PP-Module for Virtual Private Network (VPN) Clients

Version: 2.4-Draft

2021-12-15

National Information Assurance Partnership

Revision History

Version	Date	Comment
2.4-draft	2021-12-15	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 Consistency Rationale

1.1 Protection Profile

1.1.1 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 operating system. The TOE boundary is simply extended to include VPN client functionality that is built into the operating system so that additional security functionality is claimed within the scope of the TOE.

1.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the PP as follows: 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:

PP-Module Threat	Consistency Rationale

1.1.3 Consistency of Objectives

The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the GPOS PP as follows: The objectives for the TOEs are consistent with the PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
	Consistency rationale for O.AUTHENTICATION.
	Consistency rationale for O.CRYPTOGRAPHIC_FUNCTIONS.
	Consistency rationale for O.KNOWN_STATE.
	This objective is consistent with the O.PROTECTED_STORAGE objective of the Base-PP, which ensures that sensitive data is not disclosed without authorization.

The objectives for the TOE's Operational Environment are consistent with the PP based on the following rationale:

PP-Module Operational Environment Objective	Consistency Rationale

1.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PP that are needed to support Virtual Private Network (VPN) Clients functionality. This is considered to be consistent because the functionality provided by the is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the PP as well as new SFRs that are used entirely to provide functionality for Virtual Private Network (VPN) Clients. The rationale for why this does not conflict with the claims defined by the PP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
OS-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.
OS-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.
OS-FCS-COP-1-1/1	The SFR is refined to list an additional AES mode that must be supported to address VPN client requirements; the use of this mode for VPN connectivity does not impact the ability of the OS to satisfy any of its other security requirements.
	Additional SFRs
OS-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 OS PP.

OS-FIA-X509-EXT-3	This SFR defines additional uses for X.509 certificate functionality that do not conflict with those defined in the OS PP.
OS-FTP-ITC-1	This SFR defines a trusted channel for IPsec, which is added functionality that does not prevent the existing OS functions from being performed.
Mandatory SFRs	
FCS-CKM-1-VPN/VPN	
FCS-IPSEC-EXT-1	
FDP-RIP-2	
FMT-SMF-1-VPN/VPN	
FPT-TST-EXT-1-VPN/VPN	
Optional SFRs	
FPF-MFA-EXT-1	
FIA-BMA-EXT-1	
Selection-based SFRs	
FIA-PSK-EXT-1	
FIA-PSK-EXT-2	
FIA-PSK-EXT-3	
FIA-PSK-EXT-4	
FIA-PSK-EXT-5	
FIA-HOTP-EXT-1	
FIA-TOTP-EXT-1	
FIA-EAP-EXT-1	
Objective SFRs	
FAU-GEN-1-VPN/VPN	
FAU-SEL-1-VPN/VPN	
FDP-IFC-EXT-1	

1.2 Protection Profile

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

1.2.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the PP as follows: 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:

PP-Module Threat	Consistency Rationale

1.2.3 Consistency of Objectives

The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDF PP as follows: The objectives for the TOEs are consistent with the PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
	Consistency rationale for O.AUTHENTICATION.
	Consistency rationale for O.CRYPTOGRAPHIC_FUNCTIONS.
	Consistency rationale for O.KNOWN_STATE.
	This objective is consistent with the O.PROTECTED_STORAGE objective of the Base-PP, which ensures that sensitive data is not disclosed without authorization.

The objectives for the TOE's Operational Environment are consistent with the PP based on the following rationale:

PP-Module Operational Environment Objective	Consistency Rationale

1.2.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PP that are needed to support Virtual Private Network (VPN) Clients functionality. This is considered to be consistent because the functionality provided by the is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the PP as well as new SFRs that are used entirely to provide functionality for Virtual Private Network (VPN) Clients. The rationale for why this does not conflict with the claims defined by the PP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
MD-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.
MD-FCS-CKM-2-1/UNLOCKED	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
MD-FCS-COP-1-1/ENCRYPT	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
MD-FDP-IFC-EXT-1-1	TODO: The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
MD-FIA-X509-EXT-2	This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used.
MD-FMT-SMF-EXT-1	This PP-Module modifies management function 45 regarding Always-on VPN protection.
MD-FTP-ITC-EXT-1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
	Additional SFRs
MD-FDP-IFC-EXT-1-ALL/ALL	
	Mandatory SFRs

FCS-CKM-1-VPN/VPN
FCS-IPSEC-EXT-1
FDP-RIP-2
FMT-SMF-1-VPN/VPN
FPT-TST-EXT-1-VPN/VPN
Optional SFRs
FPF-MFA-EXT-1
FIA-BMA-EXT-1
Selection-based SFRs
FIA-PSK-EXT-1
FIA-PSK-EXT-2
FIA-PSK-EXT-3
FIA-PSK-EXT-4
FIA-PSK-EXT-5
FIA-HOTP-EXT-1
FIA-TOTP-EXT-1
FIA-EAP-EXT-1
Objective SFRs
FAU-GEN-1-VPN/VPN
FAU-SEL-1-VPN/VPN
FDP-IFC-EXT-1

1.3 Protection Profile

1.3.1 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.

1.3.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the PP as follows: 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:

PP-Module Threat	Consistency Rationale

1.3.3 Consistency of Objectives

The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the App PP as follows: The objectives for the TOEs are consistent with the PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
	Consistency rationale for O.AUTHENTICATION.

	Consistency rationale for O.CRYPTOGRAPHIC_FUNCTIONS.
	Consistency rationale for O.KNOWN_STATE.
	This objective is consistent with the O.PROTECTED_STORAGE objective of the Base-PP, which ensures that sensitive data is not disclosed without authorization.

The objectives for the TOE's Operational Environment are consistent with the PP based on the following rationale:

PP-Module Operational Environment Objective	Consistency Rationale

1.3.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PP that are needed to support Virtual Private Network (VPN) Clients functionality. This is considered to be consistent because the functionality provided by the is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the PP as well as new SFRs that are used entirely to provide functionality for Virtual Private Network (VPN) Clients. The rationale for why this does not conflict with the claims defined by the PP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
AP-FCS-CKM-1-1/1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified. Additionally, this behavior is selection-based in the App PP but is made mandatory since it is required for VPN client functionality.
AP-FCS-CKM-2	The ST author is instructed to make specific selections at minimum to address VPN client requirements and is modified to include Diffie-Hellman Group 14 as an additional supported method for key establishment.
AP-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.
AP-FCS-COP-1-1/1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
AP-FIA-X509-EXT-2	This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used.
AP-FTP-DIT-EXT-1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
	Additional SFRs
AP-FCS-CKM-EXT-2	This PP-Module adds a requirement for key storage, which is new functionality when compared to the Base-PP but does not interfere with its existing security functions.
AP-FCS-CKM-EXT-4	This PP-Module adds a requirement for key destruction, which is new functionality when compared to the Base-PP but does not interfere with its existing security functions.
	Mandatory SFRs
FCS-CKM-1-VPN/VPN	
FCS-IPSEC-EXT-1	
FDP-RIP-2	
FMT-SMF-1-VPN/VPN	
FPT-TST-EXT-1-VPN/VPN	

Optional SFRs
FPF-MFA-EXT-1
FIA-BMA-EXT-1
Selection-based SFRs
FIA-PSK-EXT-1
FIA-PSK-EXT-2
FIA-PSK-EXT-3
FIA-PSK-EXT-4
FIA-PSK-EXT-5
FIA-HOTP-EXT-1
FIA-TOTP-EXT-1
FIA-EAP-EXT-1
Objective SFRs
FAU-GEN-1-VPN/VPN
FAU-SEL-1-VPN/VPN
FDP-IFC-EXT-1

1.4 Protection Profile

1.4.1 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.

1.4.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the PP as follows: 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:

PP-Module Threat	Consistency Rationale

1.4.3 Consistency of Objectives

The security objectives defined by this PP-Module (see sections 4.1 and 4.2) supplement those defined in the MDM PP as follows: The objectives for the TOEs are consistent with the PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
	Consistency rationale for O.AUTHENTICATION.

	Consistency rationale for O.CRYPTOGRAPHIC_FUNCTIONS.
	Consistency rationale for O.KNOWN_STATE.
	This objective is consistent with the O.PROTECTED_STORAGE objective of the Base-PP, which ensures that sensitive data is not disclosed without authorization.

The objectives for the TOE's Operational Environment are consistent with the PP based on the following rationale:

PP-Module Operational Environment Objective	Consistency Rationale

1.4.4 Consistency of Requirements

This PP-Module identifies several SFRs from the PP that are needed to support Virtual Private Network (VPN) Clients functionality. This is considered to be consistent because the functionality provided by the is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the PP as well as new SFRs that are used entirely to provide functionality for Virtual Private Network (VPN) Clients. The rationale for why this does not conflict with the claims defined by the PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
DM-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.
DM-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.
DM-FCS-COP-1-1/1	The ST author is instructed to make specific selections at minimum to address VPN client requirements; the SFR behavior itself is unmodified.
DM-FIA-X509-EXT-2	This PP-Module adds IPsec as a new trusted protocol where x.509 certificate authentication is used.
DM-FTP-ITT-1-1/1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
DM-FTP-ITC-1-1/1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
DM-FTP-TRP-1-1/1	This PP-Module adds IPsec as a new protocol that is used to implement trusted channels.
Mandatory SFRs	
FCS-CKM-1-VPN/VPN	
FCS-IPSEC-EXT-1	
FDP-RIP-2	
FMT-SMF-1-VPN/VPN	
FPT-TST-EXT-1-VPN/VPN	
Optional SFRs	
FPF-MFA-EXT-1	
FIA-BMA-EXT-1	
Selection-based SFRs	
FIA-PSK-EXT-1	
FIA-PSK-EXT-2	
FIA-PSK-EXT-3	

FIA-PSK-EXT-4	
FIA-PSK-EXT-5	
FIA-HOTP-EXT-1	
FIA-TOTP-EXT-1	
FIA-EAP-EXT-1	
Objective SFRs	
FAU-GEN-1-VPN/VPN	
FAU-SEL-1-VPN/VPN	
FDP-IFC-EXT-1	

Appendix A - Optional SFRs

FPF-MFA-EXT-1 Multifactor Authentication Filtering

FPF-MFA-EXT-1.1

The TSF shall not forward packets to the internal network until the IKE/IPsec tunnel has been established, except those necessary to authenticate the client is authenticated according to FIA_PSK_EXT.1.

Application Note: If FPF_MFA_EXT.1 is included FIA_PSK_EXT.1 shall be included.

FIA-BMA-EXT-1 Biometric Activation

FIA-BMA-EXT-1.1

The TSF shall leverage the platform biometric features to confirm the user before initiating a trusted channel.

Application Note: In this context the platform refers to the OS or device and may be part of the TOE if those base PPs are leveraged.

Appendix B - Selection-based SFRs

FIA-PSK-EXT-1 Pre-Shared Key Composition

FIA-PSK-EXT-1.1

The TSF shall be able to use pre-shared keys for IPsec and [**selection**: *[**assignment**: other protocols that use pre-shared keys], no other protocols*].

FIA-PSK-EXT-1.2

The TSF shall be able to accept the following as pre-shared keys: [**selection**: *Generated bit-based*, *Password based*, *HMAC based one time password*, *Time based one time password*, *Combination of a generated bit-based and HMAC based one time password*, *Combination of a generated bit-based and time based one time password*, *Combination of a password based and HMAC based one time password*, *Combination of a password based and time based one time password*] keys.

Application Note: If any selection including Generated bit-based keys is selected then FIA_PSK_EXT.2 shall be included. If any selection including Password based keys is selected then FIA_PSK_EXT.3 shall be included.

If any selection including HMAC based one time password keys is selected then FIA_PSK_EXT.4 shall be included.

If any selection including time based one time password is selected then FIA_PSK_EXT.5 shall be included.

This requirement is selection dependent on FCS_IPSEC_EXT.1.11.

FIA-PSK-EXT-2 Generated Pre-Shared Keys

FIA-PSK-EXT-2.1

The TSF shall be able to [**selection**:

- *accept externally generated*,
- *generate [**selection**: 128, 256] bit-based pre-shared keys via FCS_RBG_EXT.1.*

]

Application Note: Generated PSKs are expected to be shared between components via an out of band mechanism. This requirement is selection dependent on FIA_PSK_EXT.1.

FIA-PSK-EXT-3 Password Based Pre-Shared Keys

FIA-PSK-EXT-3.1

The TSF shall support a PSK of up to [**assignment**: *positive integer of 64 or more*] characters.

FIA-PSK-EXT-3.2

The TSF shall allow PSKs to be composed of any combination of upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [**selection**: *[**assignment**: other supported special characters], no other characters*]

FIA-PSK-EXT-3.3

The TSF shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC- [**selection**: *SHA-256*, *SHA-384*, *SHA-512*], with [**assignment**: *positive integer of 4096 or more*] iterations], and output cryptographic key sizes [**selection**: *128*, *256*] that meet the following: [NIST SP 800-132].

FIA-PSK-EXT-3.4

The TSF shall not accept PSKs less than [**selection**: *a value settable by the administrator*, *[**assignment**: minimum PSK length accepted by the TOE, must be >= 6]*] and greater than the maximum PSK length defined in FIA_PSK_EXT.3.1.

FIA-PSK-EXT-3.5

The TSF shall generate all salts using an RBG that meets FCS_RBG_EXT.1 and with entropy corresponding to the key size selected for PBKDF in FIA_PSK_EXT.3.3.

FIA-PSK-EXT-3.6

The TSF shall require the PSK to be entered before every initiated connection.

FIA-PSK-EXT-3.7

The TSF shall [**selection**: *provide a password strength meter*, *check the password against a blacklist*, *perform no action to assist the user in choosing a strong password*].

Application Note: For FIA_PSK_EXT.3.1, the ST author assigns the maximum size of the PSK it supports; it must support at least 64 characters or a length defined by the platform.

For FIA_PSK_EXT.3.2, the ST author assigns any other supported characters; if there are no other supported characters, they should select "no other characters".

For FIA_PSK_EXT.3.3, the ST author selects the parameters based on the PBKDF used by the TSF.

For FIA_PSK_EXT.3.4 If the minimum length is settable, then ST author chooses "a value settable by the administrator". If the minimum length is not settable, the ST author fills in the assignment with the minimum length the PSK must be. This requirement is to ensure bounds work properly.

For FIA_PSK_EXT.3.7, the ST author may select one, both, or neither of the functions in alignment with NIST SP800-63b.

This requirement is selection dependent on FIA_PSK_EXT.1.

FIA-PSK-EXT-4 HMAC Based One Time Password Pre-shared Keys Support

FIA-PSK-EXT-4.1

The TSF shall accept and send a HOTP while initiating a VPN connection.

FIA-PSK-EXT-4.2

The TSF shall [**selection**: *verify the HOTP*, *verify the HOTP via an external authentication server*] before establishing an incoming connection.

Application Note: If verify the HOTP is selected then FIA_HOTP_EXT.1 must be included. This requirement is selection dependent on FIA_PSK_EXT.1

FIA-PSK-EXT-5 Time Based One Time Password Pre-shared Keys Support

FIA-PSK-EXT-5.1

The TSF shall accept and send a TOTP while initiating a VPN connection.

FIA-PSK-EXT-5.2

The TSF shall [**selection**: *verify the TOTP*, *verify the TOTP via an external authentication server*] before establishing an incoming connection.

Application Note: If verify the TOTP is selected then FIA_TOTP_EXT.1 must be included. This requirement is dependent on FIA_PSK_EXT.1.

FIA-HOTP-EXT-1 HMAC-Based One-Time Password Pre-Shared Keys

FIA-HOTP-EXT-1.1

The TSF shall support HMAC-Based One-Time Password authentication (HOTP) in accordance with RFC 4226 to authenticate the user before establishing VPN connection.

FIA-HOTP-EXT-1.2

The TSF shall generate a HOTP seed according to FCS_RBG_EXT.1 of [**selection**: *128*, *256*] bits.

FIA-HOTP-EXT-1.3

The TSF shall generate a new HOTP seed value for each client.

FIA-HOTP-EXT-1.4

The TSF shall utilize [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive a HOTP hash from the HOTP seed and counter.

FIA-HOTP-EXT-1.5

The TSF shall truncate the HOTP hash per FIA_HOTP_EXT.1.4 to create a HOTP of [**selection**:

- *administrator configurable chracter length of at least 6*,
- *preset character length of [**selection**: 6, 7, 8, 9, 10]*

].

FIA-HOTP-EXT-1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*,
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA-HOTP-EXT-1.7

The TSF shall not verify HOTP attempts outside of the counter look ahead window of [**selection**: *a configurable value*, *[**assignment**: a value less than or equal to 3]*] for resynchronization.

FIA-HOTP-EXT-1.8

The TSF shall increment the counter after each successful authentation.

Application Note: The selection FIA_HOTP_EXT.1.4 must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash message authentication. In FIA_HOTP_EXT.1.5 the ST author may either provide a configurable character length of at least 6 or a preset size between 6 and 10.

In FIA_HOTP_EXT.1.6 the ST may select throttle requests, account lockout, or both.

The HOTP seed and all derived values are considered secret keys for purposes of protection.

This requirement is selection dependent on FCS_PSK_EXT.4 or FPF_MFA_EXT.1

FIA-TOTP-EXT-1 Time-Based One-Time Password Pre-Shared Keys

FIA-TOTP-EXT-1.1

The TSF shall support Time-Based One-Time Password authentication in accordance with RFC 6238 to authenticate the user before establishing VPN connection.

FIA-TOTP-EXT-1.2

The TSF shall generate a TOTP seed according to FCS_RBG_EXT.1 of [**selection**: *128*, *256*] bits.

FIA-TOTP-EXT-1.3

The TSF shall generate a new TOTP seed for each client.

FIA-TOTP-EXT-1.4

The TSF shall utilize [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive a TOTP hash from the TOTP seed and current time provided by NTP.

FIA-TOTP-EXT-1.5

The TSF shall truncate the TOTP hash per FIA_TOTP_EXT.1.4 to create a TOTP of [**selection**:

- *administrator configurable character length of at least 6*,
- *preset character length of [**selection**: 6, 7, 8, 9, 10]*

]

FIA-TOTP-EXT-1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*,
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA-TOTP-EXT-1.7

The TSF shall set a time-step size of [**selection**: *a configurable value*, *[**assignment**: a value less than or equal to 30]*] seconds.

FIA-TOTP-EXT-1.8

The TSF shall not validate a drift of more than [**selection**: *a configurable value*, *[**assignment**: a value less than or equal to 3]*] time-steps.

FIA-TOTP-EXT-1.9

The TSF shall [**selection**: *allow resynchronization by recording time drift within the limit of FIA_TOTP_EXT.2.8*, *not permit resynchronization*].

Application Note: The selection FIA_TOTP_EXT.1.4 must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash message authentication. In FIA_TOTP_EXT.1.5 the ST author may either provide a configurable character length of at least 6 or a preset size between 6 and 10.

In FIA_TOTP_EXT.1.6 the ST may select throttle requests, account lockout, or both.

The TOTP seed and all derived values are considered secret keys for purposes of protection.

This requirement is selection dependent on FCS_PSK_EXT.5 or FPF_MFA_EXT.1.

FIA-EAP-EXT-1 EAP-TLS

FIA-EAP-EXT-1.1

The TSF shall implement [**selection**: *EAP-TLS protocol as specified in RFC 5216*, *EAP-TTLS as specified in RFC 5881*] as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with the TLS functional package.

FIA-EAP-EXT-1.2

The TSF shall generate random values used in the [**selection**: *EAP-TLS*, *EAP-TTLS*] exchange using the RBGspecified in FCS_RBG_EXT.1.

FIA-EAP-EXT-1.3

The TSF shall support peer authentication using certificates and [**selection**: *PSK*, *HOTP*, *TOTP*, *[**assignment**: other Authentication-verification protocols]*, *no other authentication*>] as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with the TLS functional package.

FIA-EAP-EXT-1.4

The TSF shall not forward a EAP-success response if the client certificate is not valid according to FIA_X509_EXT.1.

Appendix C - Objective SFRs

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

FAU-GEN-1-VPN/VPN Audit Data Generation

This is an objective component.

FAU-GEN-1-VPN.1/VPN

The TSF **and [selection: *TOE platform, no other component*]** shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit;
c. All administrative actions;
d. [*Specifically defined auditable events listed in* ***the Auditable Events tables***].

Application Note: In the case of "a", the audit functions referred to are those provided by the TOE. For example, in the case that the TOE was a stand-alone executable, auditing the startup and the shutdown of the TOE itself would be sufficient to meet the requirements of this clause.

Many auditable aspects of the SFRs included in this document deal with administrative actions. Item c above requires all administrative actions to be auditable, so no additional specification of the auditability of these actions is present in the Auditable Events table. While the TOE itself does not need to provide the ability to perform I&A for an administrator, this requirement implies that the TOE possess the capability to audit the events described by the Base-PP as "administrative actions" (primarily dealing with configuration of the functionality provided by the TOE).

The auditable events defined in the Auditable Events table are for the SFRs that are explicitly defined in this PP-Module. For any SFRs that are included as part of the TOE based on the claimed Base-PP, it is expected that any applicable auditable events defined for those SFRs in the Base-PP are also claimed as part of the TSF. These auditable events only apply if the client actually performs these functions. If the platform performs any of these actions, then the platform is responsible for performing the auditing, not the TSF

FAU-GEN-1-VPN.2/VPN

The TSF **and [selection: *TOE platform, no other component*]** shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, [*information specified in column three of Auditable Events table*].

FAU-SEL-1-VPN/VPN Selective Audit

This is an objective component.

FAU-SEL-1-VPN.1/VPN

The **[selection: *TSF, TOE platform*]** shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: [*event type, [success of auditable security events, failure of auditable security events], [****assignment****: list of additional attributes that audit selectivity is based upon]*].

Application Note: The intent of this requirement is to identify all criteria that can be selected to trigger an audit event. This can be configured through an interface on the client for a user/administrator to invoke, or it could be an interface that the VPN gateway uses to instruct the client on which events are to be audited. For the ST author, the assignment is used to list any additional criteria or “none”. The auditable event types are listed in the Auditable Events table

The intent of the first selection is to allow for the case where the underlying platform is responsible for some audit log generation functionality.

FDP-IFC-EXT-1 Subset Information Flow Control

This is an objective component.

FDP-IFC-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 mandatory when the MDF is the base PP (see FDP_IFC_EXT.1/ALL). Otherwise it is 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.

Appendix D - Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

D.1 Background and Scope

This appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Functional Class	Functional Components

D.2 Extended Component Definitions

FCS_CKM_EXT Cryptographic Key Management

Family Behavior

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

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.

FCS_IPSEC_EXT IPsec

Family Behavior

Components in this family describe requirements for IPsec implementation.

FPT_TST_EXT TSF Self-Test

Family Behavior

Components in this family describe requirements for self-test to verify functionality and integrity of the TOE.

FPF_MFA_EXT Multifactor Authentication Filtering

Family Behavior

Components in this family describe the requirements for multifactor authentication filtering when utilizing the VPN client.

FIA_BMA_EXT Biometric Activation

Family Behavior

Components in this family describes the requirements for biometrics when utilizing the VPN client.

FIA_PSK_EXT Pre-Shared Key Composition

Family Behavior

Components in this family describes the requirements for pre-shared keys when implementing IPsec

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

Family Behavior

Components in this family define requirements the use of HMAC-Based One-Time password authentication, including generation methods and usage restrictions.

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

Family Behavior

Components in this family define requirements the use of Time-Based One-Time password authentication, including generation methods and usage restrictions.

FCS_EAP_EXT EAP-TLS

Family Behavior

Components in this family describe the requirements for EAP-TLS.

FDP_IFC_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.

Appendix E - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this Protection Profile. However, 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, **8.2 Dependencies between components**.

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

Table 1: 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 PPModule 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_CKM.4 – Cryptographic Key Destruction	FCS_CKM.1 (which is defined in this PP-Module as FCS_CKM.1/VPN) requires FCS_CKM.4 to be claimed so that the generated keys are not disclosed through improper or nonexistent key destruction methods. Each of the supported Base-PPs except for the App PP define FCS_CKM_EXT.4 as an extended SFR, which defines key destruction functionality consistent with FCS_CKM.4, but with additional details that are specific to the respective technology types of the Base-PP. When the App PP is the Base-PP, this PP-Module defines its own instance of FCS_CKM_EXT.4 to achieve the same purpose. The dependency on FCS_CKM.4 is considered to be satisfied through the fact that a compliant TOE will always claim FCS_CKM_EXT.4, which is intended to satisfy the same purpose.
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 BasePP can associate the ability to perform the functionality defined by FAU_SEL.1/VPN to one or both of these roles. • MDF PP: The GPOS PP implicitly defines the existence of ‘user,’ ‘administrator,’ and ‘MDM’ roles in the extended SFRs FMT_MOF_EXT.1 and FMT_SMF_EXT.1. A TOE that conforms to this BasePP 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(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 the roles defined here.
FPT_STM.1 – Reliable Time Stamps	FAU_GEN.1/VPN has a dependency on FPT_STM.1 because audit records are 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 to expect that a reliable clock service is expected to 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 generalpurpose 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.
FPT_STM.1 – Reliable Time Stamps	FIA_X509_EXT.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 F - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) 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 G - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.
[OS PP]	Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 2019
[MD PP]	Protection Profile for Mobile Device Fundamentals, Version 3.1, June 2017
[MDM PP]	Protection Profile for Mobile Device Management (This needs to be updated) , Version 3.1, June 2017
[App PP]	Protection Profile for Application Software, Version 1.4, October 2021
[SD]	Supporting Document Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, November 2019

Appendix H - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
CC	Common Criteria
CEM	Common Evaluation Methodology
CRL	Certificate Revocation List
CSP	Critical Security Parameter
DH	Diffie-Hellman
DN	Distinguished Name
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Protocol
EUD	End-User Device
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IT	Information Technology
MD	Mobile Device (Fundamentals)
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OS	(General Purpose) Operating System
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
PP	Protection Profile
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
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VPN	Virtual Private Network