# Supporting Document
# Mandatory Technical Document


PP-Module for WLAN Clients

Version: 1.0

2021-03-15

**National Information Assurance Partnership**

# Foreword

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

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

**Technical Editor:**
National Information Assurance Partnership (NIAP)

**Document history:**

| Version | Date | Comment |
|---|---|---|
| 1.0 | 2021-03-15 | Initial Release |

**General Purpose:**
The purpose of this SD is to define evaluation methods for the functional behavior of PP-Module for Wireless LAN Clients products.

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

# Table of Contents

# 1 Introduction

## 1.1 Technology Area and Scope of Supporting Document

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

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

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

- WLAN Clients, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activites 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. |
| Common Criteria (CC) | Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408). |
| Common Criteria | Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory |

| | |
|---|---|
| Testing Laboratory | Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations. |
| Common Evaluation Methodology (CEM) | Common Evaluation Methodology for Information Technology Security Evaluation. |
| Distributed TOE | A TOE composed of multiple components operating as a logical whole. |
| Operational Environment (OE) | Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy. |
| Protection Profile (PP) | An implementation-independent set of security requirements for a category of products. |
| Protection Profile Configuration (PP-Configuration) | A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module. |
| Protection Profile Module (PP-Module) | An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles. |
| Security Assurance Requirement (SAR) | A requirement to assure the security of the TOE. |
| Security Functional Requirement (SFR) | A requirement for security enforcement by the TOE. |
| Security Target (ST) | A set of implementation-dependent security requirements for a specific product. |
| TOE Security 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. |
| Target of Evaluation (TOE) | The product under evaluation. |

### 1.3.2 Technical Terms

| | |
|---|---|
| Access Point (AP) | A device that provides the network interface that enables wireless client hosts to access a wired network. Once authenticated as trusted nodes on the wired infrastructure, the APs provide the encryption service on the wireless network between the wireless client and the radio frequency (RF) interface of the AP. |
| Administrator | A user that has administrative privilege to configure the TOE. |
| Authentication Credentials | The information the system uses to verify that the user or administrator is authorized to access the TOE or network. Credentials can exist in various forms, such as username/password or digital certificates. |
| Authentication Server (AS) | A server on the wired network that receives authentication credentials from wireless clients and determines their validity. |
| Critical Security Parameter (CSP) | Security related information, e.g. secret and private cryptographic keys, and authentication data such as passwords and Personal Identification Numbers (PINs), whose disclosure or modification can compromise the security of a cryptographic module. |
| Entropy | A cryptographic function that provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a |

| | |
|---|---|
| Source | measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly. |
| Extensible Authentication Protocol (EAP) | An authentication framework, used in wireless networks, that uses Public Key Infrastructure (PKI) to authenticate both the authentication server and the wireless client. |
| FIPS-Approved Cryptographic Function | A cryptographic operation that is specified for use by FIPS 140. |
| IEEE 802.1X | A standard for port-based network access control that defines an authentication mechanism for WLAN Clients to attach to a wired network. |
| Unauthorized User | A user that has not been granted the ability to use the TOE. |

# 2 Evaluation Activities for SFRs

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

Regarding design descriptions (designated by the subsections labelled 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 work unit 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 work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled 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 work units that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

## 2.1 Protection Profile for General Purpose Operating Systemss

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

### 2.1.1 Modified SFRs

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

## 2.2 Protection Profile for Mobile Device Fundamentalss

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

### 2.2.1 Modified SFRs

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

## 2.3 TOE SFR Evaluation Activities

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

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

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

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

**FIA_PAE_EXT.1 Port Access Entity Authentication**

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

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

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

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

**FTA_WSE_EXT.1 Wireless Network Access**

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

# 2.4 Evaluation Activities for Optional SFRs

**FIA_X509_EXT.4 X.509 Certificate Storage and Management**

# 2.5 Evaluation Activities for Selection-Based SFRs

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

# 2.6 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

# 3 Evaluation Activities for SARs

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

# 4 Required Supplementary Information

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

# Appendix A - References

| Identifier | Title |
|---|---|
| [CC] | Common Criteria for Information Technology Security Evaluation -<br>• Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.<br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.<br>• Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017. |
| [CEM] | Common Evaluation Methodology for Information Technology Security - Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017. |
| [GPOS] | Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019 |
| [MDF] | Protection Profile for Mobile Device Fundamentals, Version 3.2, March 4, 2021 |
| [802.11-2016] | 802.11-2016 - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications |

| | |
|---|---|
| [802.11-2016] | 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control |
| [RFC 3394] | RFC 3394 - Advanced Encryption Standard (AES) Key Wrap Algorithm |
| [RFC 4346] | RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1 |
| [RFC 5216] | RFC 5216 - The EAP-TLS Authentication Protocol |
| [RFC 5246] | RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2 |
| [RFC 5280] | RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |