Supporting Document

Mandatory Technical Document

PP-Module for Virtual Private Network (VPN) Clients

October 2017

Version 2.1

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:

V2.1 October 2017 (Initial Release – version number of 2.1 chosen for consistency with the associated PP-Module)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of Virtual Private Network (VPN) clients. This primarily relates to the implementation of the IPsec protocol but includes other related functionality.

Field of special use:

Virtual Private Network (VPN) clients, regardless of whether they are bundled with a desktop/mobile OS or delivered as a standalone third-party application.

Acknowledgements:

This SD was developed with support from NIAP VPN Client 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 VPN Client PP-Module is to describe the security functionality of a virtual private network (VPN) client in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- Protection Profile for General Purpose Operating Systems (GPOS PP); or
- Protection Profile for Mobile Device Fundamentals (MDF PP); or
- Protection Profile for Application Software (App PP).

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

- PP-Module for Virtual Private Network (VPN) Clients, version 2.1

Although Assurance Activities are defined mainly for the evaluators to follow, in general they will also help Developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Assurance 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

Assurance Activities can be defined for both SFRs and Security Assurance Requirements (SAR). These are defined in separate sections of this SD.

If any Assurance 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 Assurance Activity may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation.

In general, if all Assurance 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 Assurance Activities have been successfully completed would require a specific justification from the evaluator as to why the Assurance Activities were not sufficient for that TOE.

Similarly, at the more granular level of Assurance Components, if the Assurance Activities for an Assurance Component and all of its related SFR Assurance 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 Assurance Activities have been successfully completed would require a specific justification from the evaluator as to why the Assurance Activities were not sufficient for that TOE.

1.3 Terminology

1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

Supplementary information — information that is not necessarily included in the ST or operational guidance, and that may not necessarily be public. Examples of such information could be entropy analysis, or description of a cryptographic key management architecture used in (or in support of) the TOE. The requirement for any such supplementary information will be identified in the relevant cPP (see description in section 4).

Administrator	A user that has administrative privilege to configure the TOE in privileged mode.
Authorized	An entity granted access privileges to an object, system or system entity.
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.
IT Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Operational Environment	The environment in which the TOE is operated.
Private Network	A network that is protected from access by unauthorized users or entities.
Privileged Mode	A TOE operational mode that allows a user to perform functions that require IT Environment administrator privileges.
Public Network	A network that is visible to all users and entities and does not protect against unauthorized access (e.g. internet).
Threat Agent	An entity that tries to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Unauthorized User	An entity (device or user) who has not been authorized by an authorized administrator to access the TOE or private network.
Unprivileged Mode	A TOE operational mode that only provides VPN client functions for the VPN Client user.
VPN Client	The TOE; allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to a private network
VPN Client User	A user operating the TOE in unprivileged mode.
VPN Gateway	A component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network

1.3.2 Acronyms

Acronym	**Meaning**
AES	Advanced Encryption Standard
CC	Common Criteria

CRL	Certificate Revocation List
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DN	Distinguished Name
ESP	Encapsulating Security Payload
GPOS	General Purpose Operating System
IKE	Internet Key Exchange
IP	Internet Protocol
IT	Information Technology
MDF	Mobile Device Fundamentals
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generator
RFC	Request for Comment
SA	Security Association
SAR	Security Assurance Requirement
SD	Supporting Document
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPD	Security Policy Database
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VPN	Virtual Private Network

2 Assurance 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 6.

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 cPP.

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 GPOS PP Assurance Activities

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 from Base-PP

2.1.1.1 Cryptographic Support (FCS)

2.1.1.1.1 Cryptographic Key Management (FCS_CKM)

FCS_CKM.1(1) Cryptographic Key Generation

Refer to the Assurance Activity for FCS_CKM.1(1) in the GPOS PP for evaluating this SFR.

FCS_CKM.2(1) Cryptographic Key Establishment

For all key establishment schemes that conform to NIST SP 800-56A or 800-56B, refer to the Assurance Activity for FCS_CKM.2(1) in the GPOS PP.

If "Key establishment scheme using Diffie-Hellman group 14…" is selected, the evaluator shall ensure that the TSS describes how the implementation meets RFC 3526 Section 3. The evaluator shall also verify the correctness of the TSF's implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in FTP_ITC_EXT.1 and FTP_TRP.1 in the GPOS PP that uses Diffie-Hellman group 14. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum.

2.1.1.1.2 Cryptographic Operation (FCS_COP)

FCS_COP.1(1) Cryptographic Operation (Encryption and Decryption)

Refer to the Assurance Activity for FCS_COP.1(1) in the GPOS PP for evaluating this SFR.

2.1.2 Additional SFRs

2.1.2.1 Cryptographic Support (FCS)

2.1.2.1.1 Cryptographic Key Management (FCS_CKM)

FCS_CKM.1/VPN Cryptographic Key Generation (IKE)

TSS

The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.

Operational Guidance

There are no AGD Assurance Activities for this requirement.

Test

There are no test Assurance Activities for this requirement.

FCS_CKM_EXT.2 Cryptographic Key Storage

TSS

Regardless of whether this requirement is met by the VPN client or the OS, the evaluator will check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and how it is stored.

The evaluator shall review the TSS for to determine that it makes a case that, for each item listed as being manipulated by the VPN client, it is not written unencrypted to persistent memory, and that the item is stored by the OS.

Operational Guidance

There are no AGD Assurance Activities for this requirement.

Test

There are no test Assurance Activities for this requirement.

2.1.2.2 Identification and Authentication (FIA)

2.1.2.2.1 Certificate Use and Management (FIA_X509)

FIA_X509_EXT.3 X.509 Certificate Use and Management

The Assurance Activities below apply to FIA_X509_EXT.3.2. FIA_X509_EXT.3.1 is evaluated as part of FCS_IPSEC_EXT.1 (and conditionally as part of FPT_TUD_EXT.1 and/or FPT_TST_EXT.1) and FIA_X509_EXT.3.3 is evaluated as part of FCS_IPSEC_EXT.1.11.

TSS

The evaluator shall check the TSS to ensure that it describes whether the VPN client or the OS implements the certificate validation functionality, how the VPN client/OS chooses which certificates

to use, and any necessary instructions in the administrative guidance for configuring the OS so that desired certificates can be used.

The evaluator shall examine the TSS to confirm that it describes the behavior of the client/OS when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

Operational Guidance
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.

Test
The evaluator shall perform the following test regardless of whether the certificate validation functionality is implemented by the VPN client or by the OS:

Test 1: The evaluator shall demonstrate that 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.3.2 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.

2.1.2.3 Trusted Paths/Channels (FTP)

2.1.2.3.1 Trusted Channel Communication (FTP_ITC)

FTP_ITC.1 Inter-TSF Trusted Channel

TSS
The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN gateway and/or VPN client and/or IPsec-capable network device 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.

Operational Guidance
The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to a VPN gateway and/or VPN client and/or IPsec-capable network device, 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 a VPN gateway and/or VPN client and/or IPsec-capable network device 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 IPsec peer, the channel data is not sent in plaintext.

Test 3: The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE.

Test 4: The evaluators shall physically interrupt the connection from the TOE to the IPsec peer. 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 requirements for FCS_IPSEC_EXT.1.

2.2 MDF PP Assurance Activities

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 from Base-PP

2.2.1.1 Cryptographic Support (FCS)

2.2.1.1.1 Cryptographic Key Management (FCS_CKM)

FCS_CKM.1 Cryptographic Key Generation

Refer to the Assurance Activity for FCS_CKM.1 in the MDF PP.

FCS_CKM.2(1) Cryptographic Key Establishment

For all key establishment schemes that conform to NIST SP 800-56A or 800-56B, refer to the Assurance Activity for FCS_CKM.2(1) in the MDF PP.

If “Key establishment scheme using Diffie-Hellman group 14…” is selected, the evaluator shall ensure that the TSS describes how the implementation meets RFC 3526 Section 3. The evaluator shall also verify the correctness of the TSF’s implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in FTP_ITC_EXT.1 in the MDF PP that uses Diffie-Hellman group 14. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum.

2.2.1.1.2 Cryptographic Operation (FCS_COP)

FCS_COP.1.1(1) Cryptographic Operation (Encryption/ Decryption)

Refer to the Assurance Activity for FCS_COP.1(1) in the MDF PP.

2.2.1.2 Identification and Authentication (FIA)

2.2.1.2.1 X.509 Certificate Use and Management (FIA_X509_EXT)

FIA_X509_EXT.2 X.509 Certificate Authentication.

Refer to the Assurance Activity for FIA_X509_EXT.2 in the MDF PP.

2.2.1.3 Trusted Paths/Channels (FTP)

2.2.1.3.1 Trusted Channel Communication (FTP_ITC_EXT)

FTP_ITC_EXT.1 Trusted Channel Communication

Refer to the Assurance Activity for FTP_ITC_EXT.1 in the MDF PP.

2.2.2 Additional SFRs

2.2.2.1 Cryptographic Support (FCS)

2.2.2.1.1 Cryptographic Key Management (FCS_CKM)

FCS_CKM.1/VPN Cryptographic Key Generation (IKE)

TSS

The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.

Operational Guidance

There are no AGD Assurance Activities for this requirement.

Test

There are no test Assurance Activities for this requirement.

2.3 App PP Assurance Activities

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

2.3.1 Modified SFRs from Base-PP

2.3.2 Cryptographic Support (FCS)

2.3.2.1 Cryptographic Key Establishment (FCS_CKM)

2.3.2.1.1 FCS_CKM.1(1) Cryptographic Asymmetric Key Generation

Refer to the Assurance Activity for FCS_CKM.1(1) in the App PP.

2.3.2.1.2 FCS_CKM.2 Cryptographic Key Establishment

For all key establishment schemes that conform to NIST SP 800-56A or 800-56B, refer to the Assurance Activity for FCS_CKM.2 in the App PP.

If “Key establishment scheme using Diffie-Hellman group 14…” is selected, the evaluator shall ensure that the TSS describes how the implementation meets RFC 3526 Section 3. The evaluator shall also verify the correctness of the TSF’s implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in FTP_DIT_EXT.1 in the App PP that uses Diffie-Hellman group 14. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum.

2.3.2.2 Cryptographic Key Establishment (FCS_CKM_EXT)

2.3.2.2.1 FCS_CKM_EXT.1 Cryptographic Key Generation Services

This SFR is evaluated in conjunction with FCS_CKM.1(1) in the App PP.

2.3.2.3 Cryptographic Operation (FCS_COP)

2.3.2.3.1 FCS_COP.1(1) Cryptographic Operation – Encryption/Decryption

Refer to the Assurance Activity for FCS_COP.1(1) in the App PP.

2.3.2.4 Identification and Authentication (FIA)

2.3.2.4.1 Certificate Use and Management (FIA_X509_EXT)

FIA_X509_EXT.2 Certificate Authentication.

Refer to the Assurance Activity for FIA_X509_EXT.2 in the App PP.

2.3.3 Trusted Paths/Channels (FTP)

2.3.3.1 Protection of Data in Transit (FTP_DIT)

2.3.3.1.1 FTP_DIT_EXT.1 Protection of Data in Transit.

Refer to the Assurance Activity for FTP_DIT_EXT.1 in the App PP.

2.3.4 Additional SFRs

2.3.4.1 Cryptographic Support (FCS)

2.3.4.1.1 Cryptographic Key Establishment (FCS_CKM_EXT)

FCS_CKM_EXT.2 Cryptographic Key Storage

TSS

Regardless of whether this requirement is met by the TOE or the TOE platform, the evaluator will check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator then performs the following actions:

Persistent secrets and private keys manipulated by the platform

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the persistent secrets and private keys listed as being stored by the platform in the VPN client ST are identified as being protected in that platform's ST.

Persistent secrets and private keys manipulated by the TOE

The evaluator reviews the TSS for to determine that it makes a case that, for each item listed as being manipulated by the TOE, it is not written unencrypted to persistent memory, and that the item is stored by the platform.

Operational Guidance
There are no AGD Assurance Activities for this requirement.

Test
There are no test Assurance Activities for this requirement.

FCS_CKM_EXT.4 Cryptographic Key Destruction

TSS
The evaluator shall ensure that all plaintext secret and private cryptographic keys and CSPs (whether manipulated by the TOE or exclusively by the platform) are identified in the VPN Client ST's TSS, and that they are accounted for by the Assurance Activities in this section.

Requirement met by the platform

The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate key that are not otherwise covered by the FCS_CKM_EXT.4 requirement levied on the TOE.

For each platform listed in the ST, the evaluator shall examine the TSS of the ST of the platform to ensure that each of the secret keys, private keys, and CSPs used to generate key listed above are covered.

Requirement met by the TOE

The evaluator shall check to ensure the TSS describes when each of the plaintext keys are cleared (e.g., system power off, disconnection of an IPsec connection, when no longer needed by the VPN channel per the protocol); and the type of clearing procedure that is performed (cryptographic erase, overwrite with zeros, overwrite three or more times by a different alternating pattern, overwrite with random pattern, or block erase). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting three times with a random pattern that is changed before each write").

Operational Guidance
There are no AGD Assurance Activities for this requirement.

Test
For each key clearing situation described in the TSS, the evaluator shall repeat the following test.

Test 1: The evaluator shall utilize appropriate combinations of specialized operational environment and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

Cryptographic TOE implementations in software shall be loaded and exercised under a debugger to perform such tests. The evaluator shall perform the following test for each key subject to clearing, including intermediate copies of keys that are persisted encrypted by the TOE:

1. Load the instrumented TOE build in a debugger.

2. Record the value of the key in the TOE subject to clearing.
3. Cause the TOE to perform a normal cryptographic processing with the key from #1.
4. Cause the TOE to clear the key.
5. Cause the TOE to stop the execution but not exit.
6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file.
7. Search the content of the binary file created in #4 for instances of the known key value from #1.

The test succeeds if no copies of the key from #1 are found in step #7 above and fails otherwise.

The evaluator shall perform this test on all keys, including those persisted in encrypted form, to ensure intermediate copies are cleared.

2.4 TOE SFR Assurance Activities

2.4.1 Cryptographic Support (FCS)

2.4.1.1 IPsec (FCS_IPSEC_EXT)

2.4.1.1.1 FCS_IPSEC_EXT.1.1 IPsec

TSS

The evaluator shall examine the TSS and determine that it describes how the IPsec capabilities are implemented and how a packet is processed, e.g., what takes place at the platform and what takes place within the client. The TSS will detail the relationship between the client and the underlying platform, including which aspects are implemented by the client, and those that are provided by the underlying platform. The TSS describes how the client interacts with the platforms network stack (e.g., does the client insert itself within the stack via kernel mods, does the client simply invoke APIs to gain access to network services).

If the SPD is implemented by the client, then the TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how the available rules and actions form the SPD using terms defined in RFC 4301 such as BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA. If the SPD is implemented by the underlying platform, then the TSS describes how the client interacts with the platform to establish and populate the SPD, including the identification of the platform's interfaces that are used by the client.

Operational Guidance
The evaluator shall examine the operational guidance to verify it describes how the SPD is created and configured. If there is an administrative interface to the client, then the guidance describes how the administrator specifies rules for processing a packet. The description includes all three cases - a rule that ensures packets are encrypted/decrypted, dropped, and allowing a packet to flow in plaintext. The evaluator shall determine that the description in the operational guidance is consistent with the description in the TSS, and that the level of detail in the operational guidance is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

If the client is configured by an external application, such as the VPN gateway, then the operational guidance should indicate this and provide a description of how the client is configured by the external application. The description should contain information as to how the SPD is established and set up in an unambiguous fashion. The description should also include what is configurable via the external application, how ordering of entries may be expressed, as well as the impacts that ordering of entries may have on the packet processing.

In either case, the evaluator ensures the description provided In the TSS is consistent with the capabilities and description provided in the operational guidance.

Test
Depending on the implementation, the evaluator may be required to use a VPN gateway or some form of application to configure the client and platform. For Test 2, the evaluator is required to choose an application that allows for the configuration of the full set of capabilities of the VPN client (in conjunction with the platform). For example, if the client provides a robust interface that allows for specification of wildcards, subnets, etc., it is unacceptable for the evaluator to choose a VPN Gateway that only allows for specifying a single fully qualified IP addresses in the rule.

The evaluator shall perform the following tests:

Test 1: The evaluator shall configure an SPD on the client that is capable of the following: dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the client with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule. The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed through without modification, was encrypted by the IPsec implementation.

Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and operational guidance. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the operational guidance.

2.4.1.1.2 FCS_IPSEC_EXT.1.2

TSS

The evaluator shall check the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected). The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

Operational Guidance
If both transport mode and tunnel mode are implemented, the evaluator shall review the operational guidance to determine how the use of a given mode is specified.

Test
The evaluator shall perform the following test(s) based on the selections chosen:

Test 1 [conditional]: If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE/platform to operate in tunnel mode and also configures a VPN gateway to operate in tunnel mode. The evaluator configures the TOE/platform and the VPN gateway to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the VPN GW peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.

Test 2 [conditional]: If transport mode is selected, the evaluator uses the operational guidance to configure the TOE/platform to operate in transport mode and also configures an IPsec peer to accept IPsec connections using transport mode. The evaluator configures the TOE/platform and the endpoint device to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE/platform to connect to the remote endpoint. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.

Test 3 [conditional]: If both tunnel mode and transport mode are selected, the evaluator shall perform both Test 1 and Test 2 above, demonstrating that the TOE can be configured to support both modes.

Test 4 [conditional]: If both tunnel mode and transport mode are selected, the evaluator shall modify the testing for FCS_IPSEC_EXT.1 to include the supported mode for SPD PROTECT entries to show that they only apply to traffic that is transmitted or received using the indicated mode.

2.4.1.1.3 FCS_IPSEC_EXT.1.3

TSS
The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Operational Guidance
The evaluator checks that the operational guidance provides instructions on how to construct or acquire the SPD and uses the guidance to configure the TOE/platform for the following test.

Test
The evaluator shall perform the following test:

Test 1: The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, PROTECT, and (if applicable) BYPASS network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE/platform created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE's interfaces.

2.4.1.1.4 FCS_IPSEC_EXT.1.4

TSS
The evaluator shall examine the TSS to verify that the algorithms AES-GCM-128 and AES-GCM-256 are implemented. If the ST author has selected either AES-CBC-128 or AES-CBC-256 in the requirement, then the evaluator verifies the TSS describes these as well. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(4) Cryptographic Operations (for keyed-hash message authentication).

Operational Guidance
The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.

Test
Test 1: The evaluator shall configure the TOE/platform as indicated in the operational guidance configuring the TOE/platform to using each of the AES-GCM-128, and AES-GCM-256 algorithms, and attempt to establish a connection using ESP. If the ST Author has selected either AES-CBC-128 or AES-CBC-256, the TOE/platform is configured to use those algorithms and the evaluator attempts to establish a connection using ESP for those algorithms selected.

2.4.1.1.5 FCS_IPSEC_EXT.1.5

TSS
The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented. If IKEv1 is implemented, the evaluator shall verify that the TSS indicates whether or not XAUTH is supported, and that aggressive mode is not used for IKEv1 Phase 1 exchanges (i.e. only main mode is used). It may be that these are configurable options.

Operational Guidance
The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE/platform to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE/platform to perform NAT traversal for the test below. If XAUTH is implemented, the evaluator shall verify that the operational guidance provides instructions on how it is enabled or disabled.

If the TOE supports IKEv1, the evaluator shall verify that the operational guidance either asserts that only main mode is used for Phase 1 exchanges, or provides instructions for disabling aggressive mode.

Test
Test 1: The evaluator shall configure the TOE/platform so that it will perform NAT traversal processing as described in the TSS and RFC 7296, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed. If XAUTH is supported, the evaluator shall verify that this test can be repeated with XAUTH both enabled and disabled in the manner specified by the operational guidance.

Test 2 [conditional]: If the TOE supports IKEv1, the evaluator shall perform any applicable operational guidance steps to disable the use of aggressive mode and then attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator shall show that the TOE/platform will reject a VPN gateway from initiating an IKEv1 Phase 1 connection in aggressive mode. The evaluator should then show that main mode exchanges are supported.

2.4.1.1.6 FCS_IPSEC_EXT.1.6

TSS
The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Operational Guidance
The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.

Test
The evaluator shall use the operational guidance to configure the TOE/platform (or to configure the Operational Environment to have the TOE receive configuration) to perform the following test for each ciphersuite selected:

Test 1: The evaluator shall configure the TOE/platform to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation. The evaluator will confirm that the connection is successful by confirming that data can be passed through the connection once it is established. For example, the evaluator may connect to a webpage on the remote network and verify that it can be reached.

2.4.1.1.7 FCS_IPSEC_EXT.1.7

TSS
There are no TSS Assurance Activities for this requirement.

Operational Guidance
The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE configures the values for SA lifetimes. In addition, the evaluator shall check that the guidance has the option for either the Administrator or VPN Gateway to configure Phase 1 SAs if time-based limits are supported. Currently there are no values mandated for the number of packets or number of

bytes, the evaluator shall simply check the operational guidance to ensure that this can be configured if selected in the requirement.

Test
When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

Test 1 [conditional]: The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.

Test 2 [conditional]: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

Test 3 [conditional]: The evaluator shall perform a test similar to Test 2 for Phase 2 SAs, except that the lifetime will be 8 hours or less instead of 24 hours or less.

Test 4 [conditional]: If a fixed limit for IKEv1 SAs is supported, the evaluator shall establish an SA and observe that the connection is closed after the fixed traffic and/or time value is reached.

2.4.1.1.8 FCS_IPSEC_EXT.1.8

TSS
The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

Operational Guidance
There are no AGD Assurance Activities for this requirement.

Test
The evaluator shall perform the following test:

Test 1: For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group..

2.4.1.1.9 FCS_IPSEC_EXT.1.9

TSS

The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x" (as defined in FCS_IPSEC_EXT.1.9) and each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this EP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

Operational Guidance
There are no AGD Assurance Activities for this requirement.

Test
There are no test Assurance Activities for this requirement.

2.4.1.1.10 FCS_IPSEC_EXT.1.10

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.9.

2.4.1.1.11 FCS_IPSEC_EXT.1.11

TSS
The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication.

If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for TOEs/platforms that can generate a pre-shared key as well as TOEs/platforms that simply use a pre-shared key.

The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include whether the certificate presented identifier is compared to the ID payload presented identifier, which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN), and, if multiple fields are supported, the logical order comparison. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate.

Operational Guidance
The evaluator shall check that the operational guidance describes how pre-shared keys are to be generated and established.

The evaluator ensures the operational guidance describes how to set up the TOE/platform to use the cryptographic algorithms RSA and/or ECDSA.

In order to construct the environment and configure the TOE/platform for the following tests, the evaluator will ensure that the operational guidance also describes how to configure the TOE/platform to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE/platform as a trusted CA.

The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifier(s) for the peer.

Test
For efficiency's sake, the testing that is performed here has been combined with the testing for **FIA_X509_EXT.2.1** (for IPsec connections), **FCS_IPSEC_EXT.1.12**, **FCS_IPSEC_EXT.1.13** and

FIA_X509_EXT.2.3. The following tests shall be repeated for each peer authentication protocol selected in the **FCS_IPSEC_EXT.1.11** selection above:

Test 1: The evaluator shall have the TOE/platform generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE/platform and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE/platform a previously generated private key and corresponding certificate.

Test 2: The evaluator shall use a certificate signed using the RSA or ECDSA algorithm to authenticate the remote peer during the IKE exchange. This test ensures the remote peer has the certificate for the trusted CA that signed the TOE's certificate and it will do a bit-wise comparison on the DN. This bit-wise comparison of the DN ensures that not only does the peer have a certificate signed by the trusted CA, but the certificate is from the DN that is expected. The evaluator will configure the TOE/platform to associate a certificate (e.g., a certificate map in some implementations) with a VPN connection. This is what the DN is checked against.

Test 3: The evaluator shall test that the TOE/platform can properly handle revoked certificates – conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this draft of the PP-Module, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE/platform will not establish an SA.

Test 4 [conditional]: The evaluator shall test that given a signed certificate from a trusted CA, that when the DN does not match – any of the four fields can be modified such that they do not match the expected value, that an SA does not get established.

Test 5 [conditional]: The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection with the VPN GW peer. If the generation of the pre-shared key is supported, the evaluator shall ensure that establishment of the key is carried out for an instance of the TOE/platform generating the key as well as an instance of the TOE/platform merely taking in and using the key.

For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:

Test 6: For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.

Test 7: For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.

The following tests are conditional:

Test 8 [conditional]: If, according to the TSS, the TOE supports both Common Name and SAN certificate fields and uses the preferred logic outlined in the Application Note, the tests above with the Common Name field shall be performed using peer certificates with no SAN extension. Additionally, the evaluator shall configure the peer's reference identifier on the TOE to not match

the SAN in the peer's presented certificate but to match the Common Name in the peer's presented certificate, and verify that the IKE authentication fails.

Test 9 [conditional]: If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds. To demonstrate a bit-wise comparison of the DN, the evaluator shall change a single bit in the DN (preferably, in an Object Identifier (OID) in the DN) and verify that the IKE authentication fails.

Test 10 [conditional]: If the TOE supports both IPv4 and IPv6 and supports IP address identifier types, the evaluator must repeat test 1 and 2 with both IPv4 address identifiers and IPv6 identifiers. Additionally, the evaluator shall verify that the TOE verifies that the IP header matches the identifiers by setting the presented identifiers and the reference identifier with the same IP address that differs from the actual IP address of the peer in the IP headers and verifying that the IKE authentication fails.

Test 11 [conditional]: If, according to the TSS, the TOE performs comparisons between the peer's ID payload and the peer's certificate, the evaluator shall repeat the following test for each combination of supported identifier types and supported certificate fields (as above). The evaluator shall configure the peer to present a different ID payload than the field in the peer's presented certificate and verify that the TOE fails to authenticate the IKE peer.

2.4.1.1.12 FCS_IPSEC_EXT.1.12

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

2.4.1.1.13 FCS_IPSEC_EXT.1.13

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

2.4.1.1.14 FCS_IPSEC_EXT.1.14

TSS

The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.

Operational Guidance

There are no AGD Assurance Activities for this requirement.

Test

The evaluator follows the guidance to configure the TOE/platform to perform the following tests.

Test 1: This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.

Test 2 [conditional]: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.

Test 3: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.

Test 4: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.

2.4.2 User Data Protection (FDP)

2.4.2.1 Residual Information Protection (FDP_RIP)

2.4.2.1.1 FDP_RIP.2 Full Residual Information Protection

TSS
Requirement met by the platform

The evaluator shall examine the TSS to verify that it describes (for each supported platform) the extent to which the client processes network packets and addresses the FDP_RIP.2 requirement.

Requirement met by the TOE

"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

Operational Guidance
There are no AGD Assurance Activities for this requirement.

Test
There are no test Assurance Activities for this requirement.

2.4.3 Security Management (FMT)

2.4.3.1 Specification of Management Functions (FMT_SMF)

2.4.3.1.1 FMT_SMF.1/VPN Specification of Management Functions (VPN)

TSS
The evaluator shall check to ensure the TSS describes the client credentials and how they are used by the TOE.

Operational Guidance
The evaluator shall check to make sure that every management function mandated in the ST for this requirement are described in the operational guidance and that the description contains the information required to perform the management duties associated with each management function.

Test
The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE according to the operational guidance and testing each management activity listed in the ST.

The evaluator shall ensure that all management functions claimed in the ST can be performed by completing activities described in the AGD. Note that this may be performed in the course of completing other testing.

2.4.4 Protection of the TSF (FPT)

2.4.4.1 TSF Self-Test (FPT_TST_EXT)

2.4.4.1.1 FPT_TST_EXT.1 TSF Self-Test

Except for where it is explicitly noted, the evaluator is expected to check the following information regardless of whether the functionality is implemented by the TOE or by the TOE platform.

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. If some of the tests are performed by the TOE platform, the evaluator shall check the TSS to ensure that those tests are identified, and that the ST for each platform contains a description of those tests. Note that the tests that are required by this component are those that support security functionality in this PP-Module, which may not correspond to the set of all self-tests contained in the platform STs.

The evaluator shall examine the TSS to ensure that it describes how the integrity of stored TSF executable code is cryptographically verified 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 shall check to ensure that the cryptographic requirements listed are consistent with the description of the integrity verification process.

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. For checks implemented entirely by the platform, the evaluator ensures that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

Operational Guidance
If not present in the TSS, the evaluator ensures that the operational guidance describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. For

checks implemented entirely by the platform, the evaluator ensures that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

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.

3 Assurance Activities for Optional Requirements

There are currently no optional requirements defined by the PP-Module.

4 Assurance Activities for Selection-Based Requirements

4.1 Identification and Authentication (FIA)

4.1.1 Pre-Shared Key Composition (FIA_PSK_EXT)

4.1.1.1 FIA_PSK_EXT.1 Pre-Shared Key Composition

TSS
The evaluator shall also 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.

Requirement met by the platform

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the functions associated with pre-shared keys claimed in that platform's ST contains the same functions specified in the VPN Client's ST. If the TOE does not perform any management or input of the pre-shared keys then no further activity is required.

Requirement met by the TOE

The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported. The evaluator shall also confirm that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the FIA_PSK_EXT.1.3.

Operational Guidance
If the TOE supports bit-based pre-shared keys, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre- shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also 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.

The evaluator shall check that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.

Requirement met by the TOE

The evaluator shall examine the operational guidance to determine that it provides guidance 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 merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must include, at minimum, the same items contained in FIA_PSK_EXT.1.2.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall 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 shall repeat Test 1 using the minimum length; the maximum length; and invalid lengths that are below the minimum length, above the maximum length, null length, empty length, or zero length. The minimum and maximum length tests should be successful, and the invalid lengths must be rejected by the TOE.

Test 3 [conditional]: If the TOE supports but does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it per the instructions in the operational guidance. The evaluator shall 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 shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

5 Assurance Activities for Objective Requirements

5.1 Security Audit (FAU)

5.1.1 Security Audit Data Generation (FAU_GEN)

5.1.1.1 FAU_GEN.1 Audit Data Generation

TSS
The evaluator shall examine the TSS to determine that it describes the auditable events and the component that is responsible for each type of auditable event.

Operational Guidance
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 PP-Module 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 C-1 of the PP-Module.

In particular, the evaluator shall ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In Table C-1 of the PP-Module, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP-Module. The TOE may contain functionality that is not evaluated in the context of this PP-Module because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP-Module, which thus form the set of “all administrative actions”. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.

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 PP-Module. Additionally, the evaluator shall test that each administrative action applicable in the context of this PP-Module is auditable. 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.

5.1.2 Security Audit Event Selection (FAU_SEL)

5.1.2.1 FAU_SEL.1 Selective Audit

TSS
There are no TSS Assurance Activities for this SFR.

Operational Guidance
The evaluator shall review the administrative guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain instructions on how to set the pre-selection, or how the VPN gateway will configure the client, as well as explain the syntax (if present) for multi-value pre-selection. The administrative guidance shall also identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.

Test
The evaluator shall perform the following tests:

Test 1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.

Test 2 [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

5.2 User Data Protection (FDP)

5.2.1 Subset Information Flow Control (FDP_IFC_EXT)

5.2.1.1 FDP_IFC_EXT.1 Information Flow Control

TSS
The evaluator shall verify that the TSS section of the ST describes the routing of IP traffic through processes on the TSF when a VPN client is enabled. The evaluator shall ensure that the description indicates which traffic does not go through the VPN and which traffic does and that a configuration exists for each baseband protocol in which only the traffic identified by the ST author as necessary for establishing the VPN connection (IKE traffic and perhaps HTTPS or DNS traffic) is not encapsulated by the VPN protocol (IPsec). The ST author shall also identify in the TSS section any differences in the routing of IP traffic when using any supported baseband protocols (e.g. WiFi or, LTE).

Operational Guidance

The evaluator shall verify that the following is addressed by the documentation:

- The description above indicates that if a VPN client is enabled, all configurations route all IP traffic (other than IP traffic required to establish the VPN connection) through the VPN client.
- The AGD guidance describes how the user and/or administrator can configure the TSF to meet this requirement.

Test
The evaluator shall perform the following test:

Step 1 - The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an Internet-connected network. The evaluator shall turn on the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other Internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data.

Step 2 - The evaluator shall configure an IPsec VPN client that supports the routing specified in this requirement, and if necessary, configure the device to perform the routing specified as described in the AGD guidance. The evaluator shall turn on the sniffing tool, establish the VPN connection, and perform the same actions with the device as performed in the first step. The evaluator shall verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data.

Step 3 - The evaluator shall examine the traffic from both step one and step two to verify that all IP traffic, aside from and after traffic necessary for establishing the VPN (such as IKE, DNS, and possibly HTTPS), is encapsulated by IPsec.

Step 4 - The evaluator shall attempt to send packets to the TOE outside the VPN connection and shall verify that the TOE discards them.

6 Assurance Activities for SARs

The PP-Module 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 the PP-Module is inherently evaluated against the GPOS PP, MDF PP, or App PP as well. These PPs both include a number of Assurance Activities associated with both SFRs and SARs. Additionally, the PP-Module 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 the PP-Module.

7 Required Supplementary Information

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

8 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model
CCMB-2012-09-001, Version 3.1 Revision 5, April 2017

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2012-09-002, Version 3.1 Revision 5, April 2017

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2012-09-003, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2012-09-004, Version 3.1 Revision 5, April 2017

[APP PP] Protection Profile for Application Software, Version 1.2, 25 April 2016

[GPOS PP] Protection Profile for General Purpose Operating Systems, Version 4.1, 09 March 2016

[MDF PP] Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017

[VPN Module] PP-Module for Virtual Private Network (VPN) Clients Version 2.1, 5 October 2017