

# **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	
1.1.2	Consistency of Security Problem Definition	
1.1.3	Consistency of Objectives	
1.1.4	Consistency of Requirements	
1.2	Protection Profile	
1.2.1	Consistency of TOE Type	
1.2.2	Consistency of Security Problem Definition	
1.2.3	Consistency of Objectives	
1.2.4	Consistency of Requirements	
1.3	Protection Profile	
1.3.1	Consistency of TOE Type	
1.3.2	Consistency of Security Problem Definition	
1.3.3	Consistency of Objectives	
1.3.4	Consistency of Requirements	
1.4	Protection Profile	
1.4.1	Consistency of TOE Type	
1.4.2	Consistency of Security Problem Definition	
1.4.3	Consistency of Objectives	
1.4.4	Consistency of Requirements	
Appendix A -	Optional SFRs	
Appendix B -	Selection-based SFRs	
Appendix C -	Objective SFRs	
Appendix D -	Extended Component Definitions	
D.1	Background and Scope	
D.2	Extended Component Definitions	
Appendix E -	Implicitly Satisfied Requirements	
Appendix F -	Entropy Documentation and Assessment	
Appendix G -	Bibliography	
Appendix H -	Acronyms	

# 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.
<b>Mandatory SFRs</b>	
FCS-CKM-1-VPN/VPN	
FCS-IPSEC-EXT-1	
FDP-RIP-2	
FMT-SMF-1-VPN/VPN	
FPT-TST-EXT-1-VPN/VPN	
<b>Optional SFRs</b>	
FPF-MFA-EXT-1	
FIA-BMA-EXT-1	
<b>Selection-based SFRs</b>	
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	
<b>Objective SFRs</b>	
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
<b>Optional SFRs</b>
FPF-MFA-EXT-1
FIA-BMA-EXT-1
<b>Selection-based SFRs</b>
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
<b>Objective SFRs</b>
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:

<b>PP-Module Requirement</b>	<b>Consistency Rationale</b>
<b>Modified SFRs</b>	
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.
<b>Additional SFRs</b>	
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.
<b>Mandatory SFRs</b>	
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.

### Evaluation Activity ▼

**TSS**

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

**Guidance**

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

**Tests**

- **Test 1:** *For each included selection the evaluator shall configure the TOE per the operational guidance. The evaluator shall attempt to connect and verify other traffic is rejected per the filtering rules. The evaluator shall then provide the selected factor and confirm it is accepted and traffic is no longer blocked.*

## 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.

### Evaluation Activity ▼

**TSS**

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

**Guidance**

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

**Tests**

- **Test 1:** *The evaluator shall initiate a connection and verify that a biometric prompt is presented and accepted before the connection can proceed. The evaluator shall also verify the connection does not proceed if the biometric is not presented or accepted.*

# 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.

### Evaluation Activity ▼

#### **TSS**

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

#### **Guidance**

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

#### **Tests**

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

- **Test 1:** *For each mechanism selected in FIA\_PSK\_EXT.1.2 the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection.*

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

FIA-PSK-EXT-2.1

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.

### Evaluation Activity ▼

#### **TSS**

*If generated is selected the evaluator shall confirm that this process uses the RBG specified in FCS\_RBG\_EXT.1 and the output matches the size selected in FIA\_PSK\_EXT.2.1.*

### **Guidance**

*The evaluator shall confirm the operational guidance contains instructions for entering generated pre-shared keys for each protocol identified in the FIA\_PSK\_EXT.1.1.*

### **Tests**

- **Test 1:** [conditional] *If generate was selected the evaluator shall generate a pre-shared key and confirm the output matches the size selected in FIA\_PSK\_EXT.2.1.*

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

FIA-PSK-EXT-3.1

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  $\geq 6$ ]] 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.

### **Evaluation Activity ▼**

#### **TSS**

*The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys used. If generated is selected the evaluator shall confirm that this process uses the RBG specified in*

#### *FCS\_RBG\_EXT.1.*

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

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

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

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

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

*The evaluator shall confirm that the minimum length is described.*

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

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

#### **Guidance**

*The evaluator shall confirm the operational guidance contains instructions for entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall confirm that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.*

*The guidance must specify the allowable characters for pre-shared keys, and that list must include, at minimum, the same items contained in FIA\_PSK\_EXT.3.2.*

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

#### **Tests**

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

- **Test 1:** *The evaluator shall compose a pre-shared key of at least 64 characters that contains a combination of the allowed characters in accordance with the FIA\_PSK\_EXT.1.3 and verify that a successful protocol negotiation can be performed with the key.*
- **Test 2:** *[conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length and invalid lengths that are below the minimum length, above the maximum length, null length, empty length, or zero length. The minimum test should be successful, and the invalid lengths must be rejected by the TOE.*
- **Test 3:** *[conditional]: If the TOE initiates connections, initiate and establish a remote connection, disconnect from the connection, verify that the PSK is required when initiating the connection a second time.*
- **Test 4:** *[conditional]: If the TOE supports a password meter, the evaluator shall enter a password and verify the password checker responds per the description in the TSS.*
- **Test 5:** *[conditional]: If the TOE supports a password blacklist, the evaluator shall enter a blacklisted password and verify that the password is rejected or flagged as such.*

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

FIA-PSK-EXT-4.1

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

### Evaluation Activity ▼

#### **TSS**

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

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

#### **Guidance**

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

#### **Tests**

- **Test 1:** *The evaluator shall configure the TOE to use a supported HOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the HOTP before initiating the connection. The evaluator shall verify the server validates the HOTP or receives confirmation from an authentication server before establishing the channel.*

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

FIA-PSK-EXT-5.1

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.

### Evaluation Activity ▼

#### **TSS**

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

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

#### **Guidance**

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

#### **Tests**

- **Test 1:** *The evaluator shall configure the TOE to use a supported TOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the TOTP before initiating the connection. The evaluator shall verify the server validates the TOTP or receives confirmation from an authentication server before establishing the channel.*

## FIA-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 authentication.

**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

### Evaluation Activity ▼

#### **TSS**

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

*The evaluator shall confirm the TSS describes how the HOTP seed is generated and ensure it aligns with FCS\_RBG\_EXT.1*

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

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

*The evaluator shall confirm the TSS describes how the HOTP seed is conditioned into a HOTP hash and verify it matches the selection in FIA\_HOTP\_EXT.1.4.*

*The evaluator shall confirm the TSS describes how the HOTP hash is truncated and verify it matches the selection in FIA\_HOTP\_EXT.1.5.*

*The evaluator shall confirm the TSS describes how the TOE handles multiple*



incoming invalid requests and verify it provides anti-hammer mechanism that match the selections FIA\_HOTP\_EXT.1.6.

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

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

#### **Guidance**

The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA\_HOTP\_EXT.1 requirements.

#### **Tests**

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

- **Test 1:** Attempt to establish a connection using a factor from a different client, the test passes if the client fails to connect.
- **Test 2:** Attempt multiple connections outside the boundary set in FIA\_HOTP\_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 3:** Attempt to use a HOTP that is outside of the value allowed with for resynchronization. The test passes if the client fails to connect.
- **Test 4:** Attempt to connect with a valid HOTP, disconnect and attempt to authenticate again with the same HOTP value. The test passes if the client connects the first time and fails to connect the second time. If the HOTP generated is duplicated the test may be repeated.

### **FIA-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.

## Evaluation Activity ▼

### **TSS**

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

*The evaluator shall confirm the TSS describes how the TOTP seed is generated and ensure it aligns with FCS\_RBG\_EXT.1*

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

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

*The evaluator shall confirm the TSS describes how the TOTP seed is conditioned into a TOTP hash and verify it matches the selection in FIA\_TOTP\_EXT.1.4.*

*The evaluator shall confirm the TSS describes how the TOTP hash is truncated and verify it matches the selection in FIA\_TOTP\_EXT.1.5.*

*The evaluator shall confirm the TSS describes how the TOE handles multiple incoming requests and verify it provides anti-hammer mechanism that matches the selections FIA\_TOTP\_EXT.2.6.*

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

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

### **Guidance**

*The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA\_TOTP\_EXT.1 requirements.*

### **Tests**

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

- **Test 1:** Attempt to establish a connection using a factor from a different client, the test passes if the client fails to connect.
- **Test 2:** Attempt multiple connections outside the boundary set in FIA\_TOTP\_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 3:** Attempt to use a TOTP that is outside of the value allowed with for resynchronization. The test passes if the client fails to connect. Attempt to connect with a valid TOTP, disconnect and attempt to authenticate again with the same TOTP. The test passes if the client connects the first time and fails to connect the second time. If the TOTP generated is duplicated the test may be repeated.

## **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 RBGs specified 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.

#### Evaluation Activity ▼

##### **TSS**

*TSS TBD after public review of SRFs.*

##### **Guidance**

*Guidance TBD after public review of SRFs.*

##### **Tests**

*Tests TBD after public review of SRFs.*

# 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 audibility 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].

## Evaluation Activity ▼

### TSS

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

### Guidance

*The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the VPN Client PP-Module is described and that the description of the fields contains the information required in FAU\_GEN.1.2/VPN, and the additional information specified in the Auditable Events table of the VPN Client PP-PP-Module.*

*In particular, the evaluator shall ensure that the operational guidance is*

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

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

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

#### **Tests**

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the EAs associated with the functional requirements in the VPN Client PP-Module. Additionally, the evaluator shall test that each administrative action applicable in the context of the VPN Client PP-Module is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD\_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

### **FAU-SEL-1-VPN/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.

**Evaluation Activity** ▼

### **TSS**

*There are no TSS EAs for this SFR.*

### **Guidance**

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

### **Tests**

*The evaluator shall perform the following tests:*

- **Test 1:** *For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.*
- **Test 2:** *[conditional] If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.*

## **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.

### **Evaluation Activity ▼**

### **TSS**

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

### **Guidance**

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

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

### **Tests**

*The evaluator shall perform the following test:*

*Step 1 - The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an Internet-connected network. The evaluator shall turn on*

*the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other Internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data.*

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

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

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

# 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
<b>FCS_CKM.2 - Cryptographic Key Distribution, or FCS_COP.1 - Cryptographic Operation</b>	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.
<b>FCS_CKM.4 - Cryptographic Key Destruction</b>	<p>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.</p> <p>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.</p>
<b>FCS_COP.1 - Cryptographic Operation</b>	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.
<b>FMT_MTD.1 - Management of TSF Data</b>	<p>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:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• 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.</li><li>• 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.</li></ul>
<b>FPT_STM.1 - Reliable Time Stamps</b>	<p>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:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• MDF PP: The MDF PP explicitly defines FPT_STM.1.</li></ul>

- 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 - <ul style="list-style-type: none"><li>• <a href="#">Part 1: Introduction and General Model</a>, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.</li><li>• <a href="#">Part 2: Security Functional Components</a>, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017.</li><li>• <a href="#">Part 3: Security Assurance Components</a>, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.</li></ul>
[OS PP]	<a href="#">Protection Profile for General Purpose Operating Systems</a> , Version 4.2.1, April 2019
[MD PP]	<a href="#">Protection Profile for Mobile Device Fundamentals</a> , Version 3.1, June 2017
[MDM PP]	<a href="#">Protection Profile for Mobile Device Management (This needs to be updated)</a> , Version 3.1, June 2017
[App PP]	<a href="#">Protection Profile for Application Software</a> , 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