

# Supporting Document

## Mandatory Technical Document



PP-Module for Authentication Servers

Version: 1.0

2022-08-12

**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	2022-08-12	Initial Release

### General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of Authentication Server products.

### Acknowledgments:

This SD was developed with support from NIAP Authentication Servers 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 Security Audit (FAU)
      - 2.1.1.2 Communication (FCO)
      - 2.1.1.3 Cryptographic Support (FCS)
      - 2.1.1.4 Protection of the TSF (FPT)
      - 2.1.1.5 Trusted Path/Channels (FTP)
    - 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 Authentication Servers is to describe the security functionality of Authentication Servers 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 :

- Authentication Servers, 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 <a href="#">[CC]</a> .
-----------	---

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

Assertion	A statement from the TOE to an RP that contains information about a subscriber. Assertions may also contain verified attributes. For the purposes of this PP-Module, Assertions containing authentication status and identity attributes are made by EAP response messages in accordance with EAP-TLS or EAP-TTLS.
Authentication Policy	A policy that specifies which authenticator types are required for a particular entity. The policy may be implicit for all entities, or configurable.

Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.
Authenticator Output	The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.
Claimant	A subject whose identity is to be verified using one or more authentication protocols.
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.
Federation Protocol	A protocol to establish a trusted relationship with a relying party, and for the purposes of this PP module, to communicate authentication status for entities requesting access to resources managed by the relying party. In this PP-module, Federation Protocols include RADIUS, DIAMETER, and other standard protocols used in direct communication between the relying party and the TOE. Federation protocols that only support bearer assertions are out of scope for this PP-Module.
Relying Party (RP)	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

## 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 Security Audit (FAU)

###### FAU\_GEN\_EXT.1 Security Audit Generation

###### FAU\_GEN\_EXT.1

There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

###### FAU\_STG\_EXT.1 Protected Audit Event Storage

###### FAU\_STG\_EXT.1

There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to restricts selections in FAU\_STG\_EXT.1.2 to a subset of the available options

to account for the TOE being distributed.

## **FAU\_STG\_EXT.4 Protected Local Audit Event Storage for Distributed TOEs**

### **FAU\_STG\_EXT.4**

There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

## **2.1.1.2 Communication (FCO)**

### **FCO\_CPC\_EXT.1 Component Registration Channel Definition**

#### **FCO\_CPC\_EXT.1**

There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required deployment as a distributed TOE.

## **2.1.1.3 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.

#### **2.1.1.4 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).

#### **2.1.1.5 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.

## 2.2 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**

**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**

## **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 URName 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
[CC]	Common Criteria for Information Technology Security Evaluation -
	• <a href="#">Part 1: Introduction and General Model</a> , CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
	• <a href="#">Part 2: Security Functional Components</a> , CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
	• <a href="#">Part 3: Security Assurance Components</a> , CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	<a href="#">collaborative Protection Profile for Network Devices</a> , Version 2.2e, March 23, 2020
[NDcPP SD]	<a href="#">Supporting Document - Evaluation Activities for Network Device cPP</a> , Version 2.2, December 2019