evaluated configuration, is capable of transmitting audit information to another TOE component (as specified in FTP_ITT.1 [Base-PP] or FTP_ITC.1, respectively), the evaluator will configure a secure channel and confirm that audit records generated as

a result of actions taken by the evaluator are securely transmitted. It is sufficient to observe negotiation and establishment of the secure channel with the TOE component and the subsequent transmission of encrypted data to confirm this functionality. Alternatively, the following steps will be performed: The evaluator induces audit record transmission, then reviews the packet capture around the time of transmission and verifies that no audit data is transmitted in the clear.

While performing these tests, the evaluator will verify that the TOE behavior observed during testing is consistent with the descriptions provided in the TSS and the Guidance Documentation. Depending on the TOE configuration, there might be a large number of different possible configurations. In such cases, it is acceptable to perform subset testing, accompanied by an equivalency argument describing the evaluator's sampling methodology.

2.1.1.5 Communication (FCO)

FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1

In carrying out these activities the evaluator will determine answers to the following questions based on a combination of documentation analysis and testing (possibly also using input from carrying out the Evaluation Activities for the relevant registration channel, such as FTP_TRP.1/Join from the Base-PP), and will report the answers.

a. What stops a component from successfully communicating with TOE components (in a way that enables it to participate as part of the TOE) before it has properly authenticated and joined the TOE ?
b. What is the enablement step? (Describe what interface it uses, with a reference to the relevant section and step in the operational guidance).
    1. What stops anybody other than a Security Administrator from carrying out this step?
    2. How does the Security Administrator know that they are enabling the intended component to join? (Identification of the joiner might be part of the enablement action itself or might be part of secure channel establishment, but it must prevent unintended joining of components)
c. What stops a component successfully joining if the Security Administrator has not carried out the enablement step; or, equivalently, how does the TOE ensure that an action by an authentic Security Administrator is required before a component can successfully join?
d. What stops a component from carrying out the registration process over a different, insecure channel?
e. If the FTP_TRP.1/Join (Base-PP) channel type is selected in FCO_CPC_EXT.1.2 then how do the registration process and its secure channel ensure that the data is protected from disclosure and provides detection of modification?
f. Where the registration channel does not rely on protection of the registration environment, does the registration channel provide a sufficient level of protection (especially with regard to confidentiality) for the data that passes over it?
g. Where the registration channel is subsequently used for normal internal communication between TOE components (i.e. after the joiner has completed registration), do any of the authentication or encryption features of the registration channel result in use of a channel that has weaker protection than the normal FPT_ITT.1 (Base-PP) requirements for such a channel?
h. What is the disablement step? (Describe what interface it uses, with a reference to the relevant section and step in the operational guidance). i) What stops a component successfully communicating with other TOE components if the Security Administrator has carried out the disablement step?

TSS

The evaluator will ensure that the TSS:

a. Describes the method by which a Security Administrator enables and disables communications between pairs of TOE components.
b. Describes the relevant details according to the type of channel in the main selection made in FCO_CPC_EXT.1.2:
    1. First type: the TSS identifies the relevant SFR iteration that specifies the channel used
    2. Second type: the TSS (with support from the operational guidance if selected in FTP_TRP.1.3/Join) describes details of the channel and the mechanisms that it uses (and describes how the process ensures that the key is unique to the pair of components) – see also the Evaluation Activities for FTP_TRP.1/Join.

The evaluator will confirm that if any aspects of the registration channel are identified as not meeting FTP_ITC.1 or FPT_ITT.1 (Base-PP), then the ST has also selected the FTP_TRP.1/Join option in the main selection in FCO_CPC_EXT.1.2.

Guidance

The evaluator will examine the guidance documentation to confirm that it contains instructions for enabling and disabling communications with any individual component of a distributed TOE. The evaluator confirms that the method of disabling is such that all other components can be prevented from communicating with the component that is being removed from the TOE (preventing the remaining components from either attempting to initiate communications to the disabled component, or from responding to communications from the disabled component).

The evaluator will examine the guidance documentation to confirm that it includes recovery instructions should a connection be unintentionally broken during the registration process.

If the TOE uses a registration channel for registering components to the TOE (i.e. where the ST author uses the FTP_ITC.1, FPT_ITT.1 (Base-PP), or FTP_TRP.1/Join (Base-PP) channel types in the main selection for FCO_CPC_EXT.1.2) then the evaluator will examine the Preparative Procedures to confirm that they:

a. describe the security characteristics of the registration channel (e.g. the protocol, keys and authentication data on which it is based) and will highlight any aspects which do not meet the requirements for a steady- state inter-component channel (as in FTP_ITC.1 or FPT_ITT.1 (Base-PP))
b. identify any dependencies between the configuration of the registration channel and the security of the subsequent inter-component communications (e.g. where AES-256 inter-component communications depend on transmitting 256 bit keys between components and therefore rely on the registration channel being configured to use an equivalent key length)
c. identify any aspects of the channel can be modified by the operational environment in order to improve the channel security and will describe how this modification can be achieved (e.g. generating a new key pair, or replacing a default public key certificate).

As background for the examination of the registration channel description, it is noted that the requirements above are intended to ensure that administrators can make an accurate judgment of any risks that arise from the default registration process. Examples would be the use of self-signed certificates (i.e. certificates that are not chained to an external or local Certification Authority), manufacturer-issued certificates (where control over aspects such as revocation, or which devices are issued with recognized certificates, is outside the control of the operational environment), use of generic/non-unique keys (e.g. where the same key is present on more than one instance of a device), or well-known keys (i.e. where the confidentiality of the keys is not intended to be strongly protected – note that this need not mean there is a positive action or intention to publicize the keys).

In the case of a distributed TOE for which the ST author uses the FTP_TRP.1/Join channel type in the main selection for FCO_CPC_EXT.1.2 and the TOE relies on the operational environment to provide security for some aspects of the registration channel security then there are additional requirements on the Preparative Procedures as described in section 3.4.1.2.

Tests

(Note: paragraph 274 lists questions for which the evaluator needs to determine and report answers through the combination of the TSS, Guidance Documentation, and Tests Evaluation Activities.)

The evaluator will carry out the following tests:

1. Test 1.1: the evaluator will confirm that an IT entity that is not currently a member of the distributed TOE cannot communicate with any component of the TOE until the non-member entity is enabled by a Security Administrator for each of the non-equivalent TOE components that it is required to communicate with (non-equivalent TOE components are as defined in the minimum configuration for the distributed TOE)
2. Test 1.2: the evaluator will confirm that after enablement, an IT entity can communicate only with the components that it has been enabled for. This includes testing that the enabled communication is successful for the enabled component pair, and that communication remains unsuccessful with any other component for which communication has not been explicitly enabled Some TOEs may set up the registration channel before the enablement step is carried out, but in such a case the channel must not allow communications until after the enablement step has been completed.

The evaluator will repeat Tests 1.1 and 1.2 for each different type of enablement process that can be used in the TOE.

1. Test 2: The evaluator will separately disable each TOE component in turn and ensure that the other TOE components cannot then communicate with the disabled component, whether by attempting to initiate communications with the disabled component or by responding to communication attempts from the disabled component.
2. Test 3: The evaluator will carry out the following tests according to those that apply to the values of the main (outer) selection made in the ST for FCO_CPC_EXT.1.2.
    1. If the ST uses the first type of communication channel in the selection in FCO_CPC_EXT.1.2 then the evaluator tests the channel via the Evaluation Activities for FTP_ITC.1 or FPT_ITT.1 (Base-PP) according to the second selection – the evaluator will ensure that the test coverage for these SFRs includes their use in the registration process.
    2. If the ST uses the second type of communication channel in the selection in FCO_CPC_EXT.1.2 then the evaluator tests the channel via the Evaluation Activities for FTP_TRP.1/Join.
    3. If the ST uses the ‘no channel’ selection, then no test is required.
3. Test 4: The evaluator will perform one of the following tests, according to the TOE characteristics identified in its TSS and operational guidance:
    1. If the registration channel is not subsequently used for inter- component communication, and in all cases where the second selection in FCO_CPC_EXT.1.2 is made (i.e. using FTP_TRP.1/Join) then the evaluator will confirm that the registration channel can no longer be used after the registration process has completed, by attempting to use the channel to communicate with each of the endpoints after registration has completed
    2. If the registration channel is subsequently used for inter- component communication then the

evaluator will confirm that any aspects identified in the operational guidance as necessary to meet the requirements for a steady-state inter- component channel (as in FTP_ITC.1 or FPT_ITT.1 [Base-PP]) can indeed be carried out (e.g. there might be a requirement to replace the default key pair and/or public key certificate).

4. Test 5: For each aspect of the security of the registration channel that operational guidance states can be modified by the operational environment in order to improve the channel security (cf. AGD_PRE.1 refinement item 2 in (cf. the requirements on Preparative Procedures in 3.5.1.2), the evaluator will confirm, by following the procedure described in the operational guidance, that this modification can be successfully carried out.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_GEN.1/WLAN Audit Data Generation

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

Guidance
There are no operational guidance activities for this SFR.

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

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

2.2.2 Cryptographic Support (FCS)

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

FCS_CKM.1/WPA
TSS
The cryptographic primitives will be verified through evaluation activities specified elsewhere in this PP-Module. The evaluator will verify that the TSS describes how the primitives defined and implemented by this PP-Module are used by the TOE in establishing and maintaining secure connectivity to the wireless clients. This description will include how the GTK and PTK are generated or derived. The TSS will also provide a description of the developer's methods of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also proof of third-party testing that is performed (e.g. WPA2 certification). The evaluator will ensure that the description of the testing methodology is of sufficient detail to determine the extent to which the details of the protocol specifics are tested.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless client:

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

Step 2: The evaluator will configure the TOE to communicate with a WLAN client using IEEE 802.11-2020 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

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

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

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

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

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

Additionally, the evaluator will test the PRF function using the test vectors from:

- Section 2.4 “The PRF Function – PRF (key, prefix, data, length)” of the IEEE 802.11-02/362r6 document "Proposed Test vectors for IEEE 802.11 TGi" dated September 10, 2002
- Annex J.3 “PRF reference implementation and test vectors” of IEEE 802.11-2020

FCS_CKM.2/GTK Cryptographic Key Distribution (GTK)

FCS_CKM.2/GTK
TSS
The evaluator will check the TSS to ensure that it describes how the GTK is wrapped prior to being distributed using the AES implementation specified in this PP-Module, and also how the GTKs are distributed when multiple clients connect to the TOE.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will perform the following test using a packet sniffing tool to collect frames between a wireless client and the TOE (which may be performed in conjunction with the evaluation activity for FCS_CKM.1/PMK.

To fully test the broadcast and multicast functionality, these steps will be performed as the evaluator connects multiple clients to the TOE. The evaluator will ensure that GTKs established are sent to the appropriate participating clients.

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

Step 2: The evaluator will configure the TOE to communicate with the client using IEEE 802.11-2020 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing.

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

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

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

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

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

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

AES Key Wrap (AES-KW Tests)

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

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

authenticated-encryption with AES-KW authenticated-decryption. Additionally, the evaluator will modify one byte of the ciphertext, attempt to decrypt the modified ciphertext, and ensure that a failure is returned rather than plaintext.

AES Key Wrap with Padding (AES-KWP Tests)

- **Test 1:**

  The evaluator will test the authenticated-encryption functionality of AES-KWP for each combination of the following input parameter lengths:

  128 and 256 bit key encryption keys (KEKs)

  Three plaintext lengths. One plaintext length will be one octet. One plaintext length will be 20 octets (160 bits). One plaintext length will be the longest supported plaintext length less than or equal to 512 octets (4096 bits).

  using a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KWP authenticated encryption. To determine correctness, the evaluator will use the AES-KWP authenticated-encryption function of a known good implementation.

- **Test 2:** The evaluator will test the authenticated-decryption functionality of AES-KWP using the same test as for AES-KWP authenticated-encryption, replacing plaintext values with ciphertext values and AES-KWP authenticated-encryption with AES-KWP authenticated-decryption. Additionally, the evaluator will modify one byte of the ciphertext, attempt to decrypt the modified ciphertext, and ensure that a failure is returned rather than plaintext.

FCS_CKM.2/PMK Cryptographic Key Distribution (PMK)

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

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will establish a session between the TOE and a RADIUS server according to the configuration guidance provided. The evaluator will then examine the traffic that passes between the RADIUS server and the TOE during a successful attempt to connect a wireless client to the TOE to determine that the PMK is not exposed.

2.2.3 Identification and Authentication (FIA)

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

FIA_8021X_EXT.1
TSS
In order to show that the TSF implements the 802.1X-2010 standard correctly, the evaluator will ensure that the TSS contains the following information:

- The sections (clauses) of the standard that the TOE implements
- For each identified section, any options selected in the implementation allowed by the standards are specified
- For each identified section, any non-conformance is identified and described, including a justification for the non-conformance

Because the connection to the RADIUS server will be contained in an IPsec or RadSec (TLS) tunnel, the security mechanisms detailed in the RFCs identified in the requirement are not relied on to provide protection for these communications. Consequently, no extensive analysis of the RFCs is required. However, the evaluator will ensure that the TSS describes the measures (documentation, testing) that are taken by the product developer to ensure that the TOE conforms to the RFCs listed in this requirement.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will perform the following tests:

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

evaluator will attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.
- **Test 3:** The evaluator will demonstrate that a wireless client has no access to the test network. The evaluator will attempt to authenticate using an invalid RADIUS certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.

Note: Tests 2 and 3 above are not tests that "EAP-TLS works," although that is a by-product of the test. The test is actually that a failed authentication (under two failure modes) results in denial of access to the network, which demonstrates the enforcement of FIA_8021X_EXT.1.3.

FIA_UAU.6 Re-Authenticating

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

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will attempt to change their password as directed by the operational guidance. While making this attempt, the evaluator will verify that re-authentication is required.

If other re-authentication conditions are specified, the evaluator will cause those conditions to occur and verify that the TSF re-authenticates the authenticated user.

2.2.4 Security Management (FMT)

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

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

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

Tests

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

FMT_SMR_EXT.1 No Administration from Client

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

Guidance
The evaluator will review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. The evaluator will confirm that the TOE does not permit remote administration from a wireless client by default.

Tests
The evaluator will demonstrate that after configuring the TOE for first use from the operational guidance, it is possible to establish an administrative session with the TOE on the “wired” portion of the device. They will

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

2.2.5 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1
TSS
The evaluator will examine the TSS to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator will examine the TSS to ensure that it describes all failure conditions and how a secure state is preserved if any of these failures occur. The evaluator will ensure that the definition of a secure state is suitable to ensure the continued protection of any key material and user data.

Guidance
The evaluator will examine the operational guidance to verify that it describes applicable recovery instructions for each TSF failure state.

Tests
For each failure mode specified in the ST, the evaluator will ensure that the TOE attains a secure state (e.g., shutdown) after initiating each failure mode type.

2.2.6 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

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

Guidance
The evaluator will examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

Tests
For each supported attribute, the evaluator will perform the following test:

- **Test 1:** The evaluator successfully establishes a client session with a wireless client. The evaluator then follows the operational guidance to configure the system so that the client's access is denied based on a specific value of the attribute. The evaluator will then attempt to establish a session in contravention to the attribute setting (for instance, the client is denied WLAN access based upon the TOE interface (e.g. WLAN AP) it is connecting to, or that the client is denied access based upon the time-of-day or day-of-week it is attempting connection on). The evaluator will observe that the access attempt fails.

2.2.7 Trusted Path/Channels (FTP)

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

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

2.3 Evaluation Activities for Optional SFRs

2.3.1 Cryptographic Support (FCS)

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

FCS_CKM.2/DISTRIB
TSS
The evaluator will examine the TSS to determine that it describes which keys are distributed outside the TOE, where they are sent, and the purpose for this transfer.

Guidance
If this function is dependent on TOE configuration, the evaluator will confirm that the operational guidance contains instructions for how to configure that the keys are adequately protected.

Tests

This requirement will be tested in conjunction with the tests for the cryptographic primitives, the secure protocols, and FPT_ITT.1 (Base-PP).

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Cryptographic Support (FCS)

FCS_RADSEC_EXT.1 RadSec

FCS_RADSEC_EXT.1
TSS
The evaluator will verify that the TSS description includes the use of RADIUS over TLS, as described in RFC 6614.

If X.509v3 certificates is selected, the evaluator will ensure that the TSS description includes the use of client-side certificates for TLS mutual authentication.

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

Tests
The evaluator will demonstrate the ability to successfully establish a RADIUS over TLS connection with a RADIUS server. This test will be performed with X.509v3 certificates if selected and performed with pre-shared keys if selected.

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

FCS_RADSEC_EXT.2
TSS
The evaluator will check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator will check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator will also verify that the TSS contains a description of the denial of old SSL and TLS versions.

The evaluator will examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality) and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

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

The evaluator will also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that RADIUS over TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

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

Tests
The evaluator will perform the following tests:

- **Test 1:** The evaluator will establish a RADIUS over TLS connection using each of the ciphersuites selected in FCS_RADSEC_EXT.2.1. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
- **Test 2:** The evaluator will set the pre-shared key to a value that does not match the server's pre-shared key and demonstrate that the TOE cannot successfully complete a protocol negotiation using this key.
- **Test 3:** The evaluator will configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.
- **Test 4:** The evaluator will perform the following modifications to the traffic:
  - Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example, 1.3, represented by the two bytes 03 04) and verify that the client rejects the connection.
  - Modify at least one byte in the server’s nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE cipher suite) or that the server denies the client’s Finished handshake message.
  - Modify the server’s selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator will verify that the client rejects the connection after receiving the Server Hello.
  - Modify a byte in the Server Finished handshake message, and verify that the client rejects the connection and does not send any application data.

    - Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the client denies the connection.
- **Test 5:** [conditional] If the TOE does not generate bit-based pre-shared keys, the evaluator will obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.
- **Test 6:** [conditional] If the TOE does generate bit-based pre-shared keys, the evaluator will generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.

FCS_RADSEC_EXT.3 RadSec using Pre-Shared Keys and RSA

FCS_RADSEC_EXT.3
TSS
The evaluator will ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator and application-configured reference identifier, including which types of reference identifiers are supported (e.g., Common Name, DNS Name, URI Name, Service Name, or other application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator will ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the TOE.

Guidance
The evaluator will verify that the operational guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.

Tests
The evaluator will perform the following tests:

- **Test 1:** The evaluator will attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
- **Test 2:** The evaluator will present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator will verify that the connection fails.
- **Test 3:** The evaluator will present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator will verify that the connection fails. The evaluator will repeat this test for each supported SAN type.
- **Test 4:** The evaluator will present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator will verify that the connection succeeds.
- **Test 5:** [conditional] If the TOE does not mandate the presence of the SAN extension, the evaluator will present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator will verify that the connection succeeds. If the TOE does mandate the presence of the SAN extension, this test will be omitted.
- **Test 6:** [conditional] If wildcards are supported by the TOE, the evaluator will perform the following tests:
    - The evaluator will present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
    - The evaluator will present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g. *.example.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.example.com). The evaluator will verify that the connection succeeds. The evaluator will configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.
    - The evaluator will present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.
- **Test 7:** [conditional] If wildcards are not supported by the TOE, the evaluator will present a server certificate containing a wildcard and verify that the connection fails.
- **Test 8:** [conditional] If URI or Service name reference identifiers are supported, the evaluator will configure the DNS name and the service identifier. The evaluator will present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator will repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.

2.4.2 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

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

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

Guidance
The evaluator will examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. The guidance must specify the allowable characters for pre-shared keys, and that list must be a superset of the list contained in FIA_PSK_EXT.1.2.

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

Tests
The evaluator will also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.

- **Test 1:** The evaluator will compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance and demonstrates that a successful protocol negotiation can be performed with the key.
- **Test 2:** [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator will repeat Test 1 using the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.
- **Test 3:** [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator will obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.
- **Test 4:** [conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator will generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.

2.5 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 NDcPP 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 this Base-PP as well. The NDcPP 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 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
	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April

[CC]	2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019