Supporting Document
Mandatory Technical Document

PP-Module for VPN Client
Version: 2.6
2025-01-31
National Information Assurance Partnership

Foreword

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

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

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
2.6	2025-01-31	CC:2022 conversion, limitation of cryptographic algorithms to CNSA 1.0, incorporation of TDs
2.5	2024-06-24	Incorporation of TC feedback: Incorporation of TDs: 0662, 0672, 0690, 0697, 0711, 0725, 0753, 0788Corrections to Base-PP referencesDefinition of auditable events for Additional SFRsExplicit association of evaluation activities with components and elements
2.4	2022-03-31	Incorporation of TC feedback
2.3	2021-08-10	Support for MDF, Bluetooth updates
2.2	2021-01-05	Update release
2.1	2019-11-14	Initial Release

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

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

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

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

- Protection Profile for General Purpose Operating System, version 4.3.
- Protection Profile for Mobile Device Fundamentals, version 3.3.
- Protection Profile for Application Software, version 2.0.
- Protection Profile for Mobile Device Management, version 4.0.

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

- VPN client, Version 2.6

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

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

1.2 Structure of the Document

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

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

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

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

1.3 Terms

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

1.3.1 Common Criteria Terms

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

Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Technical Terms

Administrator	A user that has administrative privilege to configure the TOE in privileged mode.
Authorized	An entity granted access privileges to an object, system, or system entity.
Critical Security Parameter (CSP)	Security related information such as secret and private cryptographic keys, and authentication data such as passwords and PINs, whose disclosure or modification can compromise the security of a cryptographic module.
Entropy Source	This cryptographic function provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.
IT Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Private Network	A network that is protected from access by unauthorized users or entities.
Privileged Mode	A TOE operational mode that allows a user to perform functions that require IT environment administrator privileges.
Public Network	A network that is visible to all users and entities and does not protect against unauthorized access (e.g. internet).
Threat Agent	An entity that tries to harm an information system through destruction, disclosure, modification of data, or denial of service.
Unauthorized User	An entity (device or user) that has not been authorized by an authorized administrator to access the TOE or private network.
Unprivileged Mode	A TOE operational mode that only provides VPN client functions for the VPN client user.
VPN Client	The TOE; allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to a private network.
VPN Client User	A user operating the TOE in unprivileged mode.
VPN Gateway	A component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network.

2 Evaluation Activities for SFRs

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

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

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

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

2.1 Protection Profile for General Purpose Operating System

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

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the GPOS PP is the base.

2.1.2 Additional SFRs

2.1.2.1 Cryptographic Support (FCS)

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the VPN client or the OS, the evaluator shall check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator shall review the TSS to determine that it makes a case that, for each item listed as being manipulated, it is not written unencrypted to persistent memory, and that the item is stored by the OS.
Guidance
There are no guidance EAs for this requirement.
Tests
There are no test EAs for this component.

2.1.2.2 Identification and Authentication (FIA)

FIA_X509_EXT.4 X.509 Certificate Use and Management

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

FIA_X509_EXT.4.2
TSS
The evaluator shall check the TSS to ensure that it describes whether the VPN client or the OS implements the certificate validation functionality, how the VPN client/OS chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the OS so that desired certificates can be used. The evaluator shall examine the TSS to confirm that it describes the behavior of the client/OS when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Guidance
If the requirement indicates that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
Tests
The evaluator shall perform the following test regardless of whether the certificate validation functionality is implemented by the VPN client or by the OS:

- Test FIA_X509_EXT.4.2:1: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.4.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.

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

2.1.2.3 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1
TSS
The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN gateway, VPN client, or IPsec-capable network device in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.
Guidance
The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to a VPN gateway, VPN client, or IPsec-capable network device, and that it contains recovery instructions should a connection be unintentionally broken.
Tests
The evaluator shall perform the following tests:

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

Further EAs are associated with requirements for FCS_IPSEC_EXT.1.

2.2 Protection Profile for Mobile Device Fundamentals

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

2.2.1 Modified SFRs

The PP-Module does not modify any requirements when the MDF PP is the base.

2.2.2 Additional SFRs

2.2.2.1 User Data Protection (FDP)

FDP_VPN_EXT.1 Split Tunnel Prevention

FDP_VPN_EXT.1.1
TSS
The evaluator shall verify that the TSS section of the ST describes the routing of IP traffic through processes on the TSF when a VPN client is enabled. The evaluator shall ensure that the description indicates which traffic does not go through the VPN and which traffic does and that a configuration exists for each baseband protocol in which only the traffic identified by the ST author is necessary for establishing the VPN connection (IKE traffic and perhaps HTTPS or DNS traffic) is not encapsulated by the VPN protocol (IPsec). The ST author shall also identify in the TSS section any differences in the routing of IP traffic when using any supported baseband protocols (e.g. Wi-Fi, LTE).
Guidance
The evaluator shall verify that the following is addressed by the documentation: The description above indicates that if a VPN client is enabled, all configurations route all IP traffic (other than IP traffic required to establish the VPN connection) through the VPN client. The guidance describes how the user or administrator can configure the TSF to meet this requirement.
Tests
The evaluator shall perform the following test: Step 1 - The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an internet-connected network. The evaluator shall turn on the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data. Step 2 - The evaluator shall configure an IPsec VPN client that supports the routing specified in this requirement, and if necessary, configure the device to perform the routing specified as described in the AGD guidance. The evaluator shall turn on the sniffing tool, establish the

VPN connection, and perform the same actions with the device as performed in the first step. The evaluator shall verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data. Step 3 - The evaluator shall examine the traffic from both step one and step two to verify that all IP traffic, aside from and after traffic necessary for establishing the VPN (such as IKE, DNS, and possibly HTTPS), is encapsulated by IPsec. Step 4 - The evaluator shall attempt to send packets to the TOE outside the VPN connection and shall verify that the TOE discards them.

2.3 Protection Profile for Application Software

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

2.3.1 Modified SFRs

The PP-Module does not modify any requirements when the App PP is the base.

2.3.2 Additional SFRs

2.3.2.1 Cryptographic Support (FCS)

FCS_CKM.6 Cryptographic Key Destruction

FCS_CKM.6
TSS
The evaluator shall ensure that all plaintext secret and private cryptographic keys and CSPs (whether manipulated by the TOE or exclusively by the platform) are identified in the VPN client ST's TSS, and that they are accounted for by the EAs in this section. Requirement met by the platform: The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate keys that are not otherwise covered by the FCS_CKM.6 requirement levied on the TOE. For each platform listed in the ST, the evaluator shall examine the TSS of the ST of the platform to ensure that each of the secret keys, private keys, and CSPs used to generate the keys listed above are covered. Requirement met by the TOE: The evaluator shall check to ensure the TSS describes when each of the plaintext keys are cleared (e.g., system power off, disconnection of an IPsec connection, when no longer needed by the VPN channel per the protocol); and the type of clearing procedure that is performed (cryptographic erase, overwrite with zeros, overwrite three or more times by a different alternating pattern, overwrite with random pattern, or block erase). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting three times with a random pattern that is changed before each write").
Guidance
There are no guidance EAs for this requirement.
Tests
For each key clearing situation described in the TSS, the evaluator shall repeat the following test.

- Test FCS_CKM.6:1: The evaluator shall use appropriate combinations of specialized OE and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key. Cryptographic TOE implementations in software shall be loaded and exercised under a debugger to perform such tests. The evaluator shall perform the following test for each key subject to clearing, including intermediate copies of keys that are persisted encrypted by the TOE: Load the instrumented TOE build in a debugger. Record the value of the key in the TOE subject to clearing. Cause the TOE to perform a normal cryptographic processing with the key from #1. Cause the TOE to clear the key. Cause the TOE to stop the execution but not exit. Cause the TOE to dump the entire memory footprint of the TOE into a binary file. Search the content of the binary file created in #6 for instances of the known key value from #1. The test succeeds if no copies of the key from #1 are found in step #7 above and fails otherwise. The evaluator shall perform this test on all keys, including those persisted in encrypted form, to ensure intermediate copies are cleared.

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the TOE or the TOE platform, the evaluator shall check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator shall then perform the following actions: Persistent secrets and private keys manipulated by the platform: For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the persistent secrets and private keys listed as being stored by the platform in the VPN client ST are identified as being protected in that platform's ST Persistent secrets and private keys manipulated by the TOE: The evaluator shall review the TSS to determine that it makes a case that, for each item listed as being manipulated by the TOE, it is not written unencrypted to persistent memory, and that the item is stored by the platform.

Guidance
There are no guidance EAs for this requirement.
Tests
There are no test EAs for this requirement.

2.4 Protection Profile for Mobile Device Management

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

2.4.1 Modified SFRs

The PP-Module does not modify any requirements when the MDM PP is the base.

2.5 TOE SFR Evaluation Activities

The PP-Module does not define any mandatory requirements (i.e. Requirements that are included in every configuration regardless of the PP-Bases selected).

2.6 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.7 Evaluation Activities for Selection-Based SFRs

The PP-Module does not define any selection-based requirements.

2.8 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

2.9 Evaluation Activities for Implementation-dependent SFRs

The PP-Module does not define any implementation-dependent requirements.

3 Evaluation Activities for SARs

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

4 Required Supplementary Information

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

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[GPOS PP]	Protection Profile for General Purpose Operating Systems, Version 4.3, September 27, 2022
	Protection Profile for Mobile Device Fundamentals, Version 3.3, Version 3.3, September 12,

[MDF PP]	2022
[MDM PP]	Protection Profile for Mobile Device Management, Version 4.0, April 25, 2019
[App PP]	Protection Profile for Application Software, Version 2.0, June 16, 2025