Supporting Document
Mandatory Technical Document

PP-Module for Virtual Private Network (VPN) Clients
Version: 2.2
2021-01-05
National Information Assurance Partnership

Foreword

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

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

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
2.1	2019-11-14	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Virtual Private Network (VPN) Clients products.

Acknowledgements:
This SD was developed with support from NIAP Virtual Private Network (VPN) Clients Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Virtual Private Network (VPN) Clients is to describe the security functionality of Virtual Private Network (VPN) Clients products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PPs:

- Protection Profile for , Version
- Protection Profile for , Version
- Protection Profile for , Version
- Protection Profile for Mobile Device Management, Version

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

- Virtual Private Network (VPN) Clients, Version 2.2

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activites to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the

evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

The following sections list Common Criteria and technology terms used in this document.

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of	

Evaluation (TOE)	The product under evaluation.

1.3.2 Technical Terms

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.

2 Evaluation Activities for SFRs

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

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator’s verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator’s verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer’s tests are executing both in the

manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for

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

2.1.1 Modified SFRs

2.1.1.1 Cryptographic Support (FCS)

The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The OS shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECC schemes using “NIST curves” P-256, P-384, and P-521 no other curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.4, and, RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.3, FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.1, FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, FFC Schemes using safe primes that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes, No other key generation methods and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]. This SFR is functionally identical to what is defined in the GPOS PP except that ECC key generation with support for P-256 and P-384 has been made mandatory in support of IPsec due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. The ST author must select all key generation schemes used for key establishment and entity authentication. When key generation is used for key establishment, the schemes in FCS_CKM.2 and selected cryptographic protocols must match the selection. When key generation is used for entity authentication, the public key is expected to be associated with an X.509v3 certificate. If the OS acts only as a receiver in the RSA key establishment scheme, the OS does not need to implement RSA key generation. Refer to the evaluation activity for FCS_CKM.1 in the GPOS PP for evaluating this SFR. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The OS shall implement functionality to perform cryptographic key establishment in accordance with a specified key establishment method: Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” and RSA-based key establishment schemes that meets the following: RSAESPKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2, Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, No other key establishment schemes that meets the following [assignment: list of standards]. The ST author must select all key establishment schemes used for the selected cryptographic protocols. The elliptic curves used for the key establishment scheme must correlate with the curves specified in FCS_CKM.1.1. The domain parameters used for the finite field-based key establishment scheme are specified by the key generation according to FCS_CKM.1.1. Refer to the Assurance Activity for FCS_CKM.2.1 in the GPOS PP for evaluating this SFR. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum. The SFR is refined to list an additional AES mode that must be supported to address VPN client requirements; the use of this mode for VPN connectivity does not impact the ability of the OS to satisfy any of its other security requirements. The OS shall perform encryption/decryption services for data in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A), AES-GCM (as defined in NIST SP 800-38D), and AES-XTS (as defined in NIST SP 800-38E), AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012) AES Key Wrap (KW) (as defined in NIST SP 800-38F) AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F) AES-CCM (as defined in NIST SP 800-38C) AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013) No other modes and cryptographic key sizes 128-bit 256-bit . This SFR is identical to what is defined in the GPOS PP except that support for CBC and GCM mode is mandatory in order to address the requirements for FCS_IPSEC_EXT.1. In addition, both 128-bit and 256-bit for key sizes must be selected in order to meet the requirements for FCS_IPSEC_EXT.1. Refer to the EA for FCS_COP.1(1) in the GPOS PP for evaluating this SFR.

FCS_CKM.1 Cryptographic Key Generation

Refer to the evaluation activity for FCS_CKM.1 in the GPOS PP for evaluating this SFR.

FCS_CKM.2 Cryptographic Key Establishment

Refer to the Assurance Activity for FCS_CKM.2.1 in the GPOS PP for evaluating this SFR. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum.

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

Refer to the EA 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)

Components in this family describe requirements for key management functionality such as key storage and destruction. Storage of key data related to VPN functionality can be accomplished using the same mechanism defined by FCS_STO_EXT.1 in the OS PP. requires the TSF to securely store key data when not in use No specific management functions are identified. There are no auditable events foreseen. No dependencies. The VPN client OS shall store persistent secrets and private keys when not in use in OS-provided key storage. This requirement ensures that persistent secrets (credentials, secret keys) and private keys are stored securely when not in use. If some secrets/keys are manipulated by the VPN client and others are manipulated by the OS, then both of the selections can be specified by the ST author. 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. There are no AGD EAs for this requirement. There are no test EAs for this component.

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.

Guidance
There are no AGD EAs for this requirement.

Tests
There are no test EAs for this component.

2.1.2.2 Identification and Authentication (FIA)

Components in this family describe the requirements that pertain to IP traffic and information flow through the VPN client. This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the OS PP. requires the TOE to perform X.509 certificate authentication and describes the behavior that is followed if is the status of the certificate is unknown or invalid. No specific management functions are identified. There are no auditable events foreseen. FIA_X509_EXT.1 X.509 Certificate Validation FPT_TST_EXT.1 TSF Self-Test FPT_TUD_EXT.1 Trusted Update The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec exchanges, and digital signatures for FPT_TUD_EXT.1 integrity checks for FPT_TST_EXT.1 no additional uses . When a connection to determine the validity of a certificate cannot be established, the VPN client OS shall allow the administrator to choose whether to accept the certificate in these cases accept the certificate not accept the certificate . Oftentimes a connection must be established to perform a verification of the revocation status of a certificate - either to download a CRL or to perform OCSP. The selection is used to describe the behavior in the event that such a connection cannot be established (for example, due to a network error). The behavior of the TOE in these cases is described by the second selection. If the TOE has determined the certificate is valid according to all other rules in FIA_X509_EXT.1, the behavior indicated in the second selection will determine the validity. The TOE must not accept the certificate if it fails any of the other validation rules in FIA_X509_EXT.1. If the administrator-configured option is selected by the ST Author, the ST author must also make the appropriate selection in FMT_SMF.1/VPN. The VPN client OS shall not establish an SA if a certificate or certificate path is deemed invalid. The EAs 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. 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. If the requirement indicates 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. The evaluator shall perform the following test regardless of whether the certificate validation functionality is implemented by the VPN client or by the OS: 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.

FIA_X509_EXT.3 X.509 Certificate Use and Management

The EAs 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.

Guidance
If the requirement indicates 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.

Tests
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 Path/Channels (FTP)

This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing OS functions from being performed. The VPN client OS shall use IPsec to provide a trusted communication channel between itself and a remote VPN gateway a remote VPN client a remote IPsec-capable network device that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. The VPN client OS shall permit [the TSF] to initiate communication with the trusted channel. The VPN client OS shall initiate communication via the trusted channel [for all traffic traversing that connection]. The intent of the above requirement is to demonstrate that IPsec can be used to establish remote communications in transport and/or tunnel mode. 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 reestablish 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 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. 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. The evaluator shall perform the following tests: 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. The evaluator shall ensure, for each communication channel with an IPsec peer, the channel data is not sent in plaintext. The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE. 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 EAs are associated with requirements for FCS_IPSEC_EXT.1.

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.

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.

Tests
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 EAs are associated with requirements for FCS_IPSEC_EXT.1.

2.2 Protection Profile for

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

2.2.1 Modified SFRs

2.2.1.1 Cryptographic Support (FCS)

The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECC schemes using “NIST curves” P-256, P-384, and P-521 no other curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.4, and Curve25519 schemes that meet the following: RFC 7748 No other curve , and FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.1 Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3 “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography , and RSA schemes using cryptographic key sizes of 2048-bit or greater that meet FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.3, No other key generation methods . This SFR is functionally identical to what is defined in the MDF PP except that ECC key generation with support for P-256 and P-384 has been made mandatory in support of IPsec due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Curve25519 schemes are included to satisfy FDP_DAR_EXT.2.2 in the MDF PP; these schemes are not used in support of IPsec. RSA remains present as a selection since it may be used by facets of the MDF TOE that are not specifically related to VPN client functionality. Refer to the EA for FCS_CKM.1 in the MDF PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall perform cryptographic key establishment in accordance with a specified key establishment method: Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” and Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3 RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes using Integer Factorization Cryptography,” RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2 no other key establishment schemes . This SFR differs from its definition in the MDF PP by moving elliptic curve-based key establishment schemes from selectable to mandatory (due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8). It also provides the ability to claim either NIST SP 800-56A or RFC 3526 for key establishment using finite field cryptography if DH group 14 is claimed. The use of RSA is not explicitly mandated by the VPN client but may be selected in the MDF PP, which is why it remains here. For all key establishment schemes refer to the AA for FCS_CKM.2(1) in the MDF PP. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall perform [encryption/decryption] in accordance with a specified cryptographic algorithm AES-CBC (as defined in FIPS PUB 197, NIST SP 800-38A), AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012), AES-GCM (as defined in NIST SP 800-38D), and AES Key Wrap (KW) (as defined in NIST SP 800-38F) AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F) AES-CCM (as defined in NIST SP 800-38C) AES-XTS (as defined in NIST SP 800-38E) AES-

CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013) no other modes and cryptographic key sizes 128-bit key sizes and [256-bit key sizes]. This SFR is identical to what is defined in the MDF PP except that support for GCM mode and support for 256-bit key sizes are both mandatory in order to address the requirements for FCS_IPSEC_EXT.1. Refer to the EA for FCS_COP.1(1) in the MDF PP.

FCS_CKM.1 Cryptographic Key Generation

Refer to the EA for FCS_CKM.1 in the MDF PP.

FCS_CKM.2/1 Cryptographic Key Establishment

For all key establishment schemes refer to the AA for FCS_CKM.2(1) in the MDF PP. Note that because a TOE that conforms to this PP-Module must implement IPsec, the tested protocols shall include IPsec at minimum.

FCS_COP.1/1 Cryptographic Operation

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

2.2.1.2 Identification and Authentication (FIA)

This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and TLS HTTPS DTLS no other protocols , and code signing for system software updates code signing for mobile applications code signing for integrity verification other uses no additional uses . When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall 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 . This SFR is identical to what is defined in the MDF PP except that support for IPsec is mandated. Since the original SFR did not explicitly require at least one of TLS, HTTPS, or DTLS to be selected, “no other protocols” has also been added as a selection in the event that IPsec is the only protocol for which the TOE uses X.509v3 certificates for authentication. Refer to the EA for FIA_X509_EXT.2 in the MDF PP.

FIA_X509_EXT.2 X.509 Certificate Authentication

Refer to the EA for FIA_X509_EXT.2 in the MDF PP.

2.2.1.3 Trusted Path/Channels (FTP)

This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall use 802.11-2012, 802.1X, EAP-TLS, IPsec, and TLS DTLS HTTPS no other protocols to provide a communication channel between itself and another trusted IT product 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. The TSF shall permit the TSF to initiate communication via the trusted channel. The TSF shall initiate communication via the trusted channel for wireless access point connections, administrative communication, configured enterprise connections, and OTA updates no other connections . This SFR is identical to what is defined in the Base-PP except that support for IPsec is mandated. Additionally, since the Base-PP requires ‘at least one of’ the selected protocols which previously included IPsec, ‘no other protocols’ is now available as an option in the selection. Refer to the EA for FTP_ITC_EXT.1 in the MDF PP.

FTP_ITC_EXT.1 Trusted Channel Communication

Refer to the EA for FTP_ITC_EXT.1 in the MDF PP.

2.3 Protection Profile for

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

2.3.1 Modified SFRs

2.3.1.1 Cryptographic Support (FCS)

The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. Additionally, this behavior is selection-based in the App PP but is made mandatory since it is required for VPN client functionality. The application shall invoke platform-provided functionality implement functionality to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [ECC schemes] using [“NIST curves” P-256, P-384, and P-521 no other curves] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.4], and, [FFC schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.1 [FFC schemes] using Diffie-

Hellman group 14 that meet the following: RFC 3526, Section 3, [FFC Schemes using “safe-prime” groups] that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526 RFC 7919 ; [RSA schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.3]; no other key generation methods This SFR is selection-based in the App PP depending on the selection made in FCS_CKM_EXT.1. Because key generation services (whether implemented by the TOE or invoked from the platform) are required for IPsec, this SFR is mandatory for any TOE that claims conformance to this PP-Module. This SFR is functionally identical to what is defined in the App PP except that ECC key generation has been made mandatory in support of IPsec due to the mandated support for DH groups 19, and 20 in FCS_IPSEC_EXT.1.8. RSA remains present as a selection since it may be used by parts of the TOE that are not specifically related to VPN client functionality. Refer to the EA for FCS_CKM.1(1) in the App PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements and is modified to include Diffie-Hellman Group 14 as an additional supported method for key establishment. The application shall invoke platform-provided functionality implement functionality to perform cryptographic key establishment in accordance with a specified key establishment method: [Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]; and [Finite field-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”] Key establishment scheme using Diffie-Hellman group 14] that meets the following: [RFC 3526, Section 3, [FFC Schemes using “safe-prime” groups]that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526 RFC 7919 [RSA-based key establishment schemes] that meets the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2 [RSA-based key establishment schemes] that meet the following: [NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”] No other schemes . This SFR differs from its definition in the App PP by moving elliptic curve-based key establishment schemes from selectable to mandatory (due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8). It also provides the ability to claim at least one of NIST SP 800-56A, RFC 3526, or NIST SP 800-56A rev. 3 “safe-prime” groups for key establishment using finite field cryptography. For all key establishment schemes refer to the EA for FCS_CKM.2 in the App PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; specifically, since key generation services are required in some capacity in order to support VPN functionality, the ST author loses the choice of stating that the application does not have any key generation functionality. Additionally, this behavior is selection-based in the App PP but is made mandatory since it is required for VPN client functionality. The application shall invoke platform-provided functionality for asymmetric key generation implement asymmetric key generation . This selection differs from its definition in the App PP by removing the selection for “generate no asymmetric cryptographic keys” for this PP-Module because a VPN Client TOE will either perform its own key generation or interface with the underlying platform to provide this service, either of which causes FCS_CKM.1(1) to be claimed. This SFR is evaluated in conjunction with FCS_CKM.1(1) in the App PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode, AES-GCM (as defined in NIST SP 800-38D) mode, ; and AES-XTS (as defined in NIST SP 800-38E) mode no other modes and cryptographic key sizes [128-bit, 256-bit]. This SFR is selection-based in the Base-PP and remains selection-based here because this PP-Module allows for the possibility that the TSF relies on platform-provided cryptographic algorithm services for its own implementation of IPsec. However, if the TSF does claim this SFR to support IPsec, the ST author must select at minimum both AES-CBC and AES-GCM with both 128-bit and 256-bit key sizes for consistency with the relevant IPsec claims (FCS_IPSEC_EXT.1.4 requires both 128-bit and 256-bit AES-GCM and FCS_IPSEC_EXT.1.6 requires both 128-bit and 256-bit AES-CBC). If the TSF implements AES cryptography in support of both credential encryption (per FCS_STO_EXT.1) and IPsec, the evaluator shall examine the TSS to ensure that it clearly identifies the modes and key sizes that are supported for each usage of AES. There are no operational guidance EAs beyond what is required by the EA for FCS_COP.1(1) in the App PP. There are no test EAs beyond what is required by the EA for FCS_COP.1(1) in the App PP.

FCS_CKM.1/1 Cryptographic Asymmetric Key Generation

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

FCS_CKM.2 Cryptographic Key Establishment

For all key establishment schemes refer to the EA for FCS_CKM.2 in the App PP.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

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

FCS_COP.1/1 Cryptographic Operation

TSS
If the TSF implements AES cryptography in support of both credential encryption (per FCS_STO_EXT.1) and IPsec, the evaluator shall examine the TSS to ensure that it clearly identifies the modes and key sizes that are

supported for each usage of AES.
Guidance
There are no operational guidance EAs beyond what is required by the EA for FCS_COP.1(1) in the App PP.
Tests
There are no test EAs beyond what is required by the EA for FCS_COP.1(1) in the App PP.

2.3.1.2 Identification and Authentication (FIA)

This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [no other protocols]. When the application cannot establish a connection to determine the validity of a certificate, the TSF shall allow the administrator to choose whether to accept the certificate in these cases accept the certificate not accept the certificate . This SFR is identical to what is defined in the App PP except that mandatory support for IPsec is added. Additionally, because this SFR is selection-based in the App PP but is mandatory for VPN client usage, the ‘no other protocols’ selection item has been added since it is expected that IPsec is the TOE’s only use of certificates. Refer to the EA for FIA_X509_EXT.2 in the App PP.

FIA_X509_EXT.2 X.509 Certificate Authentication

Refer to the EA for FIA_X509_EXT.2 in the App PP.

2.3.1.3 Trusted Path/Channels (FTP)

This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The application shall [not encrypt any [sensitive data]] between itself and another trusted IT product. The VPN client itself is the application, and does not maintain any sensitive data of its own. Therefore, there is no need to protect (through FTP_DIT_EXT.1.1) VPN-client-specific data. For IPsec, refer to the EA for FCS_IPSEC_EXT.1 in section 2.5.1.1 below.

FTP_DIT_EXT.1 Protection of Data in Transit

For IPsec, refer to the EA for FCS_IPSEC_EXT.1 in section 2.5.1.1 below.

2.3.2 Additional SFRs

2.3.2.1 Cryptographic Support (FCS)

This PP-Module adds a requirement for key storage, which is new functionality when compared to the Base-PP but does not interfere with its existing security functions. requires the TSF to securely store key data when not in use. No specific management functions are identified. There are no auditable events foreseen. No dependencies The TOE TOE platform shall store persistent secrets and private keys when not in use in platform-provided key storage. This requirement ensures that persistent secrets and private keys are stored securely when not in use. This differs from FCS_STO_EXT.1 in the Base-PP, which only applies to secure storage of administrative credentials. If some secrets/keys are manipulated by the TOE and others are manipulated by the platform, then both of the selections can be specified by the ST author. 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. There are no AGD EAs for this requirement. There are no test EAs for this requirement. This PP-Module adds a requirement for key destruction, which is new functionality when compared to the Base-PP but does not interfere with its existing security functions. requires the TSF to destroy key data when no longer required. No specific management functions are identified. There are no auditable events foreseen. No dependencies The TOE TOE platform shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required. 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. In practice, the TOE will not implement all of the functionality associated with the requirement, since if it performs zeroization at all it will be by invoking platform interfaces to perform the storage location clear/overwrite function. The ST author should select "TOE" when, for at least one of the keys needed to meet the requirements of this PP, the TOE manipulates (reads, writes) the data identified in the requirement and thus needs to ensure that those data are cleared. In these cases, 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. In the likely event that some of the data are manipulated by the TOE and other data are manipulated entirely by the platform, the ST author must select both options. 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 EAs 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"). There are no AGD EAs for this requirement. For each key clearing situation described in the TSS, the evaluator shall repeat the following test. 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: Load the instrumented TOE build in a debugger. Record the value of the key in the TOE subject to clearing. Cause the TOE to perform a normal cryptographic processing with the key from #1. Cause the TOE to clear the key. Cause the TOE to stop the execution but not exit. Cause the TOE to dump the entire memory footprint of the TOE into a binary file. 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.

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.

Guidance
There are no AGD EAs for this requirement.

Tests
There are no test EAs 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 EAs 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").

Guidance
There are no AGD EAs for this requirement.

Tests
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 Protection Profile for Mobile Device Management

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

2.4.1 Modified SFRs

2.4.1.1 Cryptographic Support (FCS)

The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall invoke platform-provided functionality implement functionality to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECC schemes using “NIST curves” P-256, P-384, and P-521 no other curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS),” Appendix B.4, and RSA schemes using cryptographic key sizes of 2048-bit or greater that meet FIPS PUB 186-4, "Digital Signature Standard (DSS),” Appendix B.3, FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PU 186-4, “Digital Signature Standards (DSS),” Appendix B.4, FFC schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “ Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” and RFC 3526 RFC 7919 , FFC schemes using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3, No other key generation schemes . This SFR is modified from its definition in the MDM PP by mandating the key generation algorithms that are required by this PP-Module in support of IPsec due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Other selections may be chosen by the ST author as needed for parts of the TOE that are not specifically related to VPN client functionality Refer to the EA for FCS_CKM.1 in the MDM PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall invoke platform-provided functionality implement functionality to perform cryptographic key establishment in accordance with a specified key establishment method: Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” and RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” FFC schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,"' and RFC 3526 RFC 7919 Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3 No other schemes . This SFR is modified from its definition in the MDM PP by mandating the key establishment algorithms that are required by this PP-Module in support of

IPsec due to the mandated support for DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Other selections may be chosen by the ST author as needed for parts of the TOE that are not specifically related to VPN client functionality. Refer to the EA for FCS_CKM.2 in the MDM PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The TSF shall invoke platform-provided functionality implement functionality perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in FIPS PUB 197, NIST SP 800-38A), AES-GCM (as defined in NIST SP 800-38D), and AES Key Wrap (KW) (as defined in NIST SP 800-38F) AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F) AES-CCM (as defined in NIST SP 800-38C) no other modes and cryptographic key sizes [128-bit, 256-bit]. This SFR is modified from its definition in the Base-PP by mandating support for both 128-bit and 256-bit implementations of AES-CBC (which this PP-Module requires for the use of IKE and allows for the use of ESP) and AES-GCM (which this PP-Module requires for the use of ESP and allows for the use of IKE). Other AES modes may be selected by the ST author as needed to address functions not required by this PPModule. Refer to the EA for FCS_COP.1(1) in the MDM PP.

FCS_CKM.1 Cryptographic Key Generation

Refer to the EA for FCS_CKM.1 in the MDM PP.

FCS_CKM.2 Cryptographic Key Establishment

Refer to the EA for FCS_CKM.2 in the MDM PP.

FCS_COP.1/1 Cryptographic Operation

Refer to the EA for FCS_COP.1(1) in the MDM PP.

2.4.1.2 Identification and Authentication (FIA)

This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. The TSF shall Invoke platform-provided functionality to use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec HTTPS TLS DTLS SSH no protocols and code signing for system software updates code signing for integrity verification policy signing other uses no additional uses use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec as specified in the PP-Module for VPN client and HTTPS in accordance with FCS_HTTPS_EXT.1 TLS as defined in the Package for Transport Layer Security DTLS as defined in the Package for Transport Layer Security SSH as defined in the Extended Package for Secure Shell no other protocols , and code signing for system software updates code signing for integrity verification policy signing other uses no additional uses . The PP-Module requires the TOE to implement its own X.509 authentication mechanism in support of IPsec communications. Other selections may be chosen by the ST author as needed for parts of the TOE that are not specifically related to VPN client functionality. The TSF may also rely on a platform-provided mechanism for uses of X.509 that do not relate to the establishment of trusted communications, as specified in the original SFR. FIA_X509_EXT.2.2 has not been included here as the PPModule does not modify this element. Refer to the EA for FIA_X509_EXT.2 in the MDM PP.

FIA_X509_EXT.2 X.509 Certificate Authentication

Refer to the EA for FIA_X509_EXT.2 in the MDM PP.

2.4.1.3 Trusted Path/Channels (FTP)

When the MDM TOE claims this PP-Module, at least one of its interfaces will implement IPsec communications. However, this PP-Module does not specify that any one particular interface must be implemented using IPsec. If the TOE is distributed and uses IPsec to secure communications between its distributed components, FPT_ITT.1(1) is refined as below. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall [implement functionality using [IPsec as defined in the PP-Module for VPN Client]]. This SFR is selection-based in the Base-PP depending on the selections made in the Base-PP requirement FTP_ITC_EXT.1. This is not changed by the PP-Module. This SFR is modified from its definition in the Base-PP by mandating that the TSF implement IPsec communications and by prohibiting the TOE from relying on platform-provided functionality to implement this. Refer to the EA for FPT_ITT.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function. When the MDM TOE claims this PP-Module, at least one of its interfaces will implement IPsec communications. However, this PP-Module does not specify that any one particular interface must be implemented using IPsec. If the TOE uses IPsec to secure communications between itself and external trusted IT entities, FTP_ITC.1(1) is refined as below. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall implement functionality using IPsec as defined in the PP-Module for VPN Client, and SSH as defined in the Extended Package for Secure Shell mutually authenticated TLS as defined in the Package for Transport Layer Security mutually authenticated DTLS as defined in the Package for Transport Layer Security HTTPS in accordance with FCS_HTTPS_EXT.1 no other protocols and invoke platform-provided functionality to use SSH mutually authenticated TLS mutually authenticated DTLS HTTPS not invoke any platform-provided functionality to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, authentication server other capabilities that is logically distinct from other communication channels and provides assured identification of its end points and protection of channel data from modification and

disclosure. The TSF shall implement functionality and invoke platform-provided functionality not invoke platform-provided functionality to permit the MDM Server or other authorized IT entities to initiate communication via the trusted channel. The TSF shall implement functionality and invoke platform-provided functionality not invoke platform-provided functionality to initiate communication via via the trusted channel for list of services for which the TSF is able to initiate communications. This SFR is refined from its definition in the Base-PP by mandating that the “implement functionality” selection be chosen at minimum for IPsec and by prohibiting the TOE from relying on platform-provided IPsec functionality. Since the TOE may support multiple trusted channel interfaces, the ST author is given the option to select other protocols (SSH, TLS, DTLS, HTTPS) either as being implemented by the TSF or invoked from the platform. Refer to the EA for FTP_ITC.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function. When the MDM TOE claims this PP-Module, at least one of its interfaces will implement IPsec communications. However, this PP-Module does not specify that any one particular interface must be implemented using IPsec. If the TOE uses IPsec to secure communications between itself and trusted remote administrators, FPT_TRP.1(1) is refined as below. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall implement functionality using IPsec as defined in the PP-Module for VPN Client, and TLS as defined in the Package for Transport Layer Security HTTPS in accordance with FCS_HTTPS_EXT.1 SSH as defined in the Extended Package for Secure Shell no other protocols and invoke platform-provided functionality to use TLS HTTPS SSH not invoke any platform-provided functionality to provide a trusted communication channel between itself as a server peer and remote administrators that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from [modification, disclosure]. The TSF shall implement functionality and invoke platform-provided functionality not invoke platform-provided functionality to permit remote administrators to initiate communication via the trusted channel. The TSF shall implement functionality and invoke platform-provided functionality not invoke platform-provided functionality to require the use of the trusted path for [all remote administration actions]. This SFR is refined from its definition in the Base-PP by mandating that the “implement functionality” selection be chosen at minimum for IPsec and by prohibiting the TOE from relying on platform-provided IPsec functionality. Since the TOE may support multiple remote administrative interfaces, the ST author is given the option to select other protocols (SSH, TLS, HTTPS) either as being implemented by the TSF or invoked from the platform. Refer to the EA for FTP_TRP.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function.

FTP_ITT.1/1 Basic Internal TSF Data Transfer Protection

Refer to the EA for FPT_ITT.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function.

FTP_ITC.1/1 Inter-TSF Trusted Channel (Authorized IT Entities)

Refer to the EA for FTP_ITC.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function.

FTP_TRP.1/1 Trusted Path (for Remote Administration)

Refer to the EA for FTP_TRP.1(1) in the MDM PP. Note that the PP-Module does not require any separate testing for this if IPsec is not used to implement this function.

2.5 TOE SFR Evaluation Activities

2.5.1 Cryptographic Support (FCS)

FCS_CKM.1/1 VPN Cryptographic Key Generation (IKE)

TSS
The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.
Guidance
There are no AGD EAs for this requirement.
Tests
If this functionality is implemented by the TSF, refer to the following EAs, depending on the TOE’s claimed Base-PP:

- GPOS PP: FCS_CKM.1
- MDF PP: FCS_CKM.1
- App PP: FCS_CKM.1(1)
- MDM PP: FCS_CKM.1

FCS_IPSEC_EXT.1 IPsec

EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.9. EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11. EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.
TSS

In addition to the TSS EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the TOE boundary includes a general-purpose operating system or mobile device, the evaluator shall examine the TSS to ensure that it describes whether the VPN client capability is architecturally integrated with the platform itself or whether it is a separate executable that is bundled with the platform.

Guidance
In addition to the Operational Guidance EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the configuration of the IPsec behavior is from an environmental source, most notably a VPN gateway (e.g through receipt of required connection parameters from a VPN gateway), the evaluator shall ensure that the operational guidance contains any appropriate information for ensuring that this configuration can be properly applied.

Note in this case that the implementation of the IPsec protocol must be enforced entirely within the TOE boundary; i.e. it is not permissible for a software application TOE to be a graphical front-end for IPsec functionality implemented totally or in part by the underlying OS platform. The behavior referenced here is for the possibility that the configuration of the IPsec connection is initiated from outside the TOE, which is permissible so long as the TSF is solely responsible for enforcing the configured behavior. However, it is allowable for the TSF to rely on low-level platform-provided networking functions to implement the SPD from the client (e.g., enforcement of packet routing decisions).

Tests
As a prerequisite for performing the Test EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall do the following:

The evaluator shall minimally create a test environment equivalent to the test environment illustrated below. It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluator shall provide justification for any differences in the test environment.

Note that the evaluator shall perform all tests using the VPN client and a representative sample of platforms listed in the ST (for TOEs that claim to support multiple platforms).

FCS_IPSEC_EXT.1.1

FCS_IPSEC_EXT.1.2

FCS_IPSEC_EXT.1.3

FCS_IPSEC_EXT.1.4

FCS_IPSEC_EXT.1.5

FCS_IPSEC_EXT.1.6

FCS_IPSEC_EXT.1.7

FCS_IPSEC_EXT.1.8

FCS_IPSEC_EXT.1.9

FCS_IPSEC_EXT.1.10

FCS_IPSEC_EXT.1.11

FCS_IPSEC_EXT.1.12

FCS_IPSEC_EXT.1.13

FCS_IPSEC_EXT.1.14

2.5.2 User Data Protection (FDP)

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.

Guidance

There are no AGD EAs for this requirement.

Tests

There are no test EAs for this requirement.

2.5.3 Security Management (FMT)

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.

Guidance

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

Tests

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.

2.5.4 Protection of the TSF (FPT)

FPT_TST_EXT.1/VPN 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 startup; 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 the VPN Client 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.

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.

Tests

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.

2.6 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.7 Evaluation Activities for Selection-Based SFRs

2.7.1 Identification and Authentication (FIA)

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 preshared 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 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.

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.

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.

Tests
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.

2.8 Evaluation Activities for Objective SFRs

2.8.1 Security Audit (FAU)

FAU_GEN.1/VPN 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.

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 VPN Client PP-Module is described and that the description of the fields contains the information required in FAU_GEN.1.2/VPN, and the additional information specified in the Auditable Events table of the VPN Client PP-PP-Module.

In particular, the evaluator shall ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In the Auditable Events table of the VPN Client 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 the VPN Client PP-Module. The TOE may contain functionality that is not evaluated in the context of the VPN Client 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 VPN Client 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.

For each required auditable event, the evaluator shall examine the operational guidance to determine that it is clear to the reader where each event is generated (e.g. the TSF may generate its own audit logs in one location while the platform-provided auditable events are generated elsewhere).

Tests

The evaluator shall test the TOE’s ability to correctly generate audit records by having the TOE generate audit records in accordance with the EAs associated with the functional requirements in the VPN Client PP-Module. Additionally, the evaluator shall test that each administrative action applicable in the context of the VPN Client 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.

FAU_SEL.1/VPN Selective Audit

TSS

There are no TSS EAs for this SFR.

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.

Tests

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.

2.8.2 User Data Protection (FDP)

FDP_IFC_EXT.1 Subset 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 is 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).

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.

Tests
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.

3 Evaluation Activities for SARs

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

4 Required Supplementary Information

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

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[OS PP]	Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 2019
[MD PP]	Protection Profile for Mobile Device Fundamentals, Version 3.1, June 2017
[MDM PP]	Protection Profile for Mobile Device Management (This needs to be updated) , Version 3.1, June 2017
[App PP]	Protection Profile for Application Software, Version 1.3, March 2019