General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients

08 February 2016

Version 1.0

Table of Contents

List of Tables

List of Figures

Revision History

Version	Date	Description
1.0	December 2011	Initial release
2.0	February 2016	Revisions to incorporate extensions to both OS and MDF PPs

1 Introduction

This Extended Package (EP) describes security requirements for commercial off-the-shelf (COTS) Wireless Local Area Network (WLAN) Clients for the protection of data on a wireless network.

This introduction describes the features of a conformant Target of Evaluation (TOE) and discusses how this EP is to be used in conjunction with the Protection Profile for General Purpose Operating Systems (OS PP) or the Protection Profile for Mobile Device Fundamentals (MDF PP).

1.1 Conformance Claims

This EP serves to complement the OS PP or the MDF PP with additional SFRs and associated Assurance Activities specific to wireless LAN clients. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

This EP extends the OS PP when the WLAN client is installed on an operating system that is evaluated against that PP. This EP extends the MDF PP when the WLAN client is installed on a self-contained mobile device evaluated against that PP.

As an EP of either the OS PP or the MDF PP, it is expected that the content of this EP and the chosen base PP be appropriately combined in the context of each product-specific Security Target. When this EP is used with the OS PP or MDF PP, conformant TOEs are obligated to implement the functionality required in those PPs with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein. An ST must identify the applicable versions of the PP chosen and this EP in its conformance claims.

1.3 Compliant Targets of Evaluation

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

Conformant WLAN Clients support IEEE 802.1X Port Based Network Access Control. The architectural framework of Port-based access control defines three distinct roles: Supplicant (the TOE), Authenticator (WLAN Access System); and Authentication Server (AS). The WLAN Access System requires successful authentication of the TOE, relying on the AS to authenticate the TOE, before providing network access. The WLAN Access System acts as a pass through device between the TOE and the AS. The WLAN Access System allows the WLAN Client access to the private network only after it has been successfully authenticated by the AS. The TOE and AS must perform mutual machine authentication using X.509 v3 certificates and Extensible

Authentication Protocol-Transport Layer Security (EAP-TLS) messages. If either the TOE or AS fail to authenticate, the WLAN Access System ceases to communicate with the WLAN Client. Secure communication tunnels to the private network can only be established if authentication is successful.

1.4 Usage and Major Security Features of the TOE

A WLAN Client allows remote users to use client machines to establish wireless communication with a private network (through a WLAN Access System). IP packets passing between the private network and a remote access WLAN Client are encrypted. The WLAN Client protects the data between itself and the private network, providing confidentiality, integrity, and protection of data in transit, even though it traverses a wireless connection.

The focus of the Security Functional Requirements in this EP is on the following fundamental aspects of a WLAN Client:

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

The WLAN Client establishes an 802.11 tunnel between the client device and the network infrastructure using IEEE 802.1X with EAP-TLS for authentication. It performs mutual authentication to an AS in the private network as part of the EAP-TLS exchange. The EAP-TLS exchange uses certificates for mutual authentication. The WLAN Client examines the machine certificate transmitted from the AS, checks its validity, and ensures the certificate is signed by a trusted Certificate Authority (CA). The AS will authenticate the WLAN Client certificate at the same time. When the EAP-TLS exchange completes successfully, the network allows the WLAN Client to finish establishing a secure communication tunnel to the private network. The WLAN Client sets up an encrypted, authenticated channel to the WLAN Access System using a 4 way handshake, as specified in IEEE 802.11. Once the channel is established, all communication between the WLAN Client to the WLAN Access System is encrypted with AES in CCMP mode and optionally AES is GCMP mode, as specified in IEEE 802.11.

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

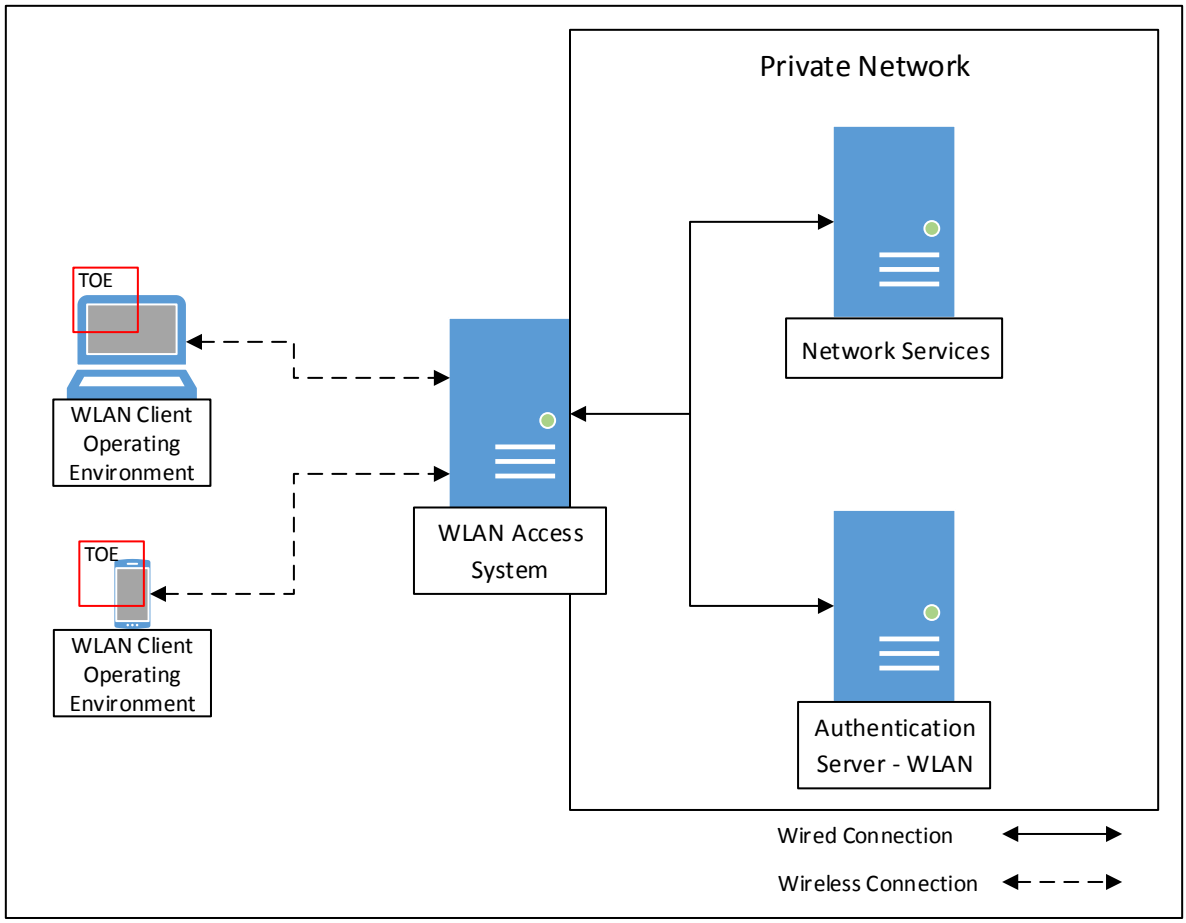

Figure 1: WLAN Client

The security features of the TOE include administration, protocol compliance, cryptographic protection, and audit generation. The WLAN Client relies on the IT environment for its proper execution as well as the following client machine protection mechanisms: audit review, audit storage, identification and authentication, security management, and session management.

2 Security Problem Definition

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

2.1 Threats

This Extended Package does not repeat any threats, assumptions, and organizational security policies identified in the base PPs, though they all apply given the conformance and hence dependence of this EP on it. Together the threats, assumptions and any organizational security policies of the base PPs and those defined in this EP describe those addressed by a WLAN Client as the Target of Evaluation.

This EP addresses threats as described in the base PPs, particularly Network Attack and Network Eavesdropping, adapted for the wireless use case. Use of wireless communications increases these threats; adversaries can launch wireless attacks without breaching the confines of the protected facility or obtaining access to the client device. Signal jamming and denial of service attacks are common and hard to prevent. Assumptions on the availability of the network are in place to address these threats since they are not covered by the requirements in this EP. However, other mechanisms can be used to protect wireless communication. Improper negotiation of security policies or enforcing weak protocol options to establish a wireless connection is a concern that could result in the disclosure or modification of user and TSF data. While it is impossible to prevent an adversary from capturing and saving ("sniffing") wireless traffic, protocol interoperability and mutual agreed upon security policies requiring strong encryption are imperative for establishing wireless LAN protection.

2.1.1 TSF Failure

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

(T.TSF_FAILURE)

2.1.2 Unauthorized Access

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

(T.UNAUTHORIZED ACCESS)

2.1.3 Undetected Actions

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

(T.UNDETECTED_ACTIONS)

2.2 Assumptions

The Assumptions for WLAN Clients can be found in Appendix A.1.1.

3 Security Objectives

3.1 Security Objectives for the TOE

The Security Problem described in Section 2 will be addressed by a combination of cryptographic capabilities. Compliant TOEs will provide security functionality that addresses threats to the TOE and enforces policies that are imposed by law or regulation. The following subsections provide a description of the security objectives required to meet the threats/policies previously discussed. The descriptions of the security objectives are in addition to that described in the base PP.

Note: in each subsection below, particular security objectives are identified (highlighted by O.) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

3.1.1 Authorized Communication

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

(O.AUTH_COMM -> FCS_TLSC_EXT.1/WLAN, FIA_PAE_EXT.1, FIA_X509_EXT.2, FTP_ITC_EXT.1)

3.1.2 Cryptographic Functions

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

(O.CRYPTOGRAPHIC_FUNCTIONS -> FCS_CKM.1.1/WLAN, FCS_CKM.2.1/WLAN)

3.1.3 System Monitoring

The TOE will provide the capability to generate audit data.

(O.SYSTEM_MONITORING -> FAU_GEN.1)

3.1.4 TOE Administration

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

(O.TOE_ADMINISTRATION -> FMT_SMF_EXT.1)

3.1.5 TSF Self Test

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

(O.TSF_SELF_TEST -> FPT_TST_EXT.1)

3.1.6 Wireless Access Point Connection

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

(O.WIRELESS_ACCESS_POINT_CONNECTION -> FTA_WSE_EXT.1)

3.2 Security Objectives for the Operational Environment

The objectives that are required to be med by the TOE's operational environment are defined in Section A.2.2.

4 Security Requirements and Rationale

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with italicized text;
- Refinement made by EP author: Indicated with **bold text** and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3); and
- Extended SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

4.2 EP Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this EP. These SFRs must be claimed regardless of whether the base PP is the OS PP or the MDF PP.

Table 1: TOE Security Functional Requirements

Functional Class	Functional Components
Security Audit (FAU)	FAU_GEN.1/WLAN Audit Data Generation (Wireless LAN)
Cryptographic Support (FCS)	FCS_CKM.1/WLAN Cryptographic key generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.2/WLAN Cryptographic Key Distribution (GTK)
	FCS_TLSC_EXT.1/WLAN Extensible Authentication Protocol-Transport Layer Security
Identification and Authentication (FIA)	FIA_PAE_EXT.1 Port Access Entity Authentication
	FIA_X509_EXT.2/WLAN X.509 Certificate Authentication (EAP-TLS)
Security Management (FMT)	FMT_SMF_EXT.1/WLAN Specification of Management Functions (Wireless LAN)
Protection of the TSF (FPT)	FPT_TST_EXT.1/WLAN TSF Cryptographic Functionality Testing (Wireless LAN)
TOE Access (FTA)	FTA_ WSE_EXT.1 Wireless Network Access
Trusted Path/Channels (FTP)	FTP_ITC_EXT.1/WLAN Trusted Channel Communication (Wireless LAN)

4.2.1 Class: Security Audit (FAU)

FAU_GEN Security Audit Data Generation

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

There are additional auditable events (listed in Table 2) that serve to extend the FAU_GEN.1 SFR found in both the OS PP and MDF PP. The following events should be combined with those of the OS PP or MDF PP in the context of a conforming Security Target.

Application Note: 1) Since this EP extends multiple PPs, it is important to note that the intention of this extension is not to combine the Auditable Events from both PPs. For example, if the MDF PP is being used as the base PP, only its Auditable Events, along with those listed in Table 2 of this EP should be used. 2) If auditing is optional in the base PP then the additional Auditable events in Table 2 are also optional. 3) If auditing is mandatory in the base PP but the base PP contains both optional and mandatory Auditable Events then the additional Auditable Events found in Table 2 of this EP must be considered mandatory (unless otherwise noted as optional).

Table 2: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/WLAN	None.	
FCS_CKM.1/WLAN	None.	
FCS_CKM.2/WLAN	None.	
FCS_CKM_EXT.4	None.	
FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session. Establishment/termination of an EAP-TLS session.	Reason for failure. Non-TOE endpoint of connection.
FIA_PAE_EXT.1	None.	
FIA_X509_EXT.2/WLAN	None.	
FMT_SMF_EXT.1/WLAN	None.	
FPT_TST_EXT.1/WLAN (note: can be performed by TOE or TOE platform)	Execution of this set of TSF self-tests. [selections: detected integrity violation, none].	[selection: The TSF binary file that caused the integrity violation, no additional information].
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure).
FTP_ITC_EXT.1/WLAN	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the non-TOE endpoint of the channel.

Assurance Activity	
TSS	There are no TSS assurance activities for this SFR.
AGD	The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the EP is described and that the description of the fields contains the information required in FAU_GEN.1.2, and the additional information specified in Table 2. The evaluator shall in particular ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In Table 2, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems. The evaluator shall also make a determination of the administrative actions that are relevant in the context of this EP. The TOE may contain functionality that is not evaluated in the context of this EP because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the EP, which thus form the set of "all administrative actions". The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.
Test	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this EP. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

4.2.2 Class: Cryptographic Support (FCS)

The cryptographic requirements are also structured to require the use of the Wi-Fi certification requirements for WPA2 enterprise, based on the IEEE 802.11 standard. The Wi-Fi Alliance WPA2 Enterprise certification program tests devices for data communications interoperability at ISO OSI layers 1 and 2, and mandates the use of the Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC) algorithm (known collectively as AES-CCMP) for secure connections. Optionally, AES-GCMP (Galois/Counter Mode Protocol) can be used.

FCS_CKM Cryptographic Key Management

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

FCS_CKM.1.1/WLAN Refinement: The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[PRF-384]*** and [selection: PRF-704, no other] and specified cryptographic key sizes ***[128 bits]*** and [selection: 256 bits, no other key sizes] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: ***[IEEE 802.11-2012]*** and [selection: IEEE 802.11ac-2014, no other standards].

Application Note: *The cryptographic key derivation algorithm required by IEEE 802.11-2012 (Section 11.6.1.2) and verified in WPA2 certification is PRF-384, which uses the HMAC-SHA-1 function and outputs 384 bits. The use of GCMP is defined in IEEE 802.11ac-2014 (Section 11.4.5) and requires a KDF based on HMAC-SHA-256 (for 128-bit symmetric keys) or HMAC-SHA-384 (for 256-bit symmetric keys). This KDF outputs 704 bits.*

This requirement applies only to the keys that are generated/derived for the communications between the access point and the client once the client has been authenticated. It refers to the derivation of the PTK from the PMK, which is done using a random value generated by the RBG specified in this EP, the HMAC function using SHA-1 as specified in this EP, as well as other information. This is specified in 802.11-2012 primarily in section 11.6.1.2.

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes how the primitives defined and implemented by this EP are used by the TOE in establishing and maintaining secure connectivity to the wireless clients. The TSS shall also provide a description of the developer's method(s) of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also any third-party testing that is performed.
AGD	There are no AGD assurance activities for this SFR.
Test	The evaluator shall perform the following tests: • Test 1: The evaluator shall configure the access point so the cryptoperiod of the session key is 1 hour. The evaluator shall successfully connect the TOE to the access point and maintain the connection for a length of time that is greater than the configured cryptoperiod. The evaluator shall use a packet capture tool to determine that after the configured cryptoperiod, a re-negotiation is initiated to establish a new session key. Finally, the evaluator shall determine that the renegotiation has been

	successful and the client continues communication with the access point. • Test 2: The evaluator shall perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless LAN access point: Step 1: The evaluator shall configure the access point to an unused channel and configure the WLAN sniffer to sniff only on that channel (i.e., lock the sniffer on the selected channel). The sniffer should also be configured to filter on the MAC address of the TOE and/or access point. Step 2: The evaluator shall configure the TOE to communicate with a WLAN access point using IEEE 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key. The pre-shared key is only used for testing. Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and the access point, and allow the TOE to authenticate, associate, and successfully complete the 4 way handshake with the client. Step 4: The evaluator shall set a timer for 1 minute, at the end of which the evaluator shall disconnect the TOE from the wireless network and stop the sniffer. Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK from the 4-way handshake frames and pre-shared key as specified in IEEE 802.11-2012. Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and access point after the 4-way handshake successfully completed, and without the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the PTK to decrypt the data portion of the packet as specified in IEEE 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text. Step 7: The evaluator shall repeat Step 6 for the next 2 data frames between the TOE and access point and without frame control value 0x4208.

FCS_CKM.2/WLAN Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/WLAN Refinement: The TSF shall decrypt **Group Temporal Key** in accordance with a specified cryptographic key distribution method [*AES Key Wrap in an EAPOL-Key frame*] that meets the following: [*RFC 3394 for AES Key Wrap, 802.11-2012 for the packet format and timing considerations*] **and does not expose the cryptographic keys**.

Application Note: *This requirement applies to the Group Temporal Key (GTK) that is received by the TOE for use in decrypting broadcast and multicast messages from the Access Point to which it's connected. 802.11-2012 specifies the format for the transfer as well as the fact that it must*

be wrapped by the AES Key Wrap method specified in RFC 3394; the TOE must be capable of unwrapping such keys.

Assurance Activity	
TSS	The evaluator shall check the TSS to ensure that it describes how the GTK is unwrapped prior to being installed for use on the TOE using the AES implementation specified in this EP.
AGD	There are no AGD assurance activities for this SFR.
Test	The evaluator shall perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless access point (which may be performed in conjunction with the assurance activity for FCS_CKM.1.1/WLAN). Step 1: The evaluator shall configure the access point to an unused channel and configure the WLAN sniffer to sniff only on that channel (i.e., lock the sniffer on the selected channel). The sniffer should also be configured to filter on the MAC address of the TOE and/or access point. Step 2: The evaluator shall configure the TOE to communicate with the access point using IEEE 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key, setting up the connections as described in the operational guidance. The pre-shared key is only used for testing. Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and access point, and allow the TOE to authenticate, associate, and successfully complete the 4-way handshake with the TOE. Step 4: The evaluator shall set a timer for 1 minute, at the end of which the evaluator shall disconnect the TOE from the access point and stop the sniffer. Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK and GTK from the 4-way handshake frames and pre-shared key as specified in IEEE 802.11-2012. Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and access point after the 4-way handshake successfully completed, and with the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the GTK to decrypt the data portion of the selected packet as specified in IEEE 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text. Step 7: The evaluator shall repeat Step 6 for the next 2 data frames with frame control value 0x4208.

FCS_TLSC_EXT Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

FCS_TLSC_EXT.1/WLAN Extensible Authentication Protocol-Transport Layer Security

FCS_TLSC_EXT.1.1/WLAN The TSF shall implement TLS 1.0 and [selection: TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246), no other TLS version] in support of the EAP-TLS protocol as specified in RFC 5216 supporting the following ciphersuites:

- Mandatory Ciphersuites in accordance with RFC 5246:
  TLS_RSA_WITH_AES_128_CBC_SHA
- Optional Ciphersuites:
  [selection:
    None
    TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
    TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
    TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

Application Note: *If any of the ECDHE ciphersuites are selected by the ST author, it is necessary to include FCS_TLSC_EXT.2/WLAN in the TSF (see Appendix C).*

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

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

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

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

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

Application Note: *The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. TLS_RSA_WITH_AES_128_CBC_SHA is required in order to ensure compliance with RFC 5246.*

TLS 1.2 is the preferred protocol. TLS 1.0 and TLS 1.1 are currently allowed due to lack of support for TLS 1.2. TLS 1.0 and TLS 1.1 do not have the extensions necessary to assure a connection

with security strength of 112-bits or better. These requirements will be revisited as new TLS versions are standardized by the IETF.

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

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

Assurance Activity	
TSS	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.
AGD	The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements). The evaluator shall check that the OPE guidance contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange, and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange.
Test	The evaluator shall write, or the ST author shall provide, an application for the purposes of testing TLS. The evaluator shall also perform the following tests: • Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a ciphersuite 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 ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES). • Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not

	established. Ideally, the two certificates should be identical except for the extendedKeyUsage field. • Test 3: The evaluator shall send a server certificate in the TLS connection that does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite or send a RSA certificate while using one of the ECDSA ciphersuites.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message. • Test 4: The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection. • Test 5: The evaluator shall perform the following modifications to the traffic: o 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. o Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message. o Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello. o Modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message. o Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data. o Send a garbled message from the Server after the Server has issued the ChangeCipherSpec message and verify that the client denies the connection.

4.2.3 Class: Identification and Authentication (FIA)

The baseline requirements for the TOE are fairly limited with respect to I&A, since no formal administrative or general purpose users are defined. The extent of the I&A required to be performed by the TOE relates to the process of becoming connected to the protected network through the Wireless Access System. Additionally, some of the requirements that might normally be considered part of the I&A process are specified in other sections of this EP, particularly those related to cryptographic protocols used for the wireless communications (WPA2). This was done to keep requirements on those protocols grouped together for understandability as well as for ease of authoring and applying assurance activities. Therefore,

the requirements in this section cover the remaining two aspects of the I&A capabilities the TOE must support:

- **802.1X-2010 Authentication.** The 802.1X-2010 standard (and associated RFCs) specifies authentication of a machine for the purposes of accessing a network. This method is used as a precursor to wireless operations using the 802.11-2012 standard. While 802.1X contains requirements for several different parties that participate in 802.1X exchanges, the requirements below are targeted at the TOE's role as a "supplicant" per 802.1X.
- **Credentials.** The protocols and mechanisms specified in this and other sections of the EP rely on certificates for use in the EAP-TLS exchange in performing the 802.1X authentication.

FIA_PAE_EXT Port Access Entity Authentication

FIA_PAE_EXT.1 Port Access Entity Authentication

FIA_PAE_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Supplicant" role.

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

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

The point of performing 802.1X authentication is to gain access to the network (assuming the authentication was successful and that all 802.11 negotiations are performed successfully); in the terminology of 802.1X, this means the TOE will gain access to the "controlled port" maintained by the wireless access system.

Assurance Activity	
TSS	There are no TSS assurance activities for this SFR.
AGD	There are no guidance activities for this SFR.
Test	The evaluator shall perform the following tests: • Test 1: The evaluator shall demonstrate that the TOE has no access to the test network. After successfully authenticating with an authentication server through a wireless access system, the evaluator shall demonstrate that the TOE does have access to the test network. • Test 2: The evaluator shall demonstrate that the TOE has no access to the test network.

	The evaluator shall attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network. • Test 3: The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid authentication server certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.

FIA_X509_EXT X.509 Certificate Validation

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

FIA_X509_EXT.2.1/WLAN The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges.

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

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: allow the administrator to choose whether to accept the certificate in these cases, allow the user to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate].

Assurance Activity	
TSS	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
AGD	The evaluator shall check the administrative guidance to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Test	The evaluator shall perform the following test for each trusted channel: Test: The evaluator shall demonstrate using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational

	guidance to determine that all supported administrator-configurable options behave in their documented manner.

4.2.4 Class: Security Management (FMT)

As indicated in Section 1 of this EP, the TOE is not required to maintain a separate management role. It is, however, required to provide functionality to configure certain aspects of TOE operation that should not be available to the general user population. If the TOE does provide some degree of administrative control, then the appropriate requirements from Appendix C should be used in the ST.

FMT_SMF_EXT Specification of Management Functions

FMT_SMF_EXT.1/WLAN Specification of Management Functions (Wireless LAN)

FMT_SMF_EXT.1.1/WLAN The TSF shall be capable of performing the following management functions: [

- *configure security policy for each wireless network:*
  - [selection: *specify the CA(s) from which the TSF will accept WLAN authentication server certificate(s), specify the FQDN(s) of acceptable WLAN authentication server certificate(s)]*
  - *security type*
  - *authentication protocol*
  - *client credentials to be used for authentication;*
- *(optional) specify wireless networks (SSIDs) to which the TSF may connect;*
- *(optional) enable/disable certificate revocation list checking;*
- *(optional) disable ad hoc wireless client-to-client connection capability;*
- *(optional) disable wireless network bridging capability (for example, bridging a connection between the WLAN and cellular radios on a smartphone so it can function as a hotspot);*
- *(optional) disable roaming capability;*
- *(optional) enable/disable IEEE 802.1X pre-authentication;*
- *(optional) enable/disable and configure PMK caching:*
  - *set the amount of time (in minutes) for which PMK entries are cached;*
  - *set the maximum number of PMK entries that can be cached.*

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

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

Assurance Activity	
TSS	There are no TSS assurance activities for this SFR.

AGD	The evaluator shall check to make sure that every management function mandated by the EP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Test	The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option listed in the requirement above. Note that the testing here may be accomplished in conjunction with the testing of other requirements, such as FCS_TLSC_EXT and FTA_WSE_EXT.

4.2.5 Class: Protection of the TSF (FPT)

FPT_TST_EXT TSF Cryptographic Functionality Testing

FPT_TST_EXT.1/WLAN TSF Cryptographic Functionality Testing (Wireless LAN)

FPT_TST_EXT.1.1/WLAN The [selection: TOE, TOE platform] shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2/WLAN The [selection: TOE, TOE platform] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

Application Note: *This SFR has been iterated in order to distinguish between the self-test functionality performed by the underlying platform and what is provided by the TSF.*

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

Assurance Activity	
TSS	The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.

AGD	The evaluator shall ensure that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.
Test	The evaluator shall perform the following tests: • Test 1: The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful. • Test 2: The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.

4.2.6 Class: TOE Access (FTA)

FTA_WSE_EXT Wireless Network Access

FTA_WSE_EXT.1 Wireless Network Access

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

Application Note: *The intent of this requirement is to allow the administrator to limit the access points to which the TOE is allowed to connect. The assignment is used by the ST author to specify the attributes (e.g., MAC Address, SSID, certificates, etc.) that can be used by the administrator to specify the acceptable access points.*

Assurance Activity	
TSS	The evaluator shall examine the TSS to determine that all of the attributes that can be used to specify acceptable networks (access points) are specifically defined.
AGD	The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.
Test	The evaluator shall also perform the following test for each attribute: • Test 1: The evaluator configures the TOE to allow a connection with a specific access point. The evaluator also configures the test environment such that the allowed access point and an access point that is not allowed are both "visible" to the TOE. The evaluator shall demonstrate that they can successfully establish a session with the allowed access point. The evaluator will then attempt to establish a session with the disallowed access point, and observe that the access attempt fails. • Test 2: The evaluator configures the TOE to allow a connection with a specific access point using EAP-TLS authentication (not only will the valid SSID be configured but the TOE will also be provided with certificates to complete the EAP-TLS authentication). The evaluator also configures the test environment such that an access point broadcasts the SSID the TOE has been configured to connect to but the authentication server does not have valid credentials. The evaluator will then attempt to establish a session with the valid SSID/invalid authentication server, and observe that the access attempt fails.

4.2.7 Class: Trusted Path/Channels (FTP)

FTP_ITC_EXT Trusted Channel Communication

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

FTP_ITC_EXT.1.1/WLAN The TSF shall use 802.11-2012, 802.1X, and EAP-TLS to provide a trusted communication channel between itself and a wireless access point that is logically distinct from other communication channels, provides assured identification of its end points, protects channel data from disclosure, and detects modification of the channel data.

FTP_ITC_EXT.1.2/WLAN The TSF shall initiate communication via the trusted channel for wireless access point connections.

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

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

Assurance Activity	
TSS	The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to an access point in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.
AGD	The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to the access point, and that it contains recovery instructions should a connection be unintentionally broken.
Test	The evaluator shall perform the following tests: • Test 1: The evaluators shall ensure that the TOE is able to initiate communications with an access point using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful. • Test 2: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. • Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.

	• Test 4: The evaluators shall physically interrupt the connection from the TOE to the access point (e.g., moving the TOE host out of range of the access point, turning the access point off). The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point. Further assurance activities are associated with the specific protocols.

4.3 Security Functional Requirements – OS PP Base

If this EP is extending the OS PP, the WLAN Client is expected to rely on the security functions implemented by the operating system as a whole and evaluated against the base PP. If a TOE claiming conformance to this EP is using the OS PP as the claimed base PP, the following sections describe any modifications that the ST author must make to the SFRs defined in the base PP in addition to what is mandated by section 4.2 above.

4.3.1 Inclusion of Additional Requirements

In order for the TOE to satisfy its defined security objectives, the OS PP claim must include all of the base requirements for the PP as well as the following additional SFRs:

4.3.2 Class: Cryptographic Support (FCS)

FCS_CKM_EXT.3 Cryptographic Key Destruction

Application Note: *This SFR exists in the OS PP and does not need to be modified for this EP. Note however that its scope is expanded to include keys and key material that are used by the TSF described by this EP. This SFR has not been iterated because it is assumed that the key destruction function is at least partially implemented by the underlying platform as opposed to the WLAN Client itself. For the purposes of this requirement, it is sufficient for the TOE to invoke the correct underlying functions of the host to perform the zeroization—it does not imply that the TOE has to include a kernel-mode memory driver to ensure the data are zeroized.*

Any security related information (such as keys, authentication data, and passwords) must be zeroized when no longer in use to prevent the disclosure or modification of security critical data.

The zeroization indicated above applies to each intermediate storage area for plaintext key/CSP (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/CSP to another location.

Additionally, although IEEE 802.11-2012 does not specify PMK lifetimes (described in IEEE 802.11-2012 Section 11.6.1.3) for Wireless LAN clients, these lifetimes should be limited, and the PMKSA cleared, in such a way as to prevent continued use of the same PMK for more than 24 hours. Thus, for PMKs, "when no longer needed" is after 24 hours.

FCS_COP.1 Cryptographic Operation

Application Note: *Several iterations of this SFR exist in the OS PP and do not need to be modified for this EP. Note however that their scope is expanded to include cryptographic operations that are required by the WLAN Client in order to perform its security functionality.*

FCS_RBG_EXT.1 Random Bit Generation

Application Note: *This SFR exists in the OS PP and does not need to be modified for this EP. Note however that its scope is expanded to include random bit generation functions that are required by the WLAN Client in order to perform its security functionality.*

4.4 Security Functional Requirements – MDF PP Base

If this EP is extending the MDF PP, the WLAN Client is expected to rely on the security functions implemented by the mobile device as a whole and evaluated against the base PP. If a TOE claiming conformance to this EP is using the MDF PP as the claimed base PP, the following sections describe any modifications that the ST author must make to the SFRs defined in the base PP in addition to what is mandated by section 4.2 above.

4.4.1 Class: Cryptographic Support (FCS)

FCS_CKM_EXT.4 Extended: Key Destruction

Application Note: *This SFR exists in the MDF PP and does not need to be modified for this EP. Note however that its scope is expanded to include keys and key material that are used by the TSF described by this EP. This SFR has not been iterated because it is assumed that the key destruction function is at least partially implemented by the underlying platform as opposed to the WLAN Client itself. For the purposes of this requirement, it is sufficient for the TOE to invoke the correct underlying functions of the host to perform the zeroization—it does not imply that the TOE has to include a kernel-mode memory driver to ensure the data are zeroized.*

Any security related information (such as keys, authentication data, and passwords) must be zeroized when no longer in use to prevent the disclosure or modification of security critical data.

The zeroization indicated above applies to each intermediate storage area for plaintext key/CSP (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/CSP to another location.

Additionally, although IEEE 802.11-2012 does not specify PMK lifetimes (described in IEEE 802.11-2012 Section 11.6.1.3) for Wireless LAN clients, these lifetimes should be limited, and the PMKSA cleared, in such a way as to prevent continued use of the same PMK for more than 24 hours. Thus, for PMKs, "when no longer needed" is after 24 hours.

FCS_COP.1 Cryptographic Operation

Application Note: *Several iterations of this SFR exist in the MDF PP and do not need to be modified for this EP. Note however that their scope is expanded to include cryptographic operations that are required by the WLAN Client in order to perform its security functionality.*

FCS_RBG_EXT.1 Random Bit Generation

Application Note: *This SFR exists in the MDF PP and does not need to be modified for this EP. Note however that its scope is expanded to include random bit generation functions that are required by the WLAN Client in order to perform its security functionality.*

5 Security Assurance Requirements

This EP does not define any SARs beyond those defined within the base PPs to which it can claim conformance. It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the OS PP or the MDF PP as well. These PPs both include a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance 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 this EP.

Appendix A - Rationale

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats addressed by WLAN Clients; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artifacts that can be used for the evaluation activities associated with this document.

A.1 Security Problem Definition

A.1.1 Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions are in addition to those defined in the base PPs and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3: TOE Assumptions

Assumption	Description of Assumption
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

A.1.2 Threats

The threats listed below are addressed by WLAN Clients. Note that these threats are in addition to those defined in the base PPs, all of which apply to WLAN Clients.

Table 4: Threats

Threat	Description of Threat
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

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

A.1.3 Organizational Security Policies

No organizational policies have been identified that are specific to WLAN Clients. However, all the organizational security policies in the base PPs apply to WLAN Clients.

A.1.4 Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

Table 5: Security Problem Definition Correspondence

Threat or Assumption	Security Objectives
A.NO_TOE_BYPASS	OE.NO_TOE_BYPASS
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN
T.TSF_FAILURE	O.TSF_SELF_TEST
T.UNAUTHORIZED_ACCESS	O.AUTH_COMM, O.CRYPTOGRAPHIC_FUNCTIONS, O.TOE_ADMINISTRATION, and O.WIRELESS_ACCESS_POINT_ CONNECTION
T.UNDETECTED_ACTIONS	O.SYSTEM_MONITORING

A.2 Security Objectives

A.2.1 Security Objectives for the TOE

The following table contains security objectives specific to WLAN Clients. These security objectives are in addition to those defined in the base PPs, all of which apply to WLAN Clients.

Table 6: Security Objectives for the TOE

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

O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide or use cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the TOE and its host environment.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.WIRELESS_ACCESS_POINT_CONNECTION	The TOE will provide the capability to restrict the wireless access points to which it will connect.

A.2.2 Security Objectives for the Operational Environment

The following table contains security objectives specific to the operational environments for WLAN Clients. These security objectives are in addition to those defined in the base PPs, all of which apply to the operational environments for WLAN Clients.

Table 7: Security Objectives for the OE

Objective	Objective Description
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

A.2.3 Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.

Appendix B - Optional Requirements

For this draft of the EP, this appendix contains additional components without supporting threats, objectives, rationale, or (in some cases) assurance activities. In tandem with the first review cycle, this supporting information will be developed and incorporated into the next release of the EP. Comments on the information contained in this section (both on whether the requirements contained are applicable to the potential conformant TOEs as well as requirements that are not contained in this appendix that are widely applicable to WLAN Client products) are welcome and solicited.

As indicated in the introduction to this EP, there are several capabilities that a TOE may implement and still be conformant to this EP. These capabilities are not required, creating a dependency on the IT environment (for instance, identification and authentication of administrators of the TOE). However, if a TOE does implement such capabilities, the ST will take the following information and include it in their ST.

B.1 Class: Identification and Authentication (FIA)

In the case that the TOE provides administrative capability, there are a number of requirements that can be applied to specify the capability, including remote administration, local administration, and protection of the administrative session. For this version of the EP, it is acceptable to use the administrative requirements from the Wireless Access System Protection Profile to specify such a capability for the client.

In the case that the TOE provides the capability to store and manage certificates used during the exchanges, the following SFR can be included in the ST. Note that this SFR is intended to be used if the certificate storage capability is actually provided by the TOE and not in cases where the TSF is relying on a storage mechanism provided by the underlying platform.

FIA_X509_EXT Certificate Validation

FIA_X509_EXT.4 Certificate Storage and Management

FIA_X509_EXT.4.1 The TSF shall store and protect certificate(s) from unauthorized deletion and modification

FIA_X509_EXT.4.2 The TSF shall provide the capability for authorized administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this EP.

Assurance Activity	
TSS	The evaluator shall examine the TSS to determine that it describes all certificate stores implemented that contain certificates used to meet the requirements of this EP. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access.
AGD	There are no AGD assurance activities for this requirement.

Test	The evaluator shall perform the following tests for each function in the system that requires the use of certificates: Test 1: The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.

B.2 **Audit Requirements**

Depending on the specific requirements selected by the ST author from this appendix, the ST author should include the appropriate auditable events in the corresponding table in the ST for the requirements selected.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.2/WLAN	Attempts to load certificates. Attempts to revoke certificates.	None.

Appendix C - Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements based on selections in the body of the EP; if certain selections are made, then additional requirements below will need to be included.

C.1 Class: Cryptographic Support (FCS)

FCS_TLSC_EXT.2/WLAN TLS Client Protocol

FCS_TLSC_EXT.2.1/WLAN The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1] and no other curves.

Application Note: *The ST author shall include this SFR if any ciphersuites beginning with 'TLS_ECDHE' are selected in FCS_TLSC_EXT.1/WLAN.*

This requirement limits the elliptic curves allowed for authentication and key agreement to the NIST curves from FCS_COP.1(3) (defined in the base PP) and FCS_CKM.1/WLAN and FCS_CKM.2/WLAN (defined in this EP).

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes the supported Elliptic Curves Extension and whether the required behavior is performed by default or may be configured.
AGD	If the TSS indicates that the supported Elliptic Curves Extension must be configured to meet the requirement, the evaluator shall verify that the operational guidance includes instructions on configuration of the supported Elliptic Curves Extension.
Test	The evaluator shall perform the following test: • Test 1: The evaluator shall configure the server to perform an ECDHE key exchange message in the TLS connection using a non-supported ECDHE curve (for example, P-192) and shall verify that the TSF disconnects after receiving the server's Key Exchange handshake message.

Appendix D - Objective Requirements

This section is reserved for requirements that are not currently prescribed by this EP but are expected to be included in future versions of the EP. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

There are no objective requirements currently defined for this EP.

Appendix E - References, Terminology, and Acronyms

[1] Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009

[2] Draft Consistency Instruction Manual, for Basic Robustness Environments, Release 4.0, CC version 3.1, 2008

[3] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001 (CHANGE NOTICES (12-03-2002))

[4] Federal Information Processing Standard Publication (FIPS-PUB) 180-3, Secure Hash Standard, October 2008

[5] Federal Information Processing Standard Publication (FIPS-PUB) 186-3, Digital Signature Standard (DSS), June 2009

[6] Federal Information Processing Standard Publication (FIPS-PUB) 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001

[7] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[8] NIST Special Publication 800-57, Recommendation for Key Management, March 2007

[9] NIST Special Publication 800-63, Electronic Authentication Guideline, April 2006

[10] NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) , March 2007

[11] NSA Glossary of Terms Used in Security and Intrusion Detection, Greg Stocksdale, NSA Information Systems Security Organization, April 1998. Need to update to CNSS 4009

[12] RFC 2865 Remote Authentication Dial In User Service (RADIUS), June 2000

[13] RFC 2868 RADIUS Attributes for Tunnel Protocol Support, June 2000

[14] RFC 3575 IANA Considerations for RADIUS, July 2003

[15] RFC 3579 RADIUS (Remote Authentication Dial In User Service Support For Extensible Authentication Protocol (EAP), September 2003

[16] RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003

[17] RFC 5216 The EAP-TLS Authentication Protocol, March 2008

[18] WPA2 Standard

[19] U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals Version 2.0, September 17, 2014

[20] U.S. Government Approved Protection Profile - Protection Profile for General Purpose Operating Systems Version 4.0, August 14, 2015

Access Point – provides the network interface that enables wireless client hosts access to 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 RF interface of the AP.

Administrator – a user that has administrative privilege to configure the TOE.

Authentication Server – an authentication server on the wired network which receives authentication credentials from wireless clients for authenticating.

Authentication Credentials – the information the system uses to verify that the user or administrator is authorized to access the TOE or network. Credentials can be as simple as username and password or stronger certificates.

Critical Security Parameter (CSP) – security related information, e.g. secret and private cryptographic keys, and authentication data such as passwords and PINs, whose disclosure or modification can compromise the security of a cryptographic module.

Entropy Source – this cryptographic function provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.

Extensible Authentication Protocol (EAP) – an authentication framework used in wireless networks. The TOE supports EAP-TLS. EAP-TLS uses PKI to authenticate both the authentication server and the wireless client.

FIPS-approved cryptographic function – a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either: 1) specified in a Federal Information Processing Standard (FIPS), or 2) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

IEEE 802.1X - IEEE standard for port-based network access control that defines an authentication mechanism to devices (wireless clients) to attach to a wired network. The main components needed to support IEEE 802.1X is the supplicant (wireless client), authenticator (the TOE), and authentication server.

IT Environment – hardware and software that are outside the TOE boundary that the support the TOE functionality and security policy.

Operational Environment – the environment in which the TOE is operated.

SAR (Security Assurance Requirements) – describes the development and evaluation methodologies for the developer and the lab to demonstrate compliance with the Security Functional Requirements. The SAR should describe specific tests for the developers and the evaluators.

SFR (Security Functional Requirement) – describes security functions that must be met by the TOE. The SFR's are tailored for the specific technology.

ST (Security Target) – describes and identifies the security properties of the TOE.

TOE (Target of Evaluation) – refers to a product or set of products that include hardware, software, and guidance that are to be evaluated against the requirements in this EP.

TOE Security Functionality (TSF) – a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) – a set of rules that regulate how assets are managed, protected and distributed within a TOE.

TOE Summary Specification (TSS) – a description of how the TOE satisfies all of the SFRs.

Unauthorized User – a user who has not been authorized by the administrator to use the TOE.

AES	Advanced Encryption Standard
AF	Authorization factor
AS	Authentication Server
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CM	Configuration management
COTS	Commercial Off-The-Shelf
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
DoD	Department of Defense
EAL	Evaluation Assurance Level
ES	Encryption Subsystem
FIPS	Federal Information Processing Standards
GCMP	Galois/Counter Mode Protocol
ISSE	Information System Security Engineers
IT	Information Technology
KDF	Key Derivation Function
OSP	Organizational Security Policy
PMK	Pairwise Master Key
PP	Protection Profile
PTK	Pairwise Temporal Key
PUB	Publication
RBG	Random Bit Generator
SAR	Security Assurance Requirements
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification