Supporting Document
Mandatory Technical Document

PP-Module for VPN Clients
Version: 2.4
2022-03-31
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
2.4	2022-03-31	Incorporation of TC feedback
2.3	2021-08-10	Support for MDF, Bluetooth updates
2.2	2021-01-05	Update release
2.1	2019-11-14	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of VPN Client products.

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

Table of Contents

against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 Diffie-Hellman (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]. This SFR is functionally identical to what is defined in the GPOS PP except that elliptic curve cryptography (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 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D and IEEE 802.11ac-2013) No other modes and cryptographic key sizes 128-bit 256-bit . This SFR is defined in the GPOS PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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. 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 GPOS 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 or 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, it is not written unencrypted to persistent memory, and that the item is stored by the OS. There are no guidance EAs for this requirement. There are no test EAs for this component. 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 GPOS PP. requires the TOE to perform X.509 certificate authentication and describes the behavior that is followed if 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 certificate revocation list (CRL) or to use the online certificate status protocol (OCSP) to check revocation status. 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 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. 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 mode, tunnel mode, or both. 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, VPN client, 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, VPN client, 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 evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, 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 evaluator 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. If this PP-Module is used to extend the GPOS PP, the TOE type for the overall TOE is still a general-purpose OS. The TOE boundary is simply extended to include VPN client functionality that is built into the OS so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the GPOS PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the GPOS PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the GPOS PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats on the GPOS PP because misconfiguration could allow VPN traffic to be subjected unexpectedly to unauthorized modification or disclosure.. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the GPOS PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the GPOS PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the GPOS PP because the GPOS PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the GPOS PP but is consistent with the A.PLATFORM assumption defined in the GPOS PP, which expects the computing platform to be trusted. The

assumption that personnel responsible for the TOE's configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the GPOS PP. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the GPOS PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the GPOS PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the GPOS PP and does not define an environment that a GPOS TOE is incapable of existing in. This is part of satisfying OE.PLATFORM as defined in the GPOS PP because physical security is required for hardware to be considered 'trusted' The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the GPOS PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified 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 GPOS to satisfy any of its other security requirements. Storage of key data related to VPN functionality can be accomplished using the same mechanism defined by FCS_STO_EXT.1 in the GPOS PP. This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the GPOS PP. This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing GPOS functions from being performed. Generation of IKE peer authentication keys is added functionality that does not prevent the existing GPOS functions from being performed. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the GPOS functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the GPOS functionality. The ability to configure the VPN client behavior does not affect whether the GPOS as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the GPOS to perform its security functions. Audit records generated by the VPN client do not interfere with GPOS functionality. The possibility of the underlying OS platform generating audit records is consistent with the GPOS PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain audit records related to VPN activity does not interfere with the ability of the GPOS to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the GPOS PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the GPOS PP because it may be a function offered by the part of the TOE described by the GPOS PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the GPOS PP but does not prevent any GPOS PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

2.2 https://github.com/commoncriteria/mobile-device v3.2 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417 In a PP-Configuration that includes the MDF PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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; 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 "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 ECC schemes using Curve25519 schemes that meet the following: RFC 7748 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 at least one of P-256 and P-384 has been made mandatory in support of IPsec due to the mandated support for at least one of DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Support for "safe-prime" groups has also been added as a selectable option for DH groups that use finite field algorithms. Curve25519 schemes remain selectable for their potential use in satisfying FDP_DAR_EXT.2.2 in the MDF PP; these schemes are not used in support of IPsec. RSA and ECC support for P-521 remain present as selections since they may be used by parts of the TOE that are not specifically related to VPN client functionality. Refer to the EAs for FCS_CKM.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the

corresponding testing is mandatory. The actual testing for those selections is not changed. 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,” 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). Finite field and Group 14 selections remain present if groups 14, 15, or 24 are selected in FCS_IPSEC_EXT.1.8. This PP-Module does not require the use of RSA for any function but it is present in the selection in case other MDF PP functions require its use. Refer to the EAs for FCS_CKM.2/UNLOCKED in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D 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 EAs for FCS_COP.1/ENCRYPT in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 [provide a VPN client which can protect all IP traffic using IPsec as defined in the PP-Module for VPN Client] with the exception of IP traffic needed to manage the VPN connection, and traffic needed for correct functioning of the TOE no other traffic when the VPN is enabled. This SFR is identical to its definition in the Base-PP except that the selection item that requires the TOE to implement its own VPN client is always selected when the TOE’s conformance claim includes this PP-Module Refer to the EAs for FDP_IFC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 mutually authenticated TLS as defined in the Package for Transport Layer Security, HTTPS, IPsec in accordance with the PP-Module for VPN Client, mutually authenticated DTLS as defined in the Package for Transport Layer Security 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. The selection of “no other protocols” is added to address the case where the TOE only claims support for the protocols that are mandated by the SFR. Refer to the EAs for FIA_X509_EXT.2 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. This PP-Module modifies management function 45 regarding Always-on VPN protection. This SFR is not reproduced in its entirety for size purposes. The only change to this SFR is the following change to management function 45: 45. enable/disable the Always On VPN protection: - a. across device - [d. no other method] M O O O Refer to the EAs for FMT_SMF_EXT.1 in the MDF PP. The only change to this SFR is the change to management function 45. Testing of all other functions is not affected. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall use 802.11-2012 in accordance with the Extended Package for WLAN Clients 802.1X in accordance with the Extended Package for WLAN Clients EAP-TLS in accordance with the Extended Package for WLAN Clients mutually authenticated TLS as defined in the Package for Transport Layer Security IPsec in accordance with the PP-Module for VPN Client and mutually authenticated DTLS as defined in the Package for Transport Layer Security 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 EAs for FTP_ITC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. If this PP-Module is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. The TOE boundary is simply extended to include VPN client functionality that is built in to the device’s software so that additional security functionality is claimed within the scope of the TOE. The

threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDF PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDF PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.EAVESDROP threat in the MDF PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.FLAWAPP threat in the MDF PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDF PP because the MDF PP makes no assumptions about the network architecture in which the TOE is deployed. The MDF PP includes the A.NOTIFY and A.PRECAUTION assumptions to mitigate the risk of physical theft of the TOE. This is consistent with the A.PHYSICAL assumption in this PP-Module because the MDF PP includes reasonable assumptions about the physical security of the TOE. This assumption is consistent with the MDF PP because the MDF PP includes the A.CONFIG assumption which assumes that all security functions are appropriately configured. This objective is consistent with the O.AUTH objective of the MDF PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.COMMS objective of the MDF PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDF PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.STORAGE objective of the MDF PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the MDF PP and does not define an environment that an MDF TOE is incapable of existing in. The operational environment of a mobile device cannot guarantee physical security, but the OE.PRECAUTION objective in the MDF PP ensures that an appropriate level of physical security is provided. The expectation of trusted configuration is consistent with OE.CONFIG 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the MDF PP. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the MDF functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the MDF functionality. The ability to configure the VPN client behavior does not affect whether the MDF as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the MDF to perform its security functions Audit records generated by the VPN client do not interfere with MDF functionality. The possibility of the underlying MDF platform generating audit records is consistent with the MDF PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain VPN client audit records does not interfere with MDM functionality. The MDF PP already contains FAU_SEL.1 as an objective SFR which means that this functionality does not conflict with the expected behavior of a mobile device. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level mobile device behavior, but there are no requirements in the MDF PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the MDF PP because it may be a function offered by the part of the TOE described by the MDF PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the MDF PP but does not prevent any MDF PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

2.2.1 Modified SFRs

2.2.1.1 Cryptographic Support (FCS)

2.2.1.2 User Data Protection (FDP)

2.2.1.3 Identification and Authentication (FIA)

2.2.1.4 Security Management (FMT)

2.2.1.5 Trusted Path/Channels (FTP)

2.3 https://github.com/commoncriteria/application release-1.4 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429

In a PP-Configuration that includes the App PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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/AK 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 DH 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 2.1 [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/AK to be claimed. This SFR is evaluated in conjunction with FCS_CKM.1/AK 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 AES-CCM (as defined in NIST SP 800-38C) mode AES-CTR (as defined in NIST SP 800-38A) 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 beyond what is required by the EA for FCS_COP.1/SKC in the App PP. There are no test EAs beyond what is required by the EA for FCS_COP.1/SKC in the App PP. 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. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The application shall encrypt all transmitted [sensitive data] using IPsec as specified in FCS_IPSEC_EXT.1 and HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server HTTPS as a server with mutual authentication in accordance with FCS_HTTPS_EXT.2 TLS as defined in the Functional Package for TLS DTLS as defined in the Functional Package for TLS SSH as defined in the Functional Package for Secure Shell no other protocols between itself and another trusted IT product. This SFR is identical to what is defined in the App PP except that mandatory support for IPsec is added, the ST author is forced to select the ‘encrypt all transmitted sensitive data’ option, and the options for invoking platform-provided functionality have been removed. Since it is possible that a conformant TOE may not use any encryption protocols other than IPsec, “no other protocols” is provided as a selectable option in the list of

supported protocols. For IPsec, refer to the EA for FCS_IPSEC_EXT.1. If other protocols are selected for FTP_DIT_EXT.1, refer to the EA for FTP_DIT_EXT.1 in the App PP. 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 or 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 guidance 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 or CSP data (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key or 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 or 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 guidance EAs for this requirement. For each key clearing situation described in the TSS, the evaluator shall repeat the following test. The evaluator shall use appropriate combinations of specialized OE 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. If this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is made more specific by defining the TOE as a specific type of application. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the App PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the App PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the App PP. The threat of a misconfigured VPN client is consistent with the T.LOCAL_ATTACK threat in the App PP. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the App PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat

in the App PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the App PP because the App PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the App PP but is consistent with the A.PLATFORM assumption defined in the App PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE's configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the App PP. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the App PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the App PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the App PP and does not define an environment that is globally applicable to all software applications. This is part of satisfying OE.PLATFORM as defined in the App PP because physical security is required for the underlying platform to be considered 'trustworthy'. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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. Additionally, this behavior is selection-based in the App PP but is made mandatory since it is required for VPN client functionality. 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 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 ST author is given guidance to make specific selections if this selection-based SFR is claimed in support of IPsec functionality. The SFR behavior itself is unmodified. This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. This PP-Module is for the VPN Client 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. This PP-Module adds a requirement for key storage, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This PP-Module adds a requirement for key destruction, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the App PP. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the application functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the general application functionality. The ability to configure the VPN client behavior does not affect whether the application as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the application to perform its security functions Audit records generated by the VPN client do not interfere with application functionality. For cases where auditing is performed by the TOE platform, a software application is installed on a general-purpose OS or mobile device, both of which can reasonably be expected to provide audit functionality. The ability to suppress the generation of certain audit records related to VPN activity does not interfere with the ability of the application to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the App PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the App PP because it may be a function offered by the OE in which a TOE defined by the App PP is deployed. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the App PP but does not prevent any App PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

2.3.1 Modified SFRs

2.3.1.1 Cryptographic Support (FCS)

2.3.1.2 Identification and Authentication (FIA)

2.3.1.3 Trusted Path/Channels (FTP)

2.3.2 Additional SFRs

2.3.2.1 Cryptographic Support (FCS)

2.4 https://github.com/commoncriteria/mdm v4.0 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=428&id=428

In a PP-Configuration that includes the MDM PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 meets 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 meets the following: FIPS PUB 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 defined in the MDM PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 PP-Module. Refer to the EA for FCS_COP.1(1) in the MDM PP. 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 PP-Module does not modify this element. Refer to the EA for FIA_X509_EXT.2 in the MDM PP. 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 defined in the MDM PP as FPT_ITT.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 above. 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. 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 the trusted channel for list of services for which the TSF is able to initiate communications. This SFR is defined in the MDM PP as FTP_ITC.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 noted by the refinements above. 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. 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 defined in the MDM PP as FTP_TRP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 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. If this PP-Module is used to extend the MDM PP, the TOE type for the overall TOE is still a mobile device management solution. The TOE boundary is simply extended to include VPN client functionality that is included with the MDM software so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDM PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDM PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the MDM PP A failure of TSF functionality could compromise the implementation of the IPsec channel, which would lead to an exploitation of the T.NETWORK_ATTACK threat. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDM PP because the MDM PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the MDM PP but is consistent with the A.MDM_SERVER_PLATFORM assumption defined in the MDM PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE’s configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the MDM PP. This objective is consistent with the O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDM PP, which expects a conformant TOE to implement measures to maintain its own integrity. There are no objectives in the MDM PP that directly relate to this objective, but it could be considered to support both the O.ACCOUNTABILITY and O.MANAGEMENT objectives in the MDM PP by ensuring that stored data cannot be modified through unauthorized mechanisms that may allow for access control and logging functions to be bypassed. This objective addresses behavior that is out of scope of the MDM PP and does not define an environment that an MDM TOE is incapable of existing in. This is part of satisfying OE.IT_ENTERPRISE as defined in the MDM PP because provisioning of physical security is a reasonable expectation for an IT enterprise. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. When this SFR relates to the PP-Module’s functionality, the ST author is instructed to make specific selections to

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for VPN Clients is to describe the security functionality of 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:

-
-
-
-

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

- VPN Clients, Version 2.4

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

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

1.2 Structure of the Document

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

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

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

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

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.

(OE)	
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Technical Terms

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.
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, 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 workunits that are performed in Section 3 Evaluation Activities for SARs.

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

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

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 https://github.com/commoncriteria/operatingsystem /release-4.2.1 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=442&id=442 In a PP-Configuration that includes the GPOS PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 Diffie-Hellman (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]. This SFR is functionally identical to what is defined in the GPOS PP except that elliptic curve cryptography (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 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D and IEEE 802.11ac-2013) No other modes and cryptographic key sizes 128-bit 256-bit . This SFR is defined in the GPOS PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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. 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 GPOS 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 or 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, it is not written unencrypted to persistent memory, and that the item is stored by the OS. There are no guidance EAs for this requirement. There are no test EAs for this component. 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 GPOS PP. requires the

TOE to perform X.509 certificate authentication and describes the behavior that is followed if 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 certificate revocation list (CRL) or to use the online certificate status protocol (OCSP) to check revocation status. 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 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. 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 mode, tunnel mode, or both. 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, VPN client, 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, VPN client, 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 evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, 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 evaluator 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. If this PP-Module is used to extend the GPOS PP, the TOE type for the overall TOE is still a general-purpose OS. The TOE boundary is simply extended to include VPN client functionality that is built into the OS so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the GPOS PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the GPOS PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the GPOS PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats on the GPOS PP because misconfiguration could allow VPN traffic to be subjected unexpectedly to unauthorized modification or disclosure.. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the GPOS PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the GPOS PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the GPOS PP because the GPOS PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the GPOS PP but is consistent with the A.PLATFORM assumption defined in the GPOS PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE’s configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the GPOS PP. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the GPOS PP, which expects a conformant TOE to implement measures to maintain its own

integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the GPOS PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the GPOS PP and does not define an environment that a GPOS TOE is incapable of existing in. This is part of satisfying OE.PLATFORM as defined in the GPOS PP because physical security is required for hardware to be considered 'trusted' The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the GPOS PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified 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 GPOS to satisfy any of its other security requirements. Storage of key data related to VPN functionality can be accomplished using the same mechanism defined by FCS_STO_EXT.1 in the GPOS PP. This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the GPOS PP. This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing GPOS functions from being performed. Generation of IKE peer authentication keys is added functionality that does not prevent the existing GPOS functions from being performed. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the GPOS functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the GPOS functionality. The ability to configure the VPN client behavior does not affect whether the GPOS as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the GPOS to perform its security functions. Audit records generated by the VPN client do not interfere with GPOS functionality. The possibility of the underlying OS platform generating audit records is consistent with the GPOS PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain audit records related to VPN activity does not interfere with the ability of the GPOS to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the GPOS PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the GPOS PP because it may be a function offered by the part of the TOE described by the GPOS PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections.

This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the GPOS PP but does not prevent any GPOS PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the https://github.com/commoncriteria/operatingsystem /release-4.2.1 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=442&id=442 In a PP-Configuration that includes the GPOS PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 Diffie-Hellman (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]. This SFR is functionally identical to what is defined in the GPOS PP except that elliptic curve cryptography (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 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D and IEEE 802.11ac-2013) No other modes and cryptographic key sizes 128-bit 256-bit . This SFR is defined in the GPOS PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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. 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 GPOS 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 or 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, it is not written unencrypted to persistent memory, and that the item is stored by the OS. There are no guidance EAs for this requirement. There are no test EAs for this component. 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 GPOS PP. requires the TOE to perform X.509 certificate authentication and describes the behavior that is followed if 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 certificate revocation list (CRL) or to use the online certificate status protocol (OCSP) to check revocation status. 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 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. 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 mode, tunnel mode, or both. 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, VPN client, 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, VPN client, 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 evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, 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 evaluator 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. If this PP-Module is used to extend the GPOS PP, the TOE type for the overall TOE is still a general-purpose OS. The TOE boundary is simply extended to include VPN client functionality that is built into the OS so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the GPOS PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the GPOS PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the GPOS PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats on the GPOS PP because misconfiguration could allow VPN traffic to be subjected unexpectedly to unauthorized modification or disclosure.. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the GPOS PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the GPOS PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the GPOS PP because the GPOS PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the GPOS PP but is consistent with the A.PLATFORM assumption defined in the GPOS PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE’s configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the GPOS PP. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the GPOS PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the GPOS PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the GPOS PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the GPOS PP and does not define an environment that a GPOS TOE is incapable of existing in. This is part of satisfying OE.PLATFORM as defined in the GPOS PP because physical security is required for hardware to be considered ‘trusted’ The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the GPOS PP. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified 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 GPOS to satisfy any of its other security requirements. Storage of key data related to VPN functionality can be accomplished using the same mechanism defined by FCS_STO_EXT.1 in the GPOS PP. This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the GPOS PP. This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing GPOS functions from being performed. Generation of IKE peer authentication keys is added functionality that does not prevent the existing GPOS functions from being performed. This SFR defines the VPN client’s IPsec implementation, which is added functionality that does not interfere with the GPOS functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the GPOS functionality. The ability to configure the VPN client behavior does not affect whether the GPOS as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the GPOS to perform its security functions. Audit records generated by the VPN client do not interfere with GPOS functionality. The possibility of the underlying OS platform generating audit records is consistent with the GPOS PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain audit records related to VPN activity does not interfere with the ability of the GPOS to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the GPOS PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the GPOS PP because it may be a function offered by the part of the TOE described by the GPOS PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the GPOS PP but does not prevent any GPOS PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only

applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. .

2.1.1 Modified SFRs

2.1.1.1 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

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

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2
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)

FCS_COP.1/1
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)

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2
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, it is not written unencrypted to persistent memory, and that the item is stored by the OS.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this component.

2.1.2.2 Identification and Authentication (FIA)

FIA_X509_EXT.3 X.509 Certificate Use and Management

FIA_X509_EXT.3
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 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 1.1:** 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)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1
TSS
The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN gateway, VPN client, 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, VPN client, 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 2.1:** The evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, 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 2.2:** The evaluator shall ensure, for each communication channel with an IPsec peer, the channel data is not sent in plaintext.
- **Test 2.3:** The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE.
- **Test 2.4:** The evaluator 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 https://github.com/commoncriteria/mobile-device v3.2 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=417&id=417 In a PP-Configuration that includes the MDF PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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; 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 “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 ECC schemes using Curve25519 schemes that meet the following: RFC 7748 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 at least one of P-256 and P-384 has been made mandatory in support of IPsec due to the mandated support for at least one of DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Support for “safe-prime” groups has also been added as a selectable option for DH groups that use finite field algorithms. Curve25519 schemes remain selectable for their potential use in satisfying FDP_DAR_EXT.2.2 in the MDF PP; these schemes are not used in support of IPsec. RSA and ECC support for P-521 remain present as selections since they may be used by parts of the TOE that are not specifically related to VPN client functionality. Refer to the EAs for FCS_CKM.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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,” 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). Finite field and Group 14 selections remain present if groups 14, 15, or 24 are selected in FCS_IPSEC_EXT.1.8. This PP-Module does not require the use of RSA for any function but it is present in the selection in case other MDF PP functions require its use. Refer to the EAs for FCS_CKM.2/UNLOCKED in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory.

The actual testing for those selections is not changed. 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D 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 EAs for FCS_COP.1/ENCRYPT in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 [provide a VPN client which can protect all IP traffic using IPsec as defined in the PP-Module for VPN Client] with the exception of IP traffic needed to manage the VPN connection, and traffic needed for correct functioning of the TOE no other traffic when the VPN is enabled. This SFR is identical to its definition in the Base-PP except that the selection item that requires the TOE to implement its own VPN client is always selected when the TOE’s conformance claim includes this PP-Module Refer to the EAs for FDP_IFC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 mutually authenticated TLS as defined in the Package for Transport Layer Security, HTTPS, IPsec in accordance with the PP-Module for VPN Client, mutually authenticated DTLS as defined in the Package for Transport Layer Security 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. The selection of “no other protocols” is added to address the case where the TOE only claims support for the protocols that are mandated by the SFR. Refer to the EAs for FIA_X509_EXT.2 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. This PP-Module modifies management function 45 regarding Always-on VPN protection. This SFR is not reproduced in its entirety for size purposes. The only change to this SFR is the following change to management function 45: 45. enable/disable the Always On VPN protection: - a. across device - [d. no other method] M O O O Refer to the EAs for FMT_SMF_EXT.1 in the MDF PP. The only change to this SFR is the change to management function 45. Testing of all other functions is not affected. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall use 802.11-2012 in accordance with the Extended Package for WLAN Clients 802.1X in accordance with the Extended Package for WLAN Clients EAP-TLS in accordance with the Extended Package for WLAN Clients mutually authenticated TLS as defined in the Package for Transport Layer Security IPsec in accordance with the PP-Module for VPN Client and mutually authenticated DTLS as defined in the Package for Transport Layer Security 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 EAs for FTP_ITC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. If this PP-Module is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. The TOE boundary is simply extended to include VPN client functionality that is built in to the device’s software so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDF PP as follows: The security objectives defined by this PP-

Module (see sections 4.1 and 4.2) supplement those defined in the MDF PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.EAVESDROP threat in the MDF PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.FLAWAPP threat in the MDF PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDF PP because the MDF PP makes no assumptions about the network architecture in which the TOE is deployed. The MDF PP includes the A.NOTIFY and A.PRECAUTION assumptions to mitigate the risk of physical theft of the TOE. This is consistent with the A.PHYSICAL assumption in this PP-Module because the MDF PP includes reasonable assumptions about the physical security of the TOE. This assumption is consistent with the MDF PP because the MDF PP includes the A.CONFIG assumption which assumes that all security functions are appropriately configured. This objective is consistent with the O.AUTH objective of the MDF PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.COMMS objective of the MDF PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDF PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.STORAGE objective of the MDF PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the MDF PP and does not define an environment that an MDF TOE is incapable of existing in. The operational environment of a mobile device cannot guarantee physical security, but the OE.PRECAUTION objective in the MDF PP ensures that an appropriate level of physical security is provided. The expectation of trusted configuration is consistent with OE.CONFIG 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. This PP-Module adds IPsec as a

new trusted protocol where x.509 certificate authentication is used. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the MDF PP. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the MDF functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the MDF functionality. The ability to configure the VPN client behavior does not affect whether the MDF as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the MDF to perform its security functions Audit records generated by the VPN client do not interfere with MDF functionality. The possibility of the underlying MDF platform generating audit records is consistent with the MDF PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain VPN client audit records does not interfere with MDM functionality. The MDF PP already contains FAU_SEL.1 as an objective SFR which means that this functionality does not conflict with the expected behavior of a mobile device. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level mobile device behavior, but there are no requirements in the MDF PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the MDF PP because it may be a function offered by the part of the TOE described by the MDF PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the MDF PP but does not prevent any MDF PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the https://github.com/commoncriteria/mobile-device v3.2 https://www.niap-

ccevs.org/Profile/Info.cfm?PPID=417&id=417 In a PP-Configuration that includes the MDF PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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; 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 “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 ECC schemes using Curve25519 schemes that meet the following: RFC 7748 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 at least one of P-256 and P-384 has been made mandatory in support of IPsec due to the mandated support for at least one of DH groups 19 and 20 in FCS_IPSEC_EXT.1.8. Support for “safe-prime” groups has also been added as a selectable option for DH groups that use finite field algorithms. Curve25519 schemes remain selectable for their potential use in satisfying FDP_DAR_EXT.2.2 in the MDF PP; these schemes are not used in support of IPsec. RSA and ECC support for P-521 remain present as selections since they may be used by parts of the TOE that are not specifically related to VPN client functionality. Refer to the EAs for FCS_CKM.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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,” 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). Finite field and Group 14 selections remain present if groups 14, 15, or 24 are selected in FCS_IPSEC_EXT.1.8. This PP-Module does not require the use of RSA for any function but it is present in the selection in case other MDF PP functions require its use. Refer to the EAs for FCS_CKM.2/UNLOCKED in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 SP 800-38C and IEEE 802.11ac-2013) AES-GCMP-256 (as defined in NIST SP 800-38D 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 EAs for FCS_COP.1/ENCRYPT in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 [provide a VPN client which can protect all IP traffic using IPsec as defined in the PP-Module for VPN Client] with the exception of IP traffic needed to manage the VPN connection, and traffic needed for correct functioning of the TOE no other traffic when the VPN is enabled. This SFR is identical to its definition in the Base-PP except that the selection item that requires the TOE to implement its own VPN client is always selected when the TOE’s conformance claim includes this PP-Module Refer to the EAs for FDP_IFC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. 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 mutually authenticated TLS as defined in the Package for Transport Layer Security, HTTPS, IPsec in accordance with the PP-Module for VPN Client, mutually authenticated DTLS as defined in the Package for Transport Layer Security 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. The selection of “no other protocols” is added to address the case where the TOE only claims support for the protocols that are mandated by the SFR. Refer to the EAs for FIA_X509_EXT.2 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. This PP-Module modifies management function 45 regarding Always-on VPN

protection. This SFR is not reproduced in its entirety for size purposes. The only change to this SFR is the following change to management function 45: 45. enable/disable the Always On VPN protection: - a. across device - [d. no other method] M O O O Refer to the EAs for FMT_SMF_EXT.1 in the MDF PP. The only change to this SFR is the change to management function 45. Testing of all other functions is not affected. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The TSF shall use 802.11-2012 in accordance with the Extended Package for WLAN Clients 802.1X in accordance with the Extended Package for WLAN Clients EAP-TLS in accordance with the Extended Package for WLAN Clients mutually authenticated TLS as defined in the Package for Transport Layer Security IPsec in accordance with the PP-Module for VPN Client and mutually authenticated DTLS as defined in the Package for Transport Layer Security 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 EAs for FTP_ITC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed. If this PP-Module is used to extend the MDF PP, the TOE type for the overall TOE is still a mobile device. The TOE boundary is simply extended to include VPN client functionality that is built in to the device’s software so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDF PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDF PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK and T.EAVESDROP threats in the MDF PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.EAVESDROP threat in the MDF PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.FLAWAPP threat in the MDF PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDF PP because the MDF PP makes no assumptions about the network architecture in which the TOE is deployed. The MDF PP includes the A.NOTIFY and A.PRECAUTION assumptions to mitigate the risk of physical theft of the TOE. This is consistent with the A.PHYSICAL assumption in this PP-Module because the MDF PP includes reasonable assumptions about the physical security of the TOE. This assumption is consistent with the MDF PP because the MDF PP includes the A.CONFIG assumption which assumes that all security functions are appropriately configured. This objective is consistent with the O.AUTH objective of the MDF PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.COMMS objective of the MDF PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDF PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.STORAGE objective of the MDF PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the MDF PP and does not define an environment that an MDF TOE is incapable of existing in. The operational environment of a mobile device cannot guarantee physical security, but the OE.PRECAUTION objective in the MDF PP ensures that an appropriate level of physical security is provided. The expectation of trusted configuration is consistent with OE.CONFIG 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the MDF PP. This SFR defines the VPN client’s IPsec implementation, which is added functionality that does not interfere with the MDF functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the MDF functionality. The ability to configure the VPN client behavior does not affect whether the MDF as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the MDF to perform its security functions Audit records generated by the VPN client do not interfere with MDF functionality. The possibility of the underlying MDF platform generating audit records is consistent with the MDF PP, which already contains FAU_GEN.1. The ability to suppress the generation of certain VPN client audit records does not interfere with MDM functionality. The MDF PP already contains FAU_SEL.1 as an objective SFR which means that this functionality does not conflict with the expected behavior of a mobile device. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level mobile device behavior, but there are no requirements in the MDF PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the MDF PP because it may be a function offered by the part of the TOE described by the MDF PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the MDF PP but does not prevent any MDF PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of

pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. .

2.2.1 Modified SFRs

2.2.1.1 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1
Refer to the EAs for FCS_CKM.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

FCS_CKM.2/UNLOCKED Cryptographic Key Establishment

FCS_CKM.2/UNLOCKED
Refer to the EAs for FCS_CKM.2/UNLOCKED in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

FCS_COP.1/ENCRYPT Cryptographic Operation

FCS_COP.1/ENCRYPT
Refer to the EAs for FCS_COP.1/ENCRYPT in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

2.2.1.2 User Data Protection (FDP)

FDP_IFC_EXT.1 Subset Information Flow Control

FDP_IFC_EXT.1
Refer to the EAs for FDP_IFC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

2.2.1.3 Identification and Authentication (FIA)

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2
Refer to the EAs for FIA_X509_EXT.2 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

2.2.1.4 Security Management (FMT)

FMT_SMF_EXT.1 Specification of Management Functions

FMT_SMF_EXT.1
Refer to the EAs for FMT_SMF_EXT.1 in the MDF PP. The only change to this SFR is the change to management function 45. Testing of all other functions is not affected.

2.2.1.5 Trusted Path/Channels (FTP)

FTP_ITC_EXT.1 Trusted Channel Communication

FTP_ITC_EXT.1
Refer to the EAs for FTP_ITC_EXT.1 in the MDF PP. The only change to this SFR is that some selections are mandated, therefore the corresponding testing is mandatory. The actual testing for those selections is not changed.

2.3 https://github.com/commoncriteria/application release-1.4 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429 In a PP-Configuration that includes the App PP, the VPN client is

expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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/AK 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 DH 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 2.1 [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/AK to be claimed. This SFR is evaluated in conjunction with FCS_CKM.1/AK 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 AES-CCM (as defined in NIST SP 800-38C) mode AES-CTR (as defined in NIST SP 800-38A) 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 beyond what is required by the EA for FCS_COP.1/SKC in the App PP. There are no test EAs beyond what is required by the EA for FCS_COP.1/SKC in the App PP. 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. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The application shall encrypt all transmitted [sensitive data] using IPsec as specified in FCS_IPSEC_EXT.1 and HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server HTTPS as a server with mutual authentication in accordance with FCS_HTTPS_EXT.2 TLS as defined in the Functional Package for TLS DTLS as defined in the Functional Package for TLS SSH as defined in the Functional Package for Secure Shell no other protocols between itself and another trusted IT product. This SFR is identical to what is defined in the App PP except that mandatory support for IPsec is added, the ST author is forced to select the 'encrypt all transmitted sensitive data' option, and the options for invoking platform-provided functionality have been removed. Since it is possible that a conformant TOE may not use any encryption protocols other than IPsec, "no other protocols" is provided as a selectable option in the list of supported protocols. For IPsec, refer to the EA for FCS_IPSEC_EXT.1. If other protocols are selected for FTP_DIT_EXT.1, refer to the EA for FTP_DIT_EXT.1 in the App PP. 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 or 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 guidance 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 or CSP data (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key or 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 or 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 guidance EAs for this requirement. For each key clearing situation described in the TSS, the evaluator shall repeat the following test. The evaluator shall use appropriate combinations of specialized OE 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. If this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is made more specific by defining the TOE as a specific type of application. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the App PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the App PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the App PP. The threat of a misconfigured VPN client is consistent with the T.LOCAL_ATTACK threat in the App PP. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the App PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the App PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the App PP because the App PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the App PP but is consistent with the A.PLATFORM assumption defined in the App PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE's configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the App PP. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the App PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the App PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the App PP and does not define an environment that is globally applicable to

all software applications. This is part of satisfying OE.PLATFORM as defined in the App PP because physical security is required for the underlying platform to be considered 'trustworthy'. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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. Additionally, this behavior is selection-based in the App PP but is made mandatory since it is required for VPN client functionality. 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 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 ST author is given guidance to make specific selections if this selection-based SFR is claimed in support of IPsec functionality. The SFR behavior itself is unmodified. This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. This PP-Module is for the VPN Client 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. This PP-Module adds a requirement for key storage, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This PP-Module adds a requirement for key destruction, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the App PP. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the application functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the general application functionality. The ability to configure the VPN client behavior does not affect whether the application as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the application to perform its security functions Audit records generated by the VPN client do not interfere with application functionality. For cases where auditing is performed by the TOE platform, a software application is installed on a general-purpose OS or mobile device, both of which can reasonably be expected to provide audit functionality. The ability to suppress the generation

of certain audit records related to VPN activity does not interfere with the ability of the application to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the App PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the App PP because it may be a function offered by the OE in which a TOE defined by the App PP is deployed. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the App PP but does not prevent any App PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the https://github.com/commoncriteria/application release-1.4 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429 In a PP-Configuration that includes the App PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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/AK 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 DH 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 2.1 [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/AK to be claimed. This SFR is evaluated in conjunction with FCS_CKM.1/AK 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 AES-CCM (as defined in NIST SP 800-38C) mode AES-CTR (as defined in NIST SP 800-38A) 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 beyond what is required by the EA for FCS_COP.1/SKC in the App PP. There are no test EAs beyond what is required by the EA for FCS_COP.1/SKC in the App PP. 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. This PP-Module adds IPsec as a new protocol that is used to implement trusted channels. The application shall encrypt all transmitted [sensitive data] using IPsec as specified in FCS_IPSEC_EXT.1 and HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server HTTPS as a server with mutual authentication in accordance with FCS_HTTPS_EXT.2 TLS as defined in the Functional Package for TLS DTLS as defined in the Functional Package for TLS SSH as defined in the Functional Package for Secure Shell no other protocols between itself and another trusted IT product. This SFR is identical to what is defined in the App PP except that mandatory support for IPsec is added, the ST author is forced to select the ‘encrypt all transmitted sensitive data’ option, and the options for invoking platform-provided functionality have been removed. Since it is possible that a conformant TOE may not use any encryption protocols other than IPsec, “no other protocols” is provided as a selectable option in the list of supported protocols. For IPsec, refer to the EA for FCS_IPSEC_EXT.1. If other protocols are selected for FTP_DIT_EXT.1, refer to the EA for FTP_DIT_EXT.1 in the App PP. 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 or 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 guidance

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 or CSP data (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key or 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 or 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 guidance EAs for this requirement. For each key clearing situation described in the TSS, the evaluator shall repeat the following test. The evaluator shall use appropriate combinations of specialized OE 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. If this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is made more specific by defining the TOE as a specific type of application. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the App PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the App PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the App PP. The threat of a misconfigured VPN client is consistent with the T.LOCAL_ATTACK threat in the App PP. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the App PP. A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the App PP. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the App PP because the App PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the App PP but is consistent with the A.PLATFORM assumption defined in the App PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE’s configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the App PP. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.PROTECTED_COMMS objective of the App PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the App PP, which expects a conformant TOE to implement measures to maintain its own integrity. This objective is consistent with the O.PROTECTED_STORAGE objective of the App PP, which ensures that sensitive data is not disclosed without authorization. This objective addresses behavior that is out of scope of the App PP and does not define an environment that is globally applicable to all software applications. This is part of satisfying OE.PLATFORM as defined in the App PP because physical security is required for the underlying platform to be considered ‘trustworthy’. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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. Additionally, this behavior is

selection-based in the App PP but is made mandatory since it is required for VPN client functionality. 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 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 ST author is given guidance to make specific selections if this selection-based SFR is claimed in support of IPsec functionality. The SFR behavior itself is unmodified. This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used. This PP-Module is for the VPN Client 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. This PP-Module adds a requirement for key storage, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This PP-Module adds a requirement for key destruction, which is new functionality when compared to the App PP but does not interfere with its existing security functions. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the App PP. This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the application functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the general application functionality. The ability to configure the VPN client behavior does not affect whether the application as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the application to perform its security functions Audit records generated by the VPN client do not interfere with application functionality. For cases where auditing is performed by the TOE platform, a software application is installed on a general-purpose OS or mobile device, both of which can reasonably be expected to provide audit functionality. The ability to suppress the generation of certain audit records related to VPN activity does not interfere with the ability of the application to satisfy its security functionality. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the App PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the App PP because it may be a function offered by the OE in which a TOE defined by the App PP is deployed. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the App PP but does not prevent any App PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. .

2.3.1 Modified SFRs

2.3.1.1 Cryptographic Support (FCS)

FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

FCS_CKM.1/AK
Refer to the EA for FCS_CKM.1/AK in the App PP.

FCS_CKM.2 Cryptographic Key Establishment

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

FCS_CKM.1 Cryptographic Key Generation Services

FCS_CKM.1
This SFR is evaluated in conjunction with FCS_CKM.1/AK in the App PP.

FCS_COP.1/SKC Cryptographic Operation

FCS_COP.1/SKC
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 beyond what is required by the EA for FCS_COP.1/SKC in the App PP.

Tests

There are no test EAs beyond what is required by the EA for FCS_COP.1/SKC in the App PP.

2.3.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.2 X.509 Certificate Authentication

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

2.3.1.3 Trusted Path/Channels (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1
For IPsec, refer to the EA for FCS_IPSEC_EXT.1. If other protocols are selected for FTP_DIT_EXT.1, refer to the EA for FTP_DIT_EXT.1 in the App PP.

2.3.2 Additional SFRs

2.3.2.1 Cryptographic Support (FCS)

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2
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 guidance EAs for this requirement.

Tests
There are no test EAs for this requirement.

FCS_CKM_EXT.4 Cryptographic Key Destruction

FCS_CKM_EXT.4
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 guidance EAs for this requirement.

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

- **Test 3.1:** The evaluator shall use appropriate combinations of specialized OE 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 https://github.com/commoncriteria/mdm v4.0 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=428&id=428 In a PP-Configuration that includes the MDM PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 meets 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 meets the following: FIPS PUB 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 defined in the MDM PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 PP-Module. Refer to the EA for FCS_COP.1(1) in the MDM PP. 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 PP-Module does not modify this element. Refer to the EA for FIA_X509_EXT.2 in the MDM PP. 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 defined in the MDM PP as FPT_ITT.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 above. 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. 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 the trusted channel for list of services for which the TSF is able to initiate communications. This SFR is defined in the MDM PP as FTP_ITC.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 noted by the refinements above. 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. 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 defined in the MDM PP as FTP_TRP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 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. If this PP-Module is used to extend the MDM PP, the TOE type for the overall TOE is still a mobile device management solution. The TOE boundary is simply extended to include VPN client functionality that is included with the MDM software so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDM PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDM PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the MDM PP A failure of TSF functionality could compromise the implementation of the IPsec channel, which would lead to an exploitation of the T.NETWORK_ATTACK threat. The

A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDM PP because the MDM PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the MDM PP but is consistent with the A.MDM_SERVER_PLATFORM assumption defined in the MDM PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE's configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the MDM PP. This objective is consistent with the O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDM PP, which expects a conformant TOE to implement measures to maintain its own integrity. There are no objectives in the MDM PP that directly relate to this objective, but it could be considered to support both the O.ACCOUNTABILITY and O.MANAGEMENT objectives in the MDM PP by ensuring that stored data cannot be modified through unauthorized mechanisms that may allow for access control and logging functions to be bypassed. This objective addresses behavior that is out of scope of the MDM PP and does not define an environment that an MDM TOE is incapable of existing in. This is part of satisfying OE.IT_ENTERPRISE as defined in the MDM PP because provisioning of physical security is a reasonable expectation for an IT enterprise. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. When this SFR relates to the PP-Module's functionality, the ST author is instructed to make specific selections to implement this behavior using the VPN client. This is done by forcing the ST author to make specific selections that are already present in the MDM PP definition of the SFR; no new behavior is introduced by this. When this SFR relates to the PP-Module's functionality, the ST author is

instructed to make specific selections to implement this behavior using the VPN client at minimum. This is done by forcing the ST author to make a specific selection that is already present in the MDM PP definition of the SFR and by removing a selection option; no new behavior is introduced by this. When this SFR relates to the PP-Module's functionality, the ST author is instructed to make specific selections to implement this behavior using the VPN client at minimum. This is done by forcing the ST author to make a specific selection that is already present in the MDM PP definition of the SFR and by removing a selection option; no new behavior is introduced by this. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the MDM PP This SFR defines the VPN client's IPsec implementation, which is added functionality that does not interfere with the MDM functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the MDM functionality. The ability to configure the VPN client behavior does not affect whether the MDM as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the MDM to perform its security functions. Audit records generated by the VPN client do not interfere with MDM functionality. The possibility of the MDM as a whole generating audit records is consistent with the MDM PP, which already contains FAU_GEN.1 The ability to suppress the generation of certain VPN client audit records does not interfere with MDM functionality. The MDM PP already contains FAU_SEL.1 as an optional SFR which means that this functionality does not conflict with the expected behavior of an MDM. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the MDM PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the MDM PP because it may be a function offered by the part of the TOE described by the MDM PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the MDM PP but does not prevent any MDM PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only

applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the https://github.com/commoncriteria/mdm v4.0 https://www.niap-ccevs.org/Profile/Info.cfm?PPID=428&id=428 In a PP-Configuration that includes the MDM PP, the VPN client is expected to rely on some of the security functions implemented by the OS as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.5. 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 meets 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 meets the following: FIPS PUB 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 defined in the MDM PP as FCS_COP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 PP-Module. Refer to the EA for FCS_COP.1(1) in the MDM PP. 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 PP-Module does not modify this element. Refer to the EA for FIA_X509_EXT.2 in the MDM PP. 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 defined in the MDM PP as FPT_ITT.1(1); the formatting of iteration convention was

updated to be consistent with the PP-Module's conventions. 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 above. 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. 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 the trusted channel for list of services for which the TSF is able to initiate communications. This SFR is defined in the MDM PP as FTP_ITC.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 noted by the refinements above. 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. 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 defined in the MDM PP as FTP_TRP.1(1); the formatting of iteration convention was updated to be consistent with the PP-Module's conventions. 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 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. If this PP-Module is used to extend the MDM PP, the TOE type for the overall TOE is still a mobile device management solution. The TOE boundary is simply extended to include VPN client functionality that is included with the MDM software so that additional security functionality is claimed within the scope of the TOE. The threats and assumptions defined by this PP-Module (see sections 3.1 and 3.2) supplement those defined in the MDM PP as follows: The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDM PP as follows: The threat of an attacker gaining access to a network interface or data that is transmitted over it is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP. The threat of a misconfigured VPN client is consistent with the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats in the MDM PP because failure to mitigate against misconfiguration makes these threats more significant. Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the MDM PP A failure of TSF functionality could compromise the implementation of the IPsec channel, which would lead to an exploitation of the T.NETWORK_ATTACK threat. The A.NO_TOE_BYPASS assumption assumes that the OE is configured in such a manner that the only network route to the protected network is through the TOE. This does not conflict with the MDM PP because the MDM PP makes no assumptions about the network architecture in which the TOE is deployed. The assumption that physical security is provided by the environment is not explicitly stated in the MDM PP but is consistent with the A.MDM_SERVER_PLATFORM assumption defined in the MDM PP, which expects the computing platform to be trusted. The assumption that personnel responsible for the TOE’s configuration are trusted to follow the guidance is consistent with the A.PROPER_ADMIN defined in the MDM PP. This objective is consistent with the

O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that trusted remote channels will enforce authentication of remote endpoints. This objective is consistent with the O.DATA_PROTECTION_TRANSIT objective of the MDM PP, which also expects that secure cryptographic functions are used to implement trusted communications. This objective is consistent with the O.INTEGRITY objective of the MDM PP, which expects a conformant TOE to implement measures to maintain its own integrity. There are no objectives in the MDM PP that directly relate to this objective, but it could be considered to support both the O.ACCOUNTABILITY and O.MANAGEMENT objectives in the MDM PP by ensuring that stored data cannot be modified through unauthorized mechanisms that may allow for access control and logging functions to be bypassed. This objective addresses behavior that is out of scope of the MDM PP and does not define an environment that an MDM TOE is incapable of existing in. This is part of satisfying OE.IT_ENTERPRISE as defined in the MDM PP because provisioning of physical security is a reasonable expectation for an IT enterprise. The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN 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 ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. When this SFR relates to the PP-Module’s functionality, the ST author is instructed to make specific selections to implement this behavior using the VPN client. This is done by forcing the ST author to make specific selections that are already present in the MDM PP definition of the SFR; no new behavior is introduced by this. When this SFR relates to the PP-Module’s functionality, the ST author is instructed to make specific selections to implement this behavior using the VPN client at minimum. This is done by forcing the ST author to make a specific selection that is already present in the MDM PP definition of the SFR and by removing a selection option; no new behavior is introduced by this. When this SFR relates to the PP-Module’s functionality, the ST author is instructed to make specific selections to implement this behavior using the VPN client at minimum. This is done by forcing the ST author to make a specific selection that is already present in the MDM PP definition of the SFR and by removing a selection option; no new behavior is introduced by this. This SFR defines the method of key generation for IKE peer authentication, which is a function that does not interfere with the functionality defined in the MDM PP This SFR defines the VPN client’s IPsec implementation, which is added functionality that does not interfere with the MDM functions. The requirement to protect against re-use of residual data is a property of the VPN client behavior and does not impact the MDM functionality. The ability to configure the VPN client behavior does not affect whether the MDM as a whole can perform its security functions. Self-testing of the VPN client functionality does not impact the ability of the MDM to perform its security functions. Audit records generated by the VPN client do not interfere with MDM functionality. The possibility of the MDM as a whole generating audit records is consistent with the MDM PP, which already contains FAU_GEN.1 The ability to suppress the generation of certain VPN client audit records does not interfere with MDM functionality. The MDM PP already contains FAU_SEL.1 as an optional SFR which means that this functionality does not conflict with the expected behavior of an MDM. The ability of the VPN client to prevent split tunneling of IPsec traffic requires it to have hooks into lower-level OS behavior, but there are no requirements in the MDM PP that would prevent this functionality from being supported. This SFR relates to biometric authentication, which does not conflict with the MDM PP because it may be a function offered by the part of the TOE described by the MDM PP. This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections. This SFR defines an additional cryptographic protocol that is beyond the scope of those defined in the MDM PP but does not prevent any MDM PP functionality from being implemented. This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections. .

2.4.1 Modified SFRs

2.4.1.1 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

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

FCS_CKM.2 Cryptographic Key Establishment

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

FCS_COP.1/1 Cryptographic Operation

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

2.4.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.2 X.509 Certificate Authentication

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

2.4.1.3 Protection of the TSF (FPT)

FPT_ITT.1/1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1/1
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.

2.4.1.4 Trusted Path/Channels (FTP)

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

FTP_ITC.1/1
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)

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

FCS_CKM.1/VPN
TSS
The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.

Guidance
There are no guidance 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/AK
- MDM PP: FCS_CKM.1

FCS_IPSEC_EXT.1 IPsec

FCS_IPSEC_EXT.1
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 OS 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 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
TSS
The evaluator shall examine the TSS and determine that it describes how the IPsec capabilities are implemented.

If the TOE is a standalone software application, the evaluator shall ensure that the TSS asserts that all IPsec functionality is implemented by the TSF. The evaluator shall also ensure that the TSS identifies what platform functionality the TSF relies upon to support its IPsec implementation, if any (e.g. does it invoke cryptographic primitive functions from the platform’s cryptographic library, enforcement of packet routing decisions by low-level network drivers).

If the TOE is part of a general-purpose desktop or mobile OS, the evaluator shall ensure that the TSS describes at a high level the architectural relationship between the VPN client portion of the TOE and the rest of the TOE (e.g. is the VPN client an integrated part of the OS or is it a standalone executable that is bundled into the OS package). If the SPD is implemented by the underlying platform in this case, 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.

In all cases, the evaluator shall also ensure that the TSS describes how the client interacts with the network stack of the platforms on which it can run (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).

The evaluator shall ensure that 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.

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.

Tests
Depending on the implementation, the evaluator may be required to use a VPN gateway or some form of application to configure the client. 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 4.1:** 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 4.2:** 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.

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, transport mode, or either mode (as selected).

Guidance
The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

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.

Tests
The evaluator shall perform the following tests based on the selections chosen:

- **Test 5.1:** [conditional]: If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures a VPN gateway to operate in tunnel mode. The evaluator configures the TOE 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 5.2:** [conditional]: If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec peer to accept IPsec connections using transport mode. The evaluator configures the TOE 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 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 5.3:** [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 5.4:** [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.

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.

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

Tests
The evaluator shall perform the following test:

- **Test 6.1:** 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-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.

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 the relevant iteration of FCS_COP.1 from the Base-PP that applies to keyed-hash message authentication.

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.

Tests

- **Test 7.1:** The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE 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 is configured to use those algorithms and the evaluator attempts to establish a connection using ESP for those algorithms selected.

FCS_IPSEC_EXT.1.5
TSS
The evaluator shall examine the TSS to verify that IKEv1, IKEv2, or both IKEv1 and 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.

Guidance
The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1, IKEv2, or both (as selected), and uses the guidance to configure the TOE 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.

Tests

- **Test 8.1:** The evaluator shall configure the TOE 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 the TOE supports IKEv1 with or without XAUTH, the evaluator shall verify that this test can be successfully repeated with XAUTH enabled and disabled in the manner specified by the operational guidance. If the TOE only supports IKEv1 with XAUTH, the evaluator shall verify that connections not using XAUTH are unsuccessful. If the TOE only supports IKEv1 without XAUTH, the evaluator shall verify that connections using XAUTH are unsuccessful.
- **Test 8.2:** [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 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.

FCS_IPSEC_EXT.1.6
TSS
The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKE payload for each supported IKE version, 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.

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.

Tests
The evaluator shall use the operational guidance to configure the TOE (or to configure the OE to have the TOE receive configuration) to perform the following test for each ciphersuite selected:

- **Test 9.1:** The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKE payload for each supported IKE version 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.

FCS_IPSEC_EXT.1.7
TSS
There are no TSS EAs for this requirement.

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.

Tests
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 10.1:** [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 10.2:** [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 10.3:** [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 10.4:** [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 or time value is reached.

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.

Guidance
There are no guidance EAs for this requirement.

Tests
The evaluator shall perform the following test:

- **Test 11.1:** 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.

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.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this requirement.

FCS_IPSEC_EXT.1.10
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.9.
FCS_IPSEC_EXT.1.11
TSS
The evaluator shall ensures that the TSS whether peer authentication is performed using RSA, ECDSA, or both.

If any selection with pre-shared keys is chosen in the selection, the evaluator shall check to ensure that the TSS describes how those selections work in conjunction with authentication of IPsec connections.

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 fields 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.

Guidance
If any selection with "Pre-shared Keys" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.

If any method other than no other method is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.

The evaluator ensures the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA, ECDSA, or either, depending which is claimed in the ST.

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

The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifiers for the peer.

Tests
For efficiency's sake, the testing that is performed here has been combined with the testing for **FIA_X509_EXT.2** and **FIA_X509_EXT.3** (for IPsec connections and depending on the Base-PP), **FCS_IPSEC_EXT.1.12**, and **FCS_IPSEC_EXT.1.13**. The following tests shall be repeated for each peer authentication protocol selected in the **FCS_IPSEC_EXT.1.11** selection above:

- **Test 12.1:** The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE 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 a previously generated private key and corresponding certificate.
- **Test 12.2:** The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.
- **Test 12.3:** The evaluator shall test that the TOE 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 current version 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 will not establish an SA
- **Test 12.4:** [conditional]: For each selection made, the evaluator shall verify factors are required, as indicated in the operational guidance, to establish an IPsec connection with the server.
  For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:
- **Test 12.5:** 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 12.6:** 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 12.7:** [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 12.8:** [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. **To demonstrate a comparison of DN values, the evaluator shall change any one of the four DN values and verify that the IKE authentication fails.**
- **Test 12.9:** [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 12.10:** [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.

FCS_IPSEC_EXT.1.12
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.
FCS_IPSEC_EXT.1.13
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.
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 or IKEv2 CHILD_SA suites (depending on the supported IKE versions) 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.

Guidance
There are no guidance EAs for this requirement.

Tests
The evaluator follows the guidance to configure the TOE to perform the following tests:

- **Test 13.1:** 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 13.2:** [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 13.3:** 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 13.4:** 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.

2.5.2 User Data Protection (FDP)

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2
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 guidance 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)

FMT_SMF.1/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

FPT_TST_EXT.1/VPN
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 14.1:** The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful.
- **Test 14.2:** 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

2.6.1 Identification and Authentication (FIA)

FIA_BMA_EXT.1 Biometric Activation

FIA_BMA_EXT.1
TSS
The evaluator shall confirm that the TSS describes the calls to the platform and verifies they align with platform documentation.

Guidance
The evaluator shall ensure that any configuration details needed to enable the biometric prompt are included in the guidance documentation.

Tests

- **Test 15.1:** The evaluator shall initiate a connection and verify that a biometric prompt is presented and accepted before the connection can proceed. The evaluator shall also verify the connection does not proceed if the biometric is not presented or accepted.

2.6.2 Packet Filtering (FPF)

FPF_MFA_EXT.1 Multifactor Authentication Filtering

FPF_MFA_EXT.1
TSS
The evaluator shall examine the TSS to verify that it describes how authentication packets are identified and how all other traffic is blocked until secondary authentication is successful.

Guidance
The evaluator shall examine the operational guidance to verify that it provides instructions to the administrator on how to configure the secondary HOTP or TOTP factors and any additional details necessary for filtering all other traffic.

Tests

- **Test 16.1:** For each included selection the evaluator shall configure the TOE per the operational guidance. The evaluator shall attempt to connect and verify other traffic is rejected per the filtering rules. The evaluator shall then provide the selected factor and confirm it is accepted and traffic is no longer blocked.

2.7 Evaluation Activities for Selection-Based SFRs

2.7.1 Cryptographic Support (FCS)

FCS_EAP_EXT.1 EAP-TLS

FCS_EAP_EXT.1
TSS
The evaluator shall verify that the TS describes the use of EAP options for each of the selected peer authentication mechanisms, that TLS with mutual authentication is used, that the random values are from an appropriate source, and that the EAP MSK is derived from the TLS master key and is used as the IKEv2 shared key.

Guidance
The evaluator shall verify that the guidance documents describe any configurable features of the EAP or TLS functionality, including instructions for configuration of the authenticators and registration processes for clients.

Tests
Testing for TLS functionality is in accordance with the TLS package. For each supported EAP method claimed in FCS_EAP_TLS_EXT.1.1 and for each authentication method claimed in FCS_EAP_TLS_EXT.1.3, the evaluator shall perform the following tests:

- **Test 17.1:** The evaluator shall follow AGD guidance to configure the TSF to use the EAP method claimed. The evaluator shall follow AGD guidance to configure the TSF to use the authentication method claimed and, for EAP-TTLS, register a client with the appropriate key material required for the authentication method. The evaluator shall establish an VPN session using a test client with a valid certificate and, for EAP-TTLS, configured to provide a correct value for the configured authenticator. The evaluator shall observe the the VPN session is successful.
- **Test 17.2:** (conditional for EAP-TTLS support): The evaluator shall cause the test client with a valid certificate to send an invalid authenticator for the claimed authentication method: For HOTP, replay the HOTP value sent previously, For TOTP or PSK, modify a byte of the properly constructed value,and observe that the TSF aborts the session
- **Test 17.3:** The evaluator shall establish a new, valid certificate for a test client using an identifier not

corresponding to a registered user. For EAP-TTLS, the evaluator shall cause the test client using this certificate to send a correct authenticator value for the registered user. The evaluator shall initiate a VPN session from the test client to the TSF and observe that the TSF aborts the session.
- **Test 17.4:** The evaluator shall follow AGD guidance to configure the TSF to use a supported EAP method and register the user with the key material required for a supported authentication method. The evaluator shall configure a test client to respond to an IKEv2 exchange with EAP-request, providing valid phase 1 handshake and valid TLS handshake, but computing the phase 2 shared key using standard (non-EAP) methods. The evaluator shall initiate a VPN session between the test client and the TSF, and observe that the TSF aborts the session.

2.7.2 Identification and Authentication (FIA)

FIA_HOTP_EXT.1 HMAC-Based One-Time Password Pre-Shared Keys

FIA_HOTP_EXT.1
TSS
The evaluator shall confirm the TSS describes how the TOE complies with the RFC.

The evaluator shall confirm the TSS describes how the HOTP seed is generated and ensure it aligns with FCS_RBG_EXT.1.

The evaluator shall confirm the TSS describes how the HOTP seed is protected and ensure it aligns with the storage requirements of the Base-PP.

The evaluator shall confirm the TSS describes how a new HOTP seed is assigned for each client and how each client is uniquely identified.

The evaluator shall confirm the TSS describes how the HOTP seed is conditioned into an HOTP hash and verify it matches the selection in FIA_HOTP_EXT.1.4.

The evaluator shall confirm the TSS describes how the HOTP hash is truncated and verify it matches the selection in FIA_HOTP_EXT.1.5.

The evaluator shall confirm the TSS describes how the TOE handles multiple incoming invalid requests and verify it provides an anti-hammer mechanism that matches the selections made in FIA_HOTP_EXT.1.6.

The evaluator shall confirm the TSS describes how the TOE handles resynchronization and how it rejects attempts outside of the look-ahead window selected in FIA_TOTP_EXT.1.7.

The evaluator shall confirm the TSS describes how the TOE counter is incremented after each successful authentication.

Guidance
The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA_HOTP_EXT.1 requirements.

Tests
The evaluator shall configure the TOE to use a supported HOTP factor then:

- **Test 18.1:** Attempt to establish a connection using a factor from a different client. The test passes if the client fails to connect.
- **Test 18.2:** Attempt multiple connections outside the boundary set in FIA_HOTP_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 18.3:** Attempt to use an HOTP that is outside of the value allowed for resynchronization. The test passes if the client fails to connect.
- **Test 18.4:** Attempt to connect with a valid HOTP, disconnect and attempt to authenticate again with the same HOTP value. The test passes if the client connects the first time and fails to connect the second time. If the HOTP generated is duplicated the test may be repeated.

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it identifies all protocols that allow pre-shared keys. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states which pre-shared key selections are supported.

Guidance
The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required.

Tests

The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE).

- **Test 19.1:** For each mechanism selected in FIA_PSK_EXT.1.2, the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection.

FIA_PSK_EXT.2 Generated Pre-Shared Keys

FIA_PSK_EXT.2
TSS
If "generate" is selected, the evaluator shall confirm that this process uses the RBG specified in FCS_RBG_EXT.1 and the output matches the size selected in FIA_PSK_EXT.2.1.

Guidance
The evaluator shall confirm the operational guidance contains instructions for entering generated pre-shared keys for each protocol identified in the FIA_PSK_EXT.1.1.

Tests

- **Test 20.1:** [conditional] If generate was selected the evaluator shall generate a pre-shared key and confirm the output matches the size selected in FIA_PSK_EXT.2.1.

FIA_PSK_EXT.3 Password-Based Pre-Shared Keys

FIA_PSK_EXT.3
TSS
The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are used.

Support for length: The evaluator shall check to ensure that the TSS describes the allowable ranges for PSK lengths, and that at least 64 characters or a length defined by the platform may be specified by the user.

Support for character set: The evaluator shall check to ensure that the TSS describes the allowable character set and that it contains the characters listed in the SFR.

Support for PBKDF: The evaluator shall examine the TSS to ensure that the use of PBKDF2 is described and that the key sizes match that described by the ST author.

The evaluator shall check that the TSS describes the method by which the PSK is first encoded and then fed to the hash algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself.

For the NIST SP 800-132-based conditioning of the PSK, the required evaluation activities will be performed when doing the evaluation activities for the appropriate requirements (FCS_COP.1/KeyedHash).

The evaluator shall confirm that the minimum length is described.

The ST author shall provide a description in the TSS regarding the salt generation. The evaluator shall confirm that the salt is generated using an RBG described in FCS_RBG_EXT.1.

[conditional] If password strength meter or password denylist is selected, the evaluator shall examine the TSS to ensure any password checking functionality provided by the TSF is described and contains details on how the function operates.

Guidance
The evaluator shall confirm the operational guidance contains instructions for 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 confirm that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.

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.3.2.

The evaluator shall confirm the operational guidance contains any necessary instructions for enabling and configuring password checking functionality.

Tests
Support for Password/Passphrase characteristics: In addition to the analysis above, the evaluator shall also perform the following tests on a TOE configured according to the Operational Guidance:

- **Test 21.1:** The evaluator shall compose a pre-shared key of at least 64 characters that contains a combination of the allowed characters in accordance with the FIA_PSK_EXT.1.3 and verify that a

successful protocol negotiation can be performed with the key.
- **Test 21.2:** [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length and invalid lengths that are below the minimum length, above the maximum length, null length, empty length, or zero length. The minimum test should be successful, and the invalid lengths must be rejected by the TOE.
- **Test 21.3:** [conditional]: If the TOE initiates connections, initiate and establish a remote connection, disconnect from the connection, verify that the PSK is required when initiating the connection a second time.
- **Test 21.4:** [conditional]: If the TOE supports a password meter, the evaluator shall enter a password and verify the password checker responds per the description in the TSS.
- **Test 21.5:** [conditional]: If the TOE supports a password denylist, the evaluator shall enter a denylisted password and verify that the password is rejected or flagged as such.

FIA_PSK_EXT.4 HMAC-Based One-Time Password Pre-shared Keys Support

FIA_PSK_EXT.4
TSS
The evaluator shall verify the TSS describes how the HOTP is input into the client and how that value is sent to the server.

The evaluator shall verify the TSS describes how the HOTP is accepted from an incoming connection and how that value is verified, either by the TOE or by an external authentication server.

Guidance
The evaluator shall verify the operational guidance contains any configuration necessary to enable HOTP.

Tests

- **Test 22.1:** The evaluator shall configure the TOE to use a supported HOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the HOTP before initiating the connection. The evaluator shall verify the server validates the HOTP or receives confirmation from an authentication server before establishing the channel.

FIA_PSK_EXT.5 Time-Based One-Time Password Pre-shared Keys Support

FIA_PSK_EXT.5
TSS
The evaluator shall verify the TSS describes how the TOTP is input into the client and how that value is sent to the server.

The evaluator shall verify the TSS describes how the TOTP is accepted from an incoming connection and how that value is verified, either by the TOE or by an external authentication server.

Guidance
The evaluator shall verify the operational guidance contains any configuration necessary to enable TOTP.

Tests

- **Test 23.1:** The evaluator shall configure the TOE to use a supported TOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the TOTP before initiating the connection. The evaluator shall verify the server validates the TOTP or receives confirmation from an authentication server before establishing the channel.

FIA_TOTP_EXT.1 Time-Based One-Time Password Pre-Shared Keys

FIA_TOTP_EXT.1
TSS
The evaluator shall confirm the TSS describes how the TOE complies with the RFC.

The evaluator shall confirm the TSS describes how the TOTP seed is generated and ensure it aligns with FCS_RBG_EXT.1.

The evaluator shall confirm the TSS describes how the TOTP seed is protected and ensure it aligns with the storage requirements of the Base-PP.

The evaluator shall confirm the TSS describes how a new TOTP seed is assigned for each client and how each client is uniquely identified.

The evaluator shall confirm the TSS describes how the TOTP seed is conditioned into a TOTP hash and verify it matches the selection in FIA_TOTP_EXT.1.4.

The evaluator shall confirm the TSS describes how the TOTP hash is truncated and verify it matches the selection in FIA_TOTP_EXT.1.5.

The evaluator shall confirm the TSS describes how the TOE handles multiple incoming requests and verify it provides an anti-hammer mechanism that matches the selections made in FIA_TOTP_EXT.1.6.

The evaluator shall confirm the TSS describes how the TOE sets a time-step value and verify it matches the selections in the ST.

The evaluator shall confirm the TSS describes how the TOE handles drift and resynchronization and verify it matches the selections. The evaluator shall ensure the TSS describes how time is kept and whether drift is calculated and recorded. If drift is recorded, the evaluator shall ensure that the TSS describes how this is done.

Guidance
The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA_TOTP_EXT.1 requirements.

Tests
The evaluator shall configure the TOE to use a supported TOTP factor then:

- **Test 24.1:** Attempt to establish a connection using a factor from a different client. The test passes if the client fails to connect.
- **Test 24.2:** Attempt multiple connections outside the boundary set in FIA_TOTP_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 24.3:** Attempt to use a TOTP that is outside of the value allowed for resynchronization. The test passes if the client fails to connect.
  Attempt to connect with a valid TOTP, disconnect and attempt to authenticate again with the same TOTP. The test passes if the client connects the first time and fails to connect the second time. If the TOTP generated is duplicated the test may be repeated.

2.8 Evaluation Activities for Objective SFRs

2.8.1 Security Audit (FAU)

FAU_GEN.1/VPN Audit Data Generation

FAU_GEN.1/VPN
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

FAU_SEL.1/VPN
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 25.1:** 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 25.2:** [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.

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.
[GPOS 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, Version 4.0, April 2019

[App PP]	Protection Profile for Application Software, Version 1.4, October 2021
[SD]	Supporting Document Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, November 2019