National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 5 October 2017

Report Number:	**CCEVS-VR-PP-0050**
Dated:	**11 June 2019**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

<u>**Common Criteria Testing Laboratory**</u>

Base Requirements

Gossamer Common Criteria Testing Laboratory
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Module for Virtual Private Network (VPN) Clients, Version 2.1 (MOD_VPN_CLI_v2.1), which is intended for use with the following Base-PPs:

- Protection Profile for General Purpose Operating Systems (GPOS PP); or
- Protection Profile for Mobile Device Fundamentals (MDF PP); or
- Protection Profile for Application Software (App PP).

It presents a summary of the MOD_VPN_CLI_v2.1 and the evaluation results.

Gossamer Security, located in Catonsville, Maryland performed the evaluation of the MOD_VPN_CLI_v2.1 concurrent with the first product evaluation against the PP-Module requirements. The evaluated product was Samsung Galaxy Devices on Android 8. For this evaluation, MOD_VPN_CLI_v2.1 extended the MDF PP.

This evaluation addressed the base and selection-based requirements of the MOD_VPN_CLI_v2.1. The MOD_VPN_CLI_v2.1 also includes several objective requirements; however, the evaluated TOE did not include any this functionality so they were not claimed by this evaluation. Likewise, since the TOE claimed conformance to the MDF PP, any MOD_VPN_CLI_v2.1 requirements that only apply when the GPOS PP or App PP is used as a Base-PP were not applicable to the evaluation.

The Validation Report (VR) author independently performed an additional review of the PP-Module as part of the completion of this VR, to confirm it meets the claimed ACE assurance requirements.

The initial results by the validation team found that the evaluation showed that the MOD_VPN_CLI_v2.1did not meet the requirements of the ACE components. These findings were confirmed by the VR author and NIAP. NIAP determined the impact of the changes were limited to evaluations that included the App PP as the Base-PP. There was a missing dependency SFR: FMT_STM for the objective SFR: FAU_GEN. After further review it was determined this SFR was intended to be implicitly met by the platform assumption A.Platform in the App PP. However, it was determined that A.Platform in the App PP should be more specific. As a result, the App PP was updated through issuance of a NIAP Technical Decision (TD). As a result, the validation team found that the VPN Client PP-Module meets the requirements of the ACE components. Since the evaluated product did not claim the App PP as its base, there was no impact on its security functionality, and the product is fully compliant.

The evaluation determined the MOD_VPN_CLI_v2.1 is both Common Criteria Part 2 Extended and Part 3 Conformant. A NIAP approved CCTL evaluated the PP-Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). The Security Target (ST) includes material from both the MDF PP and the MOD_VPN_CLI_v2.1; completion of the ASE work units satisfied the ACE work units for this PP-Module, but only for the materials defined in this PP-Module.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules that have Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP or PP-Module.

In order to promote thoroughness and efficiency, the evaluation of the MOD_VPN_CLI_v2.1 was performed concurrent with the first product evaluation against the PP-Module's requirements. In this case the Target of Evaluation (TOE) was Samsung Galaxy Devices on Android 8, performed by Gossamer Security in Catonsville, MD, United States of America.

The MOD_VPN_CLI_v2.1 has a set of "base" requirements all conformant STs must include and also has "Additional", "Selection-based," and "Objective" requirements. Additional requirements are defined for each Base-PP and must be included for TOE's claiming conformance to those Base-PP(s). Selection-based requirements must be included based on the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those the PP-Module sponsor intends to mandate in future versions, and are included as optional requirements that raise industry awareness of expected future requirements. This evaluation did not claim the optional functions these requirements described.

A specific ST may not include these discretionary requirements, so the initial use of the PP-Module addresses (in terms of the PP-Module evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ workunits performed against the PP-Module. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the MOD_VPN_CLI_v2.1 were evaluated.

The following identifies the PP-Module that is evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP-Module and any subsequent evaluations that address additional optional, selection-based, or objective requirements in the PP-Module.

Protection Profile/Extended Package	PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 2017-10-05
ST (Base)	Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 8 (MDFPP31/WLANCEP10/VPNC21) Security Target, Version 0.4, 2018/05/15
Assurance Activity Report (Base)	Assurance Activity Report (MDFPP31/WLANCEP10) for Samsung Galaxy Devices on Android 8, Version 0.3, 05/15/2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5

Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Gossamer Security, Catonsville, MD, USA

3 MOD_VPN_CLI_v2.1 Description

The MOD_VPN_CLI_v2.1 specifies information security requirements for VPN Clients, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A VPN Client in the context of this PP-Module is a software application that runs on a physical or virtual host platform, used to establish a secure IPsec connection between that host platform and a remote system, primarily using the IPsec protocol.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections should exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
A .PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

4.2 Threats

The following table shows applicable threats, in addition to those defined in the Base-PPs that the PP-Module extends.

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_ACCESS	This PP-Module does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the system or device that contains the IPsec VPN client. Therefore, the primary threat agents are the unauthorized entities that try to gain access to the protected network (in cases where tunnel mode is used) or to plaintext data that traverses the public network (regardless of whether transport mode or tunnel mode is used). The endpoint of the network communication can be both geographically and logically distant from the TOE, and can pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications over the network to be compromised.

	Plaintext communication over the network may allow critical data (such as passwords, configuration settings, and user data) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE or to the secured environmental system(s) that the TOE is being used to facilitate communications with. IPsec can be used to provide protection for this communication; however, there are myriad options that can be implemented for the protocol to be compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises. Even though the communication path is protected, there is a possibility that the IPsec peer could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the request as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate IPsec peer when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.
T.TSF_CONFIGURATION	Configuring VPN tunnels is a complex and time-consuming process, and prone to errors if the interface for doing so is not well-specified or well-behaved. The inability to configure certain aspects of the interface may also lead to the mis-specification of the desired communications policy or use of cryptography that may be desired or required for a particular site. This may result in unintended weak or plaintext communications while the user thinks that their data are being protected. Other aspects of configuring the TOE or using its security mechanisms (for example, the update process) may also result in a reduction in the trustworthiness of the VPN client.
T .UNAUTHORIZED_UPDATE	Since the most common attack vector used involves attacking unpatched versions of software containing well-known flaws, updating the VPN client is necessary to ensure that changes to threat environment are addressed. Timely application of patches ensures that the client is a "hard target", thus increasing the likelihood that product will be able to maintain and enforce its security policy. However, the updates to be applied to the product must be trustable in some manner; otherwise, an attacker can write their own "update" that instead contains malicious code of their choosing, such as a rootkit, bot, or other malware.

	Once this “update” is installed, the attacker then has control of the system and all of its data. Methods of countering this threat typically involve hashes of the updates, and potentially cryptographic operations (e.g., digital signatures) on those hashes as well. However, the validity of these methods introduces additional threats. For instance, a weak hash function could result in the attacker being able to modify the legitimate update in such a way that the hash remained unchanged. For cryptographic signature schemes, there are dependencies on 1) the strength of the cryptographic algorithm used to provide the signature, and 2) the ability of the end user to verify the signature (which typically involves checking a hierarchy of digital signatures back to a root of trust (a certificate authority)). If a cryptographic signature scheme is weak, then it may be compromised by an attacker and the end user will install a malicious update, thinking that it is legitimate. Similarly, if the root of trust can be compromised, then a strong digital signature algorithm will not stop the malicious update from being installed (the attacker will just create their own signature on the update using the compromised root of trust, and the malicious update will then be installed without detection).
T.USER_DATA_REUSE	Data traversing the TOE could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently re-used in sending network traffic to a user other than that intended by the sender of the original network traffic.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

4.3 Organizational Security Policies

The following table shows applicable organizational security policies, in addition to those defined in the Base-PPs that the PP-Module extends.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
This EP does not define any organizational security policies.	

4.4 Security Objectives

The following table shows security objectives for the TOE, in addition to those defined in the Base-PPs that the PP-Module extends.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
This Module does not define security objectives for the TOE. The Base-PPs that this PP-module extends define the objectives.	

The following table shows security objectives for the Operational Environment, in addition to those defined in the Base-PPs.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
OE.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
OE.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5 Requirements

As indicated above, the MOD_VPN_CLI_v2.1 requirements include the "base" requirements and additional requirements that are strictly or conditionally optional. The following table shows the "base" requirements validated as part of the Samsung evaluation activities referenced above. Those requirements that are listed as being verified by "PP Evaluation" were evaluated separately by the VR author as part of the completion of the ACE evaluation work units against the PP-Module. These were not included in the Samsung evaluation because they only apply in cases where the TOE extends the GPOS PP or App PP, and the Samsung evaluation used the PP-Module to extend the MDF PP.

Table 6: Base and Mandatory Additional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support)	FCS_CKM.1/VPN Cryptographic Key Generation (IKE): Additional SFR for GPOS and MDF only	Samsung Galaxy Devices on Android 8
	FCS_CKM_EXT.2 Cryptographic Key Storage: Additional SFR for GPOS and APP only	PP Evaluation
	FCS_CKM_EXT.4 Cryptographic Key Destruction: Additional SFR for APP only	PP Evaluation
	FCS_IPSEC_EXT.1 IPsec	Samsung Galaxy Devices on Android 8
FDP: User Data Protection	FDP_RIP.2 Full Residual Information Protection	Samsung Galaxy Devices on Android 8
FIA: Identification and Authentication	FIA_X509_EXT.3 X.509 Certificate Use and Management: Additional SFR for GPOS	PP Evaluation
FMT: Security Management	FMT_SMF.1/VPN Specification of Management Functions (VPN)	Samsung Galaxy Devices on Android 8
FPT: Protection of the TSF	FPT_TST_EXT.1 TSF Self-Test	Samsung Galaxy Devices on Android 8
FTP: Trusted Path/Channels	FTP_ITC.1 Inter-TSF Trusted Channel: Additional SFR for GPOS	PP Evaluation

The following table shows the "**Optional**" requirements included in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
The VPN Client Module does not include any optional requirements.		

The following table shows the "**Selection-Based**" requirements included in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors make associated selections in requirements levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1 Pre-Shared Key Composition	Samsung Galaxy Devices on Android 8

The following table shows the "**Objective**" requirements included in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1 Audit Data Generation	PP Evaluation
	FAU_SEL.1 Selective Audit	PP Evaluation
FDP: User Data Protection	FDP_IFC_EXT.1 Subset Information Flow Control	PP Evaluation

6 Assurance Requirements

The following shows the assurance requirements included in the MOD_VPN_CLI_v2.1.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Samsung Galaxy Devices on Android 8
	ASE_ECD.1: Extended Components Definition	Samsung Galaxy Devices on Android 8
	ASE_INT.1: ST Introduction	Samsung Galaxy Devices on Android 8
	ASE_OBJ.2: Security Objectives	Samsung Galaxy Devices on Android 8
	ASE_REQ.2: Derived Security Requirements	Samsung Galaxy Devices on Android 8
	ASE_SPD.1: Security Problem Definition	Samsung Galaxy Devices on Android 8

Requirement Class	Requirement Component	Verified By
	ASE_TSS.1: TOE Summary Specification	Samsung Galaxy Devices on Android 8
ADV: Development	ADV_FSP.1 Basic Functional Specification	Samsung Galaxy Devices on Android 8
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Samsung Galaxy Devices on Android 8
	AGD_PRE.1: Preparative Procedures	Samsung Galaxy Devices on Android 8
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Samsung Galaxy Devices on Android 8
	ALC_CMS.1: TOE CM Coverage	Samsung Galaxy Devices on Android 8
	ALC_TSU_EXT.1: Timely Security Updates	Samsung Galaxy Devices on Android 8
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Samsung Galaxy Devices on Android 8
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Samsung Galaxy Devices on Android 8

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 11: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Samsung Galaxy Devices on Android 8
ACE_CCL.1	Pass	Samsung Galaxy Devices on Android 8
ACE_SPD.1	Pass	Samsung Galaxy Devices on Android 8
ACE_OBJ.1	Pass	Samsung Galaxy Devices on Android 8
ACE_ECD.1	Pass	Samsung Galaxy Devices on Android 8
ACE_REQ.1	Pass	Samsung Galaxy Devices on Android 8
ACE_MCO.1	Pass	Samsung Galaxy Devices on Android 8
ACE_CCO.1	Pass	Samsung Galaxy Devices on Android 8

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_VPN_CLI_v2.1 Assurance Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017.

[7] PP-Configuration for Mobile Device Fundamentals (MDF) and Virtual Private Network (VPN) Clients, Version 1.0, 2019-03-11

[8] Protection Profile for General Purpose Operating Systems, Version 4.1, March 2016

[9] Protection Profile for Mobile Device Fundamentals, Version 3.1, June 2017

[10] Protection Profile for Application Software, Version 1.2, 22 April 2016

[11] Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 8 (MDFPP31/WLANCEP10/VPNC21) Security Target, Version 0.4, 2018/05/15

[12] Assurance Activity Report (MDFPP31/WLANCEP10) for Samsung Galaxy Devices on Android 8, Version 0.3, May 15, 2018