Comment: Comment-1-

PP-Module for VPN Client

Version: 2.6
2025-01-31
National Information Assurance Partnership

Revision History

Version	Date	Comment
2.6	2025-01-31	CC:2022 conversion, limitation of cryptographic algorithms to CNSA 1.0, incorporation of TDs
2.5	2024-06-24	Incorporation of TC feedback: • Incorporation of TDs: 0662, 0672, 0690, 0697, 0711, 0725, 0753, 0788 • Corrections to Base-PP references • Definition of auditable events for Additional SFRs • Explicit association of evaluation activities with components and elements
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

Contents

1 Introduction

1.1 Overview

FIA_X509_EXT references to the Base-PPs are now removed and where appropriate the X.509 package is referenced instead. However, it's unclear whether there is still sufficient mechanism to actually 'force' the X.509 SFRs to be included. That is to say, there is nothing in here that says "because IPsec functionality is dependent on X.509 validation, and because the Base-PPs conform to the X.509 FP, the ST shall make the relevant X.509 FP claims." The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of a virtual private network (VPN) client in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- Protection Profile for General Purpose Operating Systems (GPOS PP), Version 4.3
- Protection Profile for Mobile Device Fundamentals (MDF PP), Version 3.3
- Protection Profile for Application Software (App PP), Version 2.0
- Protection Profile for Mobile Device Management (MDM PP), Version 4.0

These Base-PPs are all valid because a VPN client may be a specific type of stand-alone software application or a built-in component of an operating system (OS), whether desktop or mobile. Regardless of which Base-PP is claimed, the VPN client functionality defined by this PP-Module will rely on the Base-PP. Sections 5.1 through 5.4 of this PP-Module describe the relevant functionality for each Base-PP, including specific selections and assignments, or inclusion of optional requirements that must be made as needed to support the VPN client functionality.

1.2 Terms

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

1.2.1 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 (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.

Configuration)	
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.

1.2.2 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 such as 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) that has not been authorized by an authorized administrator to access the TOE or private network.
Unprivileged Mode	A TOE operational mode that only provides VPN client functions for the VPN client user.
VPN Client	The TOE; allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to a private network.
VPN Client User	A user operating the TOE in unprivileged mode.
VPN Gateway	A component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network.

1.3 Compliant Targets of Evaluation

The TOE defined by this PP-Module is the VPN client, a software application that runs on a physical or virtual host platform, used to establish a secure IPsec connection between that host platform and a remote system. The VPN client is intended to be located outside or inside of a private network, and establishes a secure tunnel to an IPsec peer. For the purposes of this PP-Module, IPsec peers are defined as:

- VPN gateways
- Other VPN clients
- An IPsec-capable network device (supporting IPsec for the purposes of management)

The tunnel provides confidentiality, integrity, and data authentication for information that travels across a less trusted (sometimes public) network. All VPN clients that comply with this document will support IPsec.

This PP-Module extends the GPOS PP when the VPN client is installed on an OS discussed in that PP (e.g., Windows, Mac OS, Linux). This PP-Module extends the MDF PP when the VPN client is installed on a self-contained mobile device that is bundled with an OS (e.g. Android, BlackBerry OS, iOS, Windows Mobile). This PP-Module extends the App PP when the VPN client is provided by a third party and is a standalone application that is not a bundled part of an OS or mobile device. This PP-Module extends the MDM PP when the VPN client is included with MDM server software that is used for centralized deployment and administration of enterprise mobile device policies.

As a PP-Module of any of these PPs, it is expected that the content of this PP-Module and the chosen Base-PP be appropriately combined in the context of each product-specific ST. This PP-Module has been specifically defined such that there should be no difficulty or ambiguity in doing so. When this PP-Module is used, conformant TOEs are obligated to implement the functionality required in the claimed Base-PP with the additional functionality defined in this PP-Module in response to the threat environment discussed in this PP-Module.

1.3.1 TOE Boundary

The TOE defined by this PP-Module is purely a software solution executing on a platform (some sort of OS running on hardware). Depending on the Base-PP claimed as part of the TOE, the platform may also be part of the TOE or it may be an environmental component that the TOE vendor has no control over. Regardless of whether the platform itself is within the scope of the evaluation, the VPN client itself will rely on the platform for its execution domain and proper usage. The vendor is expected to provide sufficient installation and configuration instructions to identify an Operational Environment (OE) with the necessary features and to provide instructions for how to configure it correctly.

The PP-Module contains requirements that must be met by the TOE. Depending on the Base-PP that is claimed, there may be some variation in the applicable requirements. This is because a given Base-PP may include one or more requirements that the VPN client can inherit but are not shared between each possible Base-PP.

This is somewhat different than other PPs, but addresses most implementations of VPN clients where some part of the functionality of the IPsec tunnel is provided by the platform. In terms of the cryptographic primitives (random bit generation, encryption and decryption, key generation, etc.) it is actually desirable that a well-tested implementation in the platform is used rather than trying to implement these functions in each client.

Requirements that can be satisfied by either the TOE or the platform are identified in Section 5 by text such as “The [selection: TSF, TOE platform] shall…” The ST author will make the appropriate selection based on where that element is implemented. It is allowable for some elements in a component to be implemented by the TOE, while other elements in that same component be implemented by the platform (requirements on the usage of X.509 certificates is an example of where this might be the case, where using the information contained in the certificates and the implementation of revocation checking may be done by the TOE, but storage and protection of the certificates may be done by the platform). Note that in the cases where this PP-Module is used to extend the GPOS PP or MDF PP, the TOE includes both the VPN client and the platform. In this case, it is appropriate to indicate that the TOE satisfies this requirement. However, the ST author should make it clear, for each of these components, which are implemented by the VPN client portion of the TOE versus the platform portion.

A Supporting Document (SD) accompanies this PP-Module and contains guidance for how to evaluate the requirements defined by the PP-Module, expressed as Evaluation Activities (EAs). EAs will differ based on where the function that meets the requirement is implemented. In most cases, requirements implemented by the platform will require that the evaluator examine documents pertaining to the platform (generally the ST), while requirements implemented by the TOE may require examination of the TSS, examination of the Operational Guidance, or execution of evaluator testing. For requirements implemented by the platform, there may also be requirements where the evaluator must examine the interfaces used by the TOE to access these functions on the platform. This ensures that the functionality being invoked to satisfy the requirements of this PP-Module is the same functionality that was evaluated.

Given the degree of coupling between a VPN client and its underlying platform, it is expected that the client will be tested on each platform claimed in the ST. In cases where the platforms are simply different versions of the same OS (provided by the same platform vendor), an equivalency argument may be made in lieu of testing on each version. The argument would have to demonstrate that the client interacts in exactly the same way with the versions of the OS (i.e., the same APIs are used with the same parameters, the network stack is

modified with exactly the same kernel modules). The evaluator shall use the operational guidance to configure the TOE and underlying platform.

A TOE that conforms to this PP-Module will implement the Internet Engineering Task Force (IETF) IPsec Security Architecture for the Internet Protocol, RFC 4301, as well as the IPsec Encapsulating Security Payload (ESP) protocol. IPsec ESP is specified in RFC 2406 and RFC 4303. The IPsec VPN client will support ESP in either tunnel mode, transport mode, or both.

The IPsec VPN client will use the Internet Key Exchange (IKE)v1 protocol, IKEv2, or both. IKEv1 is implemented as defined in RFCs 2407, 2408, 2409, and 4109, and IKEv2 is implemented as specified in RFC 7296 and 4307 to authenticate and establish session keys with the VPN entities. The IKEv2 implementation also requires mandatory support for network address translation (NAT) traversal as specified in section 2.23 of RFC 7296.

To show that the TSF implements the RFCs correctly, the evaluator shall perform the EAs documented in the SD that accompanies this PP-Module. In future versions of this PP-Module, EAs may be modified or new ones may be introduced that cover more aspects of RFC compliance than what is currently described in this publication.

The IPsec VPN client enables encryption of all information that flows between itself and its IPsec peer. The VPN client serves as an endpoint for an IPsec VPN connection and performs a number of cryptographic functions related to establishing and maintaining that connection. If the cryptography used to perform endpoint authentication, generate keys, and encrypt information is sufficiently robust and the implementation has no critical design mistakes, an adversary will be unable to exhaust the encryption key space to obtain the data. Compliance with IPsec standards, use of a properly seeded Random Bit Generator (RBG), and secure authentication factors will ensure that access to the transmitted information cannot be obtained with less work than a full exhaust of the key space. Any plaintext secret and private keys or other cryptographic security parameters will be zeroized when no longer in use to prevent disclosure of security critical data.

1.4 Use Cases

A VPN client allows users on the TOE platform to establish secure IPsec communications, providing confidentiality, integrity, and protection of data, across a less trusted network to secure data in transit. This PP-Module defines three use cases for VPN clients. A conformant TOE will implement one or more of the use cases specified below.

[USE CASE 1] TOE to VPN Gateway

A VPN client allows users on the TOE platform to establish an encrypted IPsec tunnel across a less trusted, often unprotected, public network to a private network (see). In this case, the TOE provides encryption and decryption of network packets as they leave and arrive on the VPN client’s underlying platform. IP packets crossing from the private network to the public network will be encrypted if their destination is a remote access VPN client supporting the same VPN policy as the source network. The TOE is responsible for encrypting the packets that are intended to be received by the target on the private network and then encapsulating these packets in a way that allows the VPN gateway to securely receive them and forward them to their final destination.

[USE CASE 2] TOE to VPN Client

A VPN client may additionally or alternatively allow a client computer to connect directly to another computer running a VPN client (see). In this case, the functionality of the VPN client is to connect directly to another endpoint system to facilitate point-to-point communications with that system. IPsec transport mode is used for end-to-end communications. In this use case, the content of the packet data (payload) is encrypted but the original IP header is preserved. Inherent to this use case, when two peers are communicating directly, is the disclosure of the source and destination of the packets. Users should take into consideration any security risks associated with this disclosure when architecting their networks in line with this use case.

[USE CASE 3] TOE to IPsec-Capable Network Device

Similar to Use Case 2 above, a VPN client TOE can also be used to establish a secure connection to an IPsec-capable network device using IPsec, similar to how an SSH connection might be used. In this case, where a network device is being managed remotely over an IPsec connection, the network device itself must contain IPsec functionality to act as the peer for the connection (see). While this will behave functionally the same way as the scenario described by Use Case 2, the user of the TOE in Use Case 3 is a network administrator who is assumed to have administrative access to the network device they are connecting to.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (extended) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- Protection Profile for General Purpose Operating Systems, Version 4.3
- Protection Profile for Mobile Device Fundamentals, Version 3.3
- Protection Profile for Mobile Device Management, Version 4.0
- Protection Profile for Application Software, Version 2.0
- cPP-Module for Wireless LAN Clients, version 1.1
- PP-Module for Bluetooth, version 1.1
- PP-Module for Mobile Device Management Agent, version 1.2
- cPP-Module for Biometric Enrolment and Verification, version 1.1

Package Claim

- This PP-Module is Functional Package for Transport Layer Security Version 2.1 conformant.
- This PP-Module is Functional Package for X.509 Version 1.0 conformant.
- This PP-Module is Assurance Package for Flaw Remediation Version 1.0 conformant.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its OE, and any organizational security policies that the TOE is expected to enforce.

This PP-Module is written to address the situation in which a user accesses a private network (e.g. the user's office network) or terminal endpoint (e.g. a network device) using a less trusted network (such as a public Wi-Fi network or local area network). Protection of network packets is desired as they traverse a public network. To protect the data in transit from disclosure and modification, a VPN is created to establish secure communications. The VPN client provides one end of the secure VPN tunnel and performs encryption and decryption of network packets in accordance with a VPN security policy negotiated between the VPN client (TOE) and its IPsec peer.

The proper installation and configuration of the VPN client is critical to its correct operation such that proper handling of the TOE by an administrator is also addressed.

Note that as a PP-Module, all threats, assumptions, and organizational security policies (OSPs) defined in the Base-PP will also apply to a TOE unless otherwise specified, depending on which of the Base-PPs it extends. The SFRs defined in this PP-Module will mitigate the threats that are defined in the PP-Module but may also mitigate some threats defined in the Base-PPs in more comprehensive detail due to the specific capabilities provided by a VPN client.

3.1 Threats

T.TSF_CONFIGURATION

Configuring VPN tunnels is a complex and time-consuming process, and prone to errors if the interface for doing so is not well-specified or well-behaved. The inability or failure of an ignorant or careless administrator to configure certain aspects of the interface may also lead to the incorrect specification of the desired communications policy or use of cryptography that may be desired or required for a particular site. This may result in unintended weak or plaintext communications while the user thinks that their data are being protected. Other aspects of configuring the TOE or using its security mechanisms (for example, the update process) may also result in a reduction in the trustworthiness of the VPN client.

T.TSF_FAILURE

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

T.UNAUTHORIZED_ACCESS

This PP-Module does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the system or device that contains the IPsec VPN client. Therefore, the primary threat agents are the unauthorized entities that try to gain access to the protected network (in cases where tunnel mode is used) or to plaintext data that traverses the public network (regardless of whether transport mode or tunnel mode is used).

The endpoint of the network communication can be both geographically and logically distant from the TOE and can pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications over the network to be compromised.

Plaintext communication over the network may allow critical data (such as passwords, configuration settings, and user data) to be read or manipulated directly by a malicious user or process on intermediate systems, leading to a compromise of the TOE or to the secured environmental systems that the TOE is being used to facilitate communications with. IPsec can be used to provide protection for this communication; however, there are numerous options that can be implemented for the protocol to be compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification, but will not be able to interact with other diverse equipment that is typically found in large enterprises.

Even though the communication path is protected, there is a possibility that the IPsec peer could be tricked into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE and respond to the request as if it were the TOE. In a similar manner, the TOE could also be tricked into thinking that it is establishing communications with a legitimate IPsec peer when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and

modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and “playing back” that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.

T.USER_DATA_REUSE
Data traversing the TOE could inadvertently be sent to a different user as a consequence of a poorly-designed TOE; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently reused in sending network traffic to a user other than that intended by the sender of the original network traffic.

3.2 Assumptions

These assumptions are made on the Operational Environment (OE) in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an OE that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

A.NO_TOE_BYPASS
Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.

A.PHYSICAL
Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TRUSTED_CONFIG
Personnel configuring the TOE and its OE will follow the applicable security configuration guidance.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the Operational Environment

OE.NO_TOE_BYPASS
Information cannot flow onto the network to which the VPN client’s host is connected without passing through the TOE.

OE.PHYSICAL
Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

OE.TRUSTED_CONFIG
Personnel configuring the TOE and its OE will follow the applicable security configuration guidance.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
A.NO_TOE_BYPASS	OE.NO_TOE_BYPASS	This assumption is satisfied by the environmental objective that ensures network routes do not exist that allow traffic to be transmitted from the TOE system to its intended destination without going through the TOE’s IPsec tunnel.
A.PHYSICAL	OE.PHYSICAL	This assumption is satisfied by the environmental objective that ensures the TOE is not deployed on a system that is vulnerable to loss of physical custody.
A.TRUSTED_CONFIG	OE.TRUSTED_CONFIG	This assumption is satisfied by the environmental objective that ensures that anyone responsible for administering the TOE can be trusted not to misconfigure it, whether intentionally or not.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Protection Profile for Protection Profile for General Purpose Operating System Security Functional Requirements Direction

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.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the GPOS PP and relevant to the secure operation of the TOE.

5.1.1.1 Cryptographic Support (FCS)

FCS_CKM.1: Cryptographic Key Generation

This SFR is functionally identical to what is defined in the GPOS PP except that ECC key generation with support for P-384 has been made mandatory in support of IPsec due to the mandated support for Diffie-Hellman (DH) group 20 in FCS_IPSEC_EXT.1.8.

The text of the requirement is replaced with:

The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm

- ***ECC schemes using “NIST curve” P-384 that meet the following: FIPS PUB 186-5, “Digital Signature Standard (DSS),” Appendix A.2, and,***

[selection:

- *RSA schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.1*
- *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 [* ***selection:*** *RFC 3526, RFC 7919]*
- ***No other key generation methods***

] .

FCS_CKM.2: Cryptographic Key Establishment

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-384 has been made mandatory in support of IPsec due to the mandated support for DH group 20 in FCS_IPSEC_EXT.1.8.

The text of the requirement is replaced with:

The TSF shall **implement functionality to perform cryptographic key establishment** in accordance with a specified cryptographic key **establishment** method:

- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” and***

[selection:

- *Finite field-based key establishment schemes that meets NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”*
- ***No other key generation methods***

] .

5.1.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the GPOS PP is claimed as the Base-PP.

5.1.2.1 Auditable Events for GPOS PP Additional SFRs

Table 2: Auditable Events for GPOS PP Additional SFRs

Requirement	Auditable Events	Additional Audit Record Contents

5.1.2.2 Cryptographic Support (FCS)

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1

The [**selection**: *VPN client* , *OS*] shall store persistent secrets and private keys when not in use in OS-provided key storage.

Application Note: 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.

Evaluation Activities

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the VPN client or the OS, the evaluator shall 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 shall confirm that the TSS lists for what purpose it is used, and how it is stored.

The evaluator shall review the TSS 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.

5.1.2.3 Identification and Authentication (FIA)

FIA_X509_EXT.4 X.509 Certificate Use and Management

FIA_X509_EXT.4.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec exchanges, and [**selection**: *digital signatures for FPT_TUD_EXT.1 , integrity checks for FPT_TST_EXT.1 , no additional uses*] .

FIA_X509_EXT.4.2

When a connection to determine the validity of a certificate cannot be established, the [**selection, choose one of**: *VPN client* , *OS*] shall [**selection, choose one of**: *allow the administrator to choose whether to accept the certificate in these cases , accept the certificate , not accept the certificate*] .

Application Note: 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 in , version , 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 in , version . 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.

FIA_X509_EXT.4.3

The [**selection, choose one of**: *VPN client , OS*] shall not establish an SA if a certificate or certificate path is deemed invalid.

Evaluation Activities

FIA_X509_EXT.4.1
FIA_X509_EXT.4.1 is evaluated as part of FCS_IPSEC_EXT.1 (and conditionally as part of FPT_TUD_EXT.1 or FPT_TST_EXT.1).

FIA_X509_EXT.4.2
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 FIA_X509_EXT.4.2:1: 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.4.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.*

FIA_X509_EXT.4.3
FIA_X509_EXT.4.3 is evaluated as part of FCS_IPSEC_EXT.1.11.

5.1.2.4 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

The **[selection, choose one of: *VPN client* , *OS*] shall use IPsec to** provide a **trusted** communication channel between itself and **[selection:**

- ***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** .

FTP_ITC.1.2

The **[selection, choose one of: *VPN client* , *OS*]** shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The **[selection, choose one of: *VPN client* , *OS*]** shall initiate communication via the trusted channel for [*all traffic traversing that connection*].

Application Note: 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.

Evaluation Activities

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 FTP_ITC.1:1: The evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, or IPsec-capable network device using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test FTP_ITC.1:2: The evaluator shall ensure, for each communication channel with an IPsec peer, the channel data is not sent in plaintext.*
- *Test FTP_ITC.1:3: The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE.*
- *Test FTP_ITC.1:4: The evaluator shall physically interrupt the connection from the TOE to the IPsec peer. The evaluator 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.

5.2 Protection Profile for Protection Profile for Mobile Device Fundamentals Security Functional Requirements Direction

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.

5.2.1 Modified SFRs

The SFRs listed in this section are defined in the MDF PP and relevant to the secure operation of the TOE.

5.2.1.1 Trusted Path/Channels (FTP)

FCS_CKM.1: Cryptographic Key Generation

This SFR is functionally identical to what is defined in the MDF PP except that ECC key generation with support for P-384 has been made mandatory in support of IPsec due to the mandated support for DH group 20 in FCS_IPSEC_EXT.1.8. 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 support remains present as a selection since it may be used by parts of the TOE that are not specifically related to VPN client functionality.

The text of the requirement is replaced with:

The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm

- **ECC schemes using "NIST curve" P-384 that meets the following: FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2**

and [**selection:**

- *RSA schemes using cryptographic key sizes of [* ***assignment:*** *3072-bit or greater] that meet the following: [FIPS PUB 186-5, “Digital Signature Standard (DSS),” Appendix A.1]*
- ***ECC schemes using Curve25519 schemes that meet the following: [RFC 7748]***
- *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 [* ***selection:*** *RFC 3526, RFC 7919]*
- ***no other key generation methods***

].

FCS_CKM.2/UNLOCKED: Cryptographic Key Establishment

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 group 20 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.

The text of the requirement is replaced with:

The TSF shall perform **cryptographic key establishment** in accordance with a specified cryptographic key establishment method:

- **[Elliptic curve-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]**

[**selection:**

- *[RSA-based key establishment schemes] that meet the following: [* ***selection:***
  - *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"*
- *[Finite field-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]*
- ***no other key establishment schemes***

].

FDP_IFC_EXT.1: Subset Information Flow Control

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.

The text of the requirement is replaced with:

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 [**selection:** *[* ***assignment:*** *traffic needed for correct functioning of the TOE], no other traffic*] when the VPN is enabled.

FTP_ITC_EXT.1: Trusted Channel Communication

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.

The text of FTP_ITC_EXT.1.1 is replaced with (the other elements are unaffected):

The TSF shall use

- 802.11-2012 in accordance with the [*PP-Module for Wireless LAN Clients, version 1.1*],
- 802.1X in accordance with the [*PP-Module for Wireless LAN Clients, version 1.1*],
- EAP-TLS in accordance with the [*PP-Module for Wireless LAN Clients, version 1.1*],
- Mutually authenticated TLS in accordance with the [*Functional Package for TLS, version 2.1*],
- **IPsec in accordance with the [** ***PP-Module for VPN Clients, version 2.6*** **],**

and [**selection:**

- *mutually authenticated DTLS as defined in the Functional Package for TLS, version 2.1*
- *HTTPS*
- ***no other***

] protocols to provide a communication channel between itself and another trusted IT product using certificates as defined in [*Functional Package for X.509, version 1.0*] 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.

5.2.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the MDF PP is claimed as the Base-PP.

5.2.2.1 Auditable Events for MDF PP Additional SFRs

Table 3: Auditable Events for MDF PP Additional SFRs

Requirement	Auditable Events	Additional Audit Record Contents

5.2.2.2 User Data Protection (FDP)

FDP_VPN_EXT.1 Split Tunnel Prevention

FDP_VPN_EXT.1.1

The TSF shall ensure that all IP traffic (other than IP traffic required to establish the VPN connection) flow through the IPsec VPN client.

Application Note: This requirement is implementation-dependent on the MDF PP being the Base-PP claimed by the TOE. In this case, this requirement must be claimed.

For all other Base-PPs, this requirement is strictly optional.

This requirement is used when the VPN client is able to enforce the requirement through its own components. This generally will have to be done through using hooks provided by the platform such that the TOE is able to ensure that no IP traffic can flow through other network interfaces.

Evaluation Activities

FDP_VPN_EXT.1.1
TSS
The evaluator shall verify that the TSS section of the ST describes the routing of IP traffic through processes on the TSF when a VPN client is enabled. The evaluator shall ensure that the description indicates which traffic does not go through the VPN and which traffic does and that a configuration exists for each baseband protocol in which only the traffic identified by the ST author is necessary for establishing the VPN connection (IKE traffic and perhaps HTTPS or DNS traffic) is not encapsulated by the VPN protocol (IPsec). The ST author shall also identify in the TSS section any differences in the routing of IP traffic when using any supported baseband protocols (e.g. Wi-Fi, LTE).

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

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

Tests
The evaluator shall perform the following test:

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

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

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

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

5.3 Protection Profile for Protection Profile for Application Software Security Functional Requirements Direction

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.

5.3.1 Modified SFRs

The SFRs listed in this section are defined in the App PP and relevant to the secure operation of the TOE.

5.3.1.1 Trusted Path/Channels

FCS_CKM.2: Cryptographic Key Establishment

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 group 20 in FCS_IPSEC_EXT.1.8. The selection for "no other schemes" was added in case the algorithms that IPsec requires are the TSF's only use of key establishment.

The text of the requirement is replaced with:

The **application** shall **[selection:**

- ***invoke platform-provided functionality***
- ***implement functionality***

] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **[Elliptic curve-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]**

[**selection:**

- ***[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"]***
- ***[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 [* ***selection:*** *RFC 3526, RFC 7919]*
- *Module-Lattice-Based Key-Encapsulation Mechanism Standard using the parameter set ML-KEM-1024 that meets the following: [FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard]*
- ***no other key establishment schemes***

].

FCS_CKM_EXT.1: Cryptographic Key Generation Services

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.

The text of the requirement is replaced with:

The application shall [**selection:**

- *invoke platform-provided functionality for asymmetric key generation*
- *implement asymmetric key generation*

].

FCS_COP.1/SKC: Cryptographic Operation - Encryption/Decryption

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 for consistency with the relevant IPsec claims (FCS_IPSEC_EXT.1.4 requires AES-GCM and FCS_IPSEC_EXT.1.6 requires AES-CBC). The "no other modes" selection is added for the case where no AES claims need to be made beyond what is mandated for IPsec.

The text of the requirement is replaced with:

The **application** shall **[selection: *perform, invoke the platform to perform*]** [*encryption and 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 [**selection:**

- *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 size of [*256-bits*].

FTP_DIT_EXT.1: Protection of Data in Transit

This SFR is identical to what is defined in the App PP except that the selection for IPsec is mandated, the ST author is forced to select the "encrypt all transmitted sensitive data" option, and the options for invoking platform-provided IPsec functionality have been removed. Since it is possible for a conformant TOE to implement IPsec while relying on the platform for some other protocol (e.g., using platform-provided TLS to obtain IPsec configuration from a gateway), the other platform-provided protocol selections remain. Additionally, since it is possible that a conformant TOE may not implement any encryption protocols other than IPsec, “no other protocols” is provided as a selectable option in the list of supported protocols.

The text of the requirement is replaced with:

The application shall [**selection:**

- *encrypt all transmitted [sensitive data] with **IPsec as defined in the PP-Module for VPN Client and** [**selection:***
  - *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 using mutual authentication in accordance with FCS_HTTPS_EXT.2*
  - *TLS as a server as defined in the Functional Package for TLS and also supports functionality for [**selection:** mutual authentication, none]*
  - *TLS as a client as defined in the Functional Package for TLS*
  - *DTLS as a server as defined in the Functional Package for TLS and also supports functionality for [**selection:** mutual authentication, none]*
  - *DTLS as a client as defined in the Functional Package for TLS*
  - *SSH as defined in the Functional Package for Secure Shell*
  - ***no other functions***

  *] for [**assignment:** function(s)] using certificates as defined in the Functional Package for X.509*
- *invoke platform-provided functionality to encrypt all transmitted sensitive data with [**selection:** HTTPS, TLS, DTLS, SSH] for [**assignment:** function(s)] using certificates as defined in the Functional Package for X.509*

] between itself and another trusted IT product.

5.3.2 Additional SFRs

This section defines additional SFRs that must be added to the TOE boundary in order to implement the functionality in any PP-Configuration where the App PP is claimed as the Base-PP.

5.3.2.1 Auditable Events for App PP Additional SFRs

Table 4: Auditable Events for App PP Additional SFRs

Requirement	Auditable Events	Additional Audit Record Contents

5.3.2.2 Cryptographic Support (FCS)

FCS_CKM.6 Cryptographic Key Destruction

FCS_CKM.6.1

The **[selection: *TOE* , *TOE platform*]** shall destroy [**assignment**: *list of cryptographic keys (including keying material)*] when [**selection**: *no longer needed* , *[**assignment**: assignment: other circumstances for key or keying material destruction]*] .

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [**assignment**: *cryptographic key destruction method*] that meets the following: [**assignment**: *list of standards*] .

Application Note: 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-Module, 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. The ST author should select "TOE platform" when native OS functionality is used to perform the key destruction.

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.

Evaluation Activities

FCS_CKM.6
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 keys that are not otherwise covered by the FCS_CKM.6 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 the keys 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 FCS_CKM.6:1: 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 #6 for instances of the known key value from #1.*

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

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

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1

The [**selection**: *VPN client* , *OS*] shall store persistent secrets and private keys when not in use in platform-provided key storage.

Application Note: 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.

Evaluation Activities

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the TOE or the TOE platform, the evaluator shall 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 shall confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator shall then perform 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 shall review the TSS 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.

5.4 Protection Profile for Protection Profile for Mobile Device Management Security Functional Requirements Direction

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.

5.4.1 Modified SFRs

The SFRs listed in this section are defined in the MDM PP and relevant to the secure operation of the TOE.

5.4.1.1 Trusted Path/Channels (FTP)

FCS_CKM.1: Cryptographic Key Generation

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 group 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. The selection for "no other key generation methods" was added in case the algorithms that IPsec requires are the TSF's only use of key generation.

The text of the requirement is replaced with:

The TSF shall **[selection: *invoke platform-provided functionality, implement functionality*]** to generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm

- **ECC schemes using "NIST curve" P-384 that meets the following: FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2**

[**selection:**

- *RSA schemes using cryptographic key sizes of 3072 bits that meet the following: [FIPS PUB 186-5, “Digital Signature Standard (DSS),” Appendix A.1]*
- *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 [**selection:** RFC 3526, RFC 7919]*
- ***No other key generation methods***

].

FCS_CKM.2: Cryptographic Key Establishment

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 group 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. The selection for "no other schemes" was added in case the algorithms that IPsec requires are the TSF's only use of key establishment.

The text of the requirement is replaced with:

The TSF shall **[selection: *invoke platform-provided functionality, implement functionality*]** to perform **cryptographic key establishment** in accordance with a specified cryptographic key establishment method:

- **[Elliptic curve-based key establishment schemes] that meet the following: [NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]**

[**selection:**

- *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 NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete*

Logarithm Cryptography”
- ***no other key establishment schemes***

].

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

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/INTER_XFER_IT 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. The "not invoke or implement any other protocol functionality" is added for the case where the TOE's implementation of IPsec is the only trusted channel protocol the TSF uses.

The text of FTP_ITC.1.1/INTER_XFER_IT is replaced with (the other elements are unaffected):

The TSF shall
- **implement functionality using IPsec as defined in the PP-Module for VPN Client, and**

[**selection:**
- ***invoke platform-provided functionality to use [selection:***
  - ***SSH***
  - ***mutually authenticated TLS***
  - ***mutually authenticated DTLS***
  - ***HTTPS***
- ***implement functionality using [selection:***
  - ***SSH as defined in the Functional 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***
- ***not invoke or implement any other protocol functionality***

] **to** provide a **trusted** communication channel between itself and **authorized** IT **entities supporting the following capabilities: audit server, [selection:** ***authentication server, [assignment: other capabilities]*** **]** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.

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

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/TRUSTPATH_REM_ADMIN 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. The "not invoke or implement any other protocol functionality" is added for the case where the TOE's implementation of IPsec is the only trusted path protocol the TSF uses.

The text of FTP_TRP.1.1/TRUSTPATH_REM_ADMIN is replaced with (the other elements are unaffected):

The TSF shall
- **implement functionality using IPsec as defined in the PP-Module for VPN Client, and**

[**selection:**
- ***invoke platform-provided functionality to use [selection:***
  - ***TLS***
  - ***HTTPS***
  - ***SSH***
- ***implement functionality using [selection:***
  - ***TLS as defined in the Package for Transport Layer Security***

- ***HTTPS in accordance with FCS_HTTPS_EXT.1***
- ***SSH as defined in the Functional Package for Secure Shell***

- ***not invoke or implement any other protocol functionality***

] **to** provide a **trusted** communication path between itself **as a [selection:** ***server, peer*** **] and another trusted IT product** that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from [*modification or disclosure*].

5.4.2 Additional SFRs

This PP-Module does not define any additional SFRs for any PP-Configuration where the MDM PP is claimed as the Base-PP.

5.5 TOE Security Functional Requirements

This PP-Module does not define any mandatory SFRs.

5.6 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 5: SFR Rationale

Threat	Addressed by	Rationale
T.TSF_CONFIGURATION	FIA_X509_EXT.4	This SFR mitigates the threat by providing the ability to verify the integrity of the TSF using X.509 certificates.
T.UNAUTHORIZED_ACCESS	FTP_ITC.1	This SFR mitigates the threat by defining the use of IPsec for protecting data in transit.
T.USER_DATA_REUSE	FCS_CKM_EXT.2	This SFR mitigates the threat by requiring the TOE to store sensitive data in the OS’ key storage.
	FCS_CKM_EXT.2	This SFR mitigates the threat by requiring the TOE or its platform to store sensitive data in the OS' key storage.
	FCS_CKM.6	This SFR mitigates the threat by requiring the TOE or its platform to zeroize key data when no longer needed.
	FDP_VPN_EXT.1	This SFR mitigates the threat by optionally requiring the TOE to prohibit split-tunneling so that network traffic cannot be transmitted outside of an established IPsec tunnel.

6 Consistency Rationale

6.1 Protection Profile for Protection Profile for General Purpose Operating System

6.1.1 Consistency of TOE Type

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.

6.1.2 Consistency of Security Problem Definition

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:

Table 6: Consistency of Security Problem Definition (GPOS PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_CONFIGURATION	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.
T.TSF_FAILURE	A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the GPOS PP.
T.UNAUTHORIZED_ACCESS	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.
T.USER_DATA_REUSE	Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the GPOS PP.
A.NO_TOE_BYPASS	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.
A.PHYSICAL	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.
A.TRUSTED_CONFIG	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.

6.1.3 Consistency of OE Objectives

Table 7: Consistency of OE Objectives (GPOS PP base)

PP-Module OE Objective	Consistency Rationale
OE.NO_TOE_BYPASS	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.
OE.PHYSICAL	This is part of satisfying OE.PLATFORM as defined in the GPOS PP because physical security is required for hardware to be considered 'trusted.'
OE.TRUSTED_CONFIG	The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the GPOS PP.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the GPOS PP that are needed to support VPN client functionality. This is considered to be consistent because the functionality provided by the GPOS PP is being used for its intended purpose. The PP-Module identifies new SFRs that are used entirely to provide functionality for VPN client. The rationale for why this does not conflict with the claims defined by the GPOS PP are as follows:

Table 8: Consistency of Requirements (GPOS PP base)

PP-Module

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FCS_CKM.1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FCS_CKM.2	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
Additional SFRs	
FCS_CKM_EXT.2	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.
FIA_X509_EXT.4	This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the GPOS PP.
FTP_ITC.1	This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing GPOS functions from being performed.
Mandatory SFRs	
This PP-Module does not define any Mandatory requirements.	
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent requirements.	
Selection-based SFRs	
This PP-Module does not define any Selection-based requirements.	

6.2 Protection Profile for Protection Profile for Mobile Device Fundamentals

6.2.1 Consistency of TOE Type

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 into the device's software so that additional security functionality is claimed within the scope of the TOE.

6.2.2 Consistency of Security Problem Definition

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:

Table 9: Consistency of Security Problem Definition (MDF PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_CONFIGURATION	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.
T.TSF_FAILURE	A failure of TSF functionality could compromise the local system, which is consistent with the T.FLAWAPP threat in the MDF PP.
T.UNAUTHORIZED_ACCESS	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.
T.USER_DATA_REUSE	Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.EAVESDROP threat in the MDF PP.
A.NO_TOE_BYPASS	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.
A.PHYSICAL	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.
A.TRUSTED_CONFIG	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.

6.2.3 Consistency of OE Objectives

Table 10: Consistency of OE Objectives (MDF PP base)

PP-Module OE Objective	Consistency Rationale
OE.NO_TOE_BYPASS	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.
OE.PHYSICAL	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.
OE.TRUSTED_CONFIG	The expectation of trusted configuration is consistent with OE.CONFIG in the MDF PP.

6.2.4 Consistency of Requirements

This PP-Module identifies several SFRs from the MDF PP that are needed to support VPN client functionality. This is considered to be consistent because the functionality provided by the MDF PP is being used for its intended purpose. The PP-Module identifies new SFRs that are used entirely to provide functionality for VPN client. The rationale for why this does not conflict with the claims defined by the MDF PP are as follows:

Table 11: Consistency of Requirements (MDF PP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FCS_CKM.1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FCS_CKM.2/UNLOCKED	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FDP_IFC_EXT.1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FTP_ITC_EXT.1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
Additional SFRs	
FDP_VPN_EXT.1	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.
Mandatory SFRs	
This PP-Module does not define any Mandatory requirements.	
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent requirements.	
Selection-based SFRs	

This PP-Module does not define any Selection-based requirements.

6.3 Protection Profile for Protection Profile for Application Software

6.3.1 Consistency of TOE Type

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.

6.3.2 Consistency of Security Problem Definition

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:

Table 12: Consistency of Security Problem Definition (App PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_CONFIGURATION	The threat of a misconfigured VPN client is consistent with the T.LOCAL_ATTACK threat in the App PP.
T.TSF_FAILURE	A failure of TSF functionality could compromise the local system, which is consistent with the T.LOCAL_ATTACK threat in the App PP.
T.UNAUTHORIZED_ACCESS	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.
T.USER_DATA_REUSE	Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the App PP.
A.NO_TOE_BYPASS	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.
A.PHYSICAL	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.
A.TRUSTED_CONFIG	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.

6.3.3 Consistency of OE Objectives

Table 13: Consistency of OE Objectives (App PP base)

PP-Module OE Objective	Consistency Rationale
OE.NO_TOE_BYPASS	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.
OE.PHYSICAL	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'.
OE.TRUSTED_CONFIG	The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the App PP.

6.3.4 Consistency of Requirements

This PP-Module identifies several SFRs from the App PP that are needed to support VPN client functionality. This is considered to be consistent because the functionality provided by the App PP is being used for its intended purpose. The PP-Module identifies new SFRs that are used entirely to provide functionality for VPN client. The rationale for why this does not conflict with the claims defined by the App PP are as follows:

Table 14: Consistency of Requirements (App PP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	

FCS_CKM.2	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.
FCS_CKM_EXT.1	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.
FCS_COP.1/SKC	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FTP_DIT_EXT.1	This PP-Module requires the existing selection of IPsec to be chosen to satisfy the dependency on this PP-Module
Additional SFRs	
FCS_CKM.6	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.
FCS_CKM_EXT.2	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.
Mandatory SFRs	
This PP-Module does not define any Mandatory requirements.	
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent requirements.	
Selection-based SFRs	
This PP-Module does not define any Selection-based requirements.	

6.4 Protection Profile for Protection Profile for Mobile Device Management

6.4.1 Consistency of TOE Type

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.

6.4.2 Consistency of Security Problem Definition

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:

Table 15: Consistency of Security Problem Definition (MDM PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.TSF_CONFIGURATION	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.
T.TSF_FAILURE	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.
T.UNAUTHORIZED_ACCESS	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.

T.USER_DATA_REUSE	Inadvertent disclosure of user data to an unauthorized recipient is consistent with the T.NETWORK_EAVESDROP threat in the MDM PP.
A.NO_TOE_BYPASS	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.
A.PHYSICAL	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.
A.TRUSTED_CONFIG	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.

6.4.3 Consistency of OE Objectives

Table 16: Consistency of OE Objectives (MDM PP base)

PP-Module OE Objective	Consistency Rationale
OE.NO_TOE_BYPASS	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.
OE.PHYSICAL	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.
OE.TRUSTED_CONFIG	The expectation of trusted configuration is consistent with OE.PROPER_USER and OE.PROPER_ADMIN in the MDM PP.

6.4.4 Consistency of Requirements

This PP-Module identifies several SFRs from the MDM PP that are needed to support VPN client functionality. This is considered to be consistent because the functionality provided by the MDM PP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the MDM PP are as follows:

Table 17: Consistency of Requirements (MDM PP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FCS_CKM.1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FCS_CKM.2	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
FTP_ITC.1/INTER_XFER_IT	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.
FTP_TRP.1/TRUSTPATH_REM_ADMIN	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.
Additional SFRs	
This PP-Module does not add any requirements when the MDM PP is the base.	
Mandatory SFRs	
This PP-Module does not define any Mandatory requirements.	
Optional SFRs	

Optional SFRs

This PP-Module does not define any Optional requirements.

Objective SFRs

This PP-Module does not define any Objective requirements.

Implementation-dependent SFRs

This PP-Module does not define any Implementation-dependent requirements.

Selection-based SFRs

This PP-Module does not define any Selection-based requirements.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

This PP-Module does not define any Strictly Optional SFRs or SARs.

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

This PP-Module does not define any Implementation-dependent SFRs.

Appendix B - Selection-based Requirements

This PP-Module does not define any Selection-based SFRs.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 18: Extended Component Definitions

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_CKM_EXT Cryptographic Key Management
Identification and Authentication (FIA)	FIA_X509_EXT X.509 Certificate Use and Management
User Data Protection (FDP)	FDP_VPN_EXT Subset Information Flow Control

C.2 Extended Component Definitions

C.2.1 Cryptographic Support (FCS)

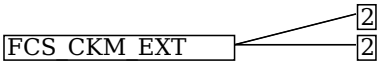
This PP-Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.1.1 FCS_CKM_EXT Cryptographic Key Management

Family Behavior

Components in this family describe requirements for key management functionality such as key storage and destruction.

Component Leveling



FCS_CKM_EXT.2, Cryptographic Key Storage, requires the TSF to securely store key data when not in use.

FCS_CKM_EXT.2, Cryptographic Key Storage, requires the TSF to securely store key data when not in use.

Management: FCS_CKM_EXT.2

No specific management functions are identified.

Audit: FCS_CKM_EXT.2

There are no auditable events foreseen.

FCS_CKM_EXT.2 Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies to: No dependencies.

FCS_CKM_EXT.2.1

The [**selection**: *VPN client* , *OS*] shall store persistent secrets and private keys when not in use in OS-provided key storage.

Management: FCS_CKM_EXT.2

No specific management functions are identified.

Audit: FCS_CKM_EXT.2

There are no auditable events foreseen.

FCS_CKM_EXT.2 Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies to: No dependencies.

FCS_CKM_EXT.2.1

The [**selection**: *VPN client , OS*] shall store persistent secrets and private keys when not in use in platform-provided key storage.

C.2.2 Identification and Authentication (FIA)

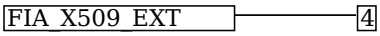
This PP-Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.2.1 FIA_X509_EXT X.509 Certificate Use and Management

Family Behavior

Components in this family describe the requirements that pertain to IP traffic and information flow through the VPN client.

Component Leveling



FIA_X509_EXT.4, X.509 Certificate Use and Management, 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.

Management: FIA_X509_EXT.4

No specific management functions are identified.

Audit: FIA_X509_EXT.4

There are no auditable events foreseen.

FIA_X509_EXT.4 X.509 Certificate Use and Management

Hierarchical to:	No other components.
Dependencies to:	FIA_X509_EXT.1 X.509 Certificate Validation
	FPT_TST_EXT.1 TSF Self-Test
	FPT_TUD_EXT.1 Trusted Update

FIA_X509_EXT.4.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec exchanges, and [**selection**: *digital signatures for FPT_TUD_EXT.1 , integrity checks for FPT_TST_EXT.1 , no additional uses*] .

FIA_X509_EXT.4.2

When a connection to determine the validity of a certificate cannot be established, the [**selection, choose one of**: *VPN client , OS*] shall [**selection, choose one of**: *allow the administrator to choose whether to accept the certificate in these cases , accept the certificate , not accept the certificate*] .

FIA_X509_EXT.4.3

The [**selection, choose one of**: *VPN client , OS*] shall not establish an SA if a certificate or certificate path is deemed invalid.

C.2.3 User Data Protection (FDP)

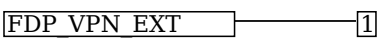
This PP-Module defines the following extended components as part of the FDP class originally defined by CC Part 2:

C.2.3.1 FDP_VPN_EXT Subset Information Flow Control

Family Behavior

Components in this family describe the requirements that pertain to IP traffic and information flow through the VPN client.

Component Leveling



FDP_VPN_EXT.1, Split Tunnel Prevention, requires the TSF to process all IP traffic through its VPN client functionality.

Management: FDP_VPN_EXT.1

No specific management functions are identified.

Audit: FDP_VPN_EXT.1

There are no auditable events foreseen.

FDP_VPN_EXT.1 Split Tunnel Prevention

Hierarchical to:	No other components.
Dependencies to:	FCS_IPSEC_EXT.1 IPsec

FDP_VPN_EXT.1.1

The TSF shall ensure that all IP traffic (other than IP traffic required to establish the VPN connection) flow through the IPsec VPN client.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Table 19 : Implicitly Satisfied Requirements

Requirement	Rationale for Satisfaction
FCS_CKM.2 – Cryptographic Key Distribution, or FCS_COP.1 – Cryptographic Operation	FCS_CKM.1 (which is defined in this PP-Module as FCS_CKM.1/VPN) requires one of FCS_CKM.2 or FCS_COP.1 to be claimed so that the generated keys can serve some security-relevant purpose. Each of the Base-PPs for this PP-Module define an iteration of FCS_COP.1 for symmetric cryptography that is expected to use the IKE keys generated by FCS_CKM.1/VPN. Therefore, this dependency is satisfied through requirements defined in the Base-PPs.
FCS_COP.1 – Cryptographic Operation	FCS_IPSEC_EXT.1 has a dependency on FCS_COP.1 because of the cryptographic operations that are needed in support of implementing the IPsec protocol. FCS_COP.1 is not defined in this PP-Module because each of the supported Base-PPs define iterations of FCS_COP.1 that support the functions that are relevant to IPsec.
FMT_MTD.1 – Management of TSF Data	FAU_SEL.1/VPN has a dependency on FMT_MTD.1 to enforce appropriate access controls on the audit configuration, as this is TSF data. This SFR is not explicitly defined in any of the supported Base-PPs but the dependency is implicitly addressed by each Base-PP in the following manner: • GPOS PP: The GPOS PP implicitly defines the existence of ‘user’ and ‘administrator’ roles in the extended SFRs FMT_MOF_EXT.1 and FMT_SMF_EXT.1. A TOE that conforms to this Base-PP can associate the ability to perform the functionality defined by FAU_SEL.1/VPN to one or both of these roles. • MDF PP: The MDF PP implicitly defines the existence of ‘user,’ ‘administrator,’ and ‘MDM’ roles in the SFRs FMT_MOF_EXT.1 and FMT_SMF.1. A TOE that conforms to this Base-PP can associate the ability to perform the functionality defined by FAU_SEL.1/VPN to one or more of these roles. • App PP: The App PP does not define the existence of a separately authenticated management interface; instead, the App PP assumes that authentication to the underlying OS platform is sufficient authorization to access the application’s management functionality. • MDM PP: The MDM PP defines the existence of management roles in FMT_SMR.1/SECMAN_ROLES. A TOE that conforms to this Base-PP can associate the ability to perform the functionality defined by FAU_SEL.1/VPN to one or more of the roles defined here.
FPT_STM.1 – Reliable Time Stamps	FAU_GEN.1/VPN has a dependency on FPT_STM.1 because audit data is required to have timestamps that are based on reliable clock data. All of the supported Base-PPs either define this requirement explicitly or provide rationale for why the reader should expect that a reliable clock service should be present. Depending on the claimed Base-PP, the dependency is satisfied in the following manner: • GPOS PP: The GPOS PP states that FPT_STM.1 is implicitly satisfied by the requirements of FAU_GEN.1 since that requirement could not be satisfied if no clock service was present. Additionally, a clock service is reasonably assumed to be provided by a general-purpose OS. • MDF PP: The MDF PP explicitly defines FPT_STM.1. • App PP: The App PP assumption A.PLATFORM assumes that the general-purpose computing platform on which the TOE is installed is ‘a trustworthy computing platform.’ System time data is not explicitly mentioned but a clock service is reasonably assumed to be provided by a general-purpose computer. • MDM PP: The MDM PP assumption A.MDM_SERVER_PLATFORM assumes that the platform on which the TOE is installed will provide reliable time services.
FPT_STM.1 – Reliable Time Stamps	FAU_GEN.1 has a dependency on FPT_STM.1. While not explicitly stated in the PP, it is assumed that this will be provided by the underlying hardware platform on which the TOE is installed. This is because the TOE is installed as a software or firmware product that runs on general-purpose computing hardware so a hardware clock is assumed to be available.

Appendix E - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PPs. As with other Base-PP requirements, the only additional requirement is that the entropy documentation also applies to the specific VPN client capabilities of the TOE in addition to the functionality required by the claimed Base-PP.

Appendix F - Acronyms

Table 20: Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
CRL	Certificate Revocation List
CSP	Critical Security Parameter
DH	Diffie-Hellman
DN	Distinguished Name
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
EP	Extended Package
ESP	Encapsulating Security Protocol
EUD	End-User Device
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
FP	Functional Package
FQDN	Fully Qualified Domain Name
IKE	Internet Key Exchange
IP	Internet Protocol
IT	Information Technology
MD	Mobile Device (MD)
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System (OS)
OSP	Organizational Security Policy
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
PUB	Publication
RBG	Random Bit Generation
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SD	Supporting Document

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPD	Security Policy Database
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
VPN	Virtual Private Network

Appendix G - Bibliography

Table 21: Bibliography

Identifier	Title
[App PP]	Protection Profile for Application Software, Version 2.0, June 16, 2025
[GPOS PP]	Protection Profile for General Purpose Operating Systems, Version 4.3 , September 27, 2022
[MDF PP]	Protection Profile for Mobile Device Fundamentals, Version 3.3 , Version 3.3, September 12, 2022
[MDM PP]	Protection Profile for Mobile Device Management, Version 4.0, April 25, 2019
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.