National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

PP-Configuration for General Purpose Operating Systems and Virtual Private Network (VPN) Clients, Version 1.0, 09 January 2020

Report Number: CCEVS-VR-PP-0067
Dated: 09 February 2021
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 6982
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base Requirements

DEKRA Testing and Certification S.A.U.
Avda. Pirineos, 7 28700 San Sebastián de los Reyes
Madrid, Spain

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-Configuration for General Purpose Operating Systems and Virtual Private Network (VPN) Clients, Version 1.0 (CFG_GPOS-VPNC_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for General Purpose Operating Systems (PP_GPOS_V4.2.1) Base-PP and the PP-Module for Virtual Private Network (VPN) Clients, Version 2.1 (MOD_VPN_CLI_V2.1). It presents a summary of the CFG_GPOS-VPNC_V1.0 and the evaluation results.

DEKRA Testing and Certification S.A.U. (DEKRA), located in Madrid, Spain, performed the evaluation of the CFG_GPOS-VPNC_V1.0 and MOD_VPN_CLI_V2.1 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Microsoft Windows 10, Windows Server version 1909 (Windows).

This evaluation addressed the base security functional requirements of MOD_VPN_CLI_V2.1 as part of CFG_GPOS-VPNC_V1.0. The PP-Module defines additional requirements, some of which the Windows evaluation claimed. The General Purpose Operating Systems (PP_GPOS_V4.2.1) Base-PP was previously validated to ensure compliance with Common Criteria requirements. The results of that evaluation were included in Validation Report Number CCEVS-VR-PP-0047, Version 1.0, dated 01 May 2019. The Validation Report (VR) author independently performed an additional review of the PP-Configuration and PP-Module as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_GPOS-VPNC_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration and PP-Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from both PP_GPOS_V4.2.1 and 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, and only when the PP-Module is in the defined PP-Configuration.

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 Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 work units specific to the technology described by the PP or PP-Module. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_GPOS-VPNC_V1.0 and MOD_VPN_CLI_V2.1 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Microsoft Windows 10, Windows Server version 1909, performed by DEKRA Testing and Certification S.A.U in Madrid, Spain.

This evaluation addressed the base security functional requirements of MOD_VPN_CLI_V2.1 as part of CFG_GPOS-VPNC_V1.0. The PP-Module defines additional requirements, some of which the Windows evaluation claimed.

MOD_VPN_CLI_V2.1 contains a set of base requirements that all conformant STs must include, and additionally contains selection-based and objective requirements. Objective requirements are requirements that are optional in the current version of the PP-Module but are expected to be included in future versions of the PP-Module as mandatory. Additionally, since MOD_VPN_CLI_V2.1 may extend multiple Base-PPs, it also defines requirements that only apply when a specific Base-PP is claimed. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units 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 CFG_GPOS-VPNC_V1.0 were evaluated.

The following identifies the PP-Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP-Module.

PP-Configuration	PP-Configuration for General Purpose Operating Systems and Virtual Private Network (VPN) Clients, Version 1.0, 09 January 2020
Base-PP	Protection Profile for General Purpose Operating Systems (PP_GPOS_V4.2.1)
Module(s) in PP-Configuration	PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017

ST (Base)	Microsoft Windows Common Criteria Evaluation, Microsoft Windows 10 and Microsoft Windows Server version 1909 (November 2019 Update) Security Target, Version 0.04, 16 January 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	DEKRA Testing and Certification S.A.U. Avda. Pirineos, 7 28700 San Sebastián de los Reyes Madrid, Spain

3 CFG_GPOS-VPNC_V1.0 Description

CFG_GPOS-VPNC_V1.0 is a PP-Configuration that combines the following:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1 (PP_GPOS_V4.2.1)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.1 (MOD_VPN_CLI_V2.1)

This PP-Configuration is for a software application that includes General Purpose Operating Systems (GPOS) and Virtual Private Network (VPN) Client functionality.

A VPN Client is a piece of software that allows a computer to establish a VPN with a remote peer or gateway. The VPN allows for confidentiality and integrity of the network traffic that passes over it. Specifically, MOD_VPN_CLI_V2.1 defines IPsec as the mechanism used to implement a VPN. In the context of CFG_GPOS-VPNC_V1.0, the VPN Client is a software component of a general-purpose operating system that is integrated with that operating system.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_GPOS-VPNC_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_GPOS_V4.2.1	
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act *as* the user, so requirements which confine malicious subjects are still in scope.
From MOD_VPN_CLI_V2.1	
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

Table 2 shows the threats defined in the individual components of CFG_GPOS-VPNC_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_GPOS_V4.2.1	
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
From MOD_VPN_CLI_V2.1	
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

Threat Name	Threat Definition
	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_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

Threat Name	Threat Definition
	"playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.
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

Table 3 shows the organizational security policies defined in the individual components of CFG_GPOS-VPNC_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_GPOS_V4.2.1	
No OSPs defined in PP_GPOS_V4.2.1.	
From MOD_VPN_CLI_V2.1	
No OSPs defined in MOD_VPN_CLI_V2.1.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_GPOS-VPNC_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_GPOS_V4.2.1	
O.ACCOUNTABILITY	Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.
O.INTEGRITY	Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.
From MOD_VPNC_V2.1	
No TOE Objectives defined in MOD_VPNC_V2.1 beyond those in the Base-PP.	

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_GPOS-VPNC_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_GPOS_V4.2.1	
OE.PLATFORM	The OS relies on being installed on trusted hardware.
OE.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
From MOD_VPN_CLI_V2.1	
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 Functional Requirements

As indicated above, CFG_GPOS-VPNC_V1.0 includes both PP_GPOS_V4.2.1 and MOD_VPN_CLI_V2.1. The functional requirements from PP_GPOS_V4.2.1 were evaluated separately so this section applies only to requirements of MOD_VPN_CLI_V2.1.

Requirements in the MOD_VPN_CLI_V2.1 are comprised of the "base" requirements, additional requirements that are selection-based or objective, and additional requirements that are dependent on the Base-PP that the PP-Module is used with. The following table contains the "base" requirements that were validated as part of the DEKRA evaluation activities referenced above as well as the additional requirements that depend on the Base-PP that is claimed. In the case of the DEKRA evaluation, only those that apply when PP_GPOS_V4.2.1 is the Base-PP were claimed by the TOE; those associated with other Base-PPs did not apply and have been evaluated through evaluation of the PP-Module work unites.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
Applicable when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FCS: Cryptographic Support	FCS_CKM.1/VPN: Cryptographic Key Generation (IKE)	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
	FCS_CKM_EXT.2: Cryptographic Key Storage	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
FIA: Identification and Authentication	FIA_X509_EXT.3: X.509 Certificate Use and Management	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
Applicable when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
FCS: Cryptographic Support	FCS_CKM.1/VPN: Cryptographic Key Generation (IKE)	PP-Module Evaluation
Applicable when the Protection Profile for Application Software is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Storage	PP-Module Evaluation
	FCS_CKM_EXT.4: Cryptographic Key Destruction	PP-Module Evaluation
Applicable to all TOEs		
FCS: Cryptographic Support	FCS_IPSEC_EXT.1: IPsec	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)

Requirement Class	Requirement Component	Verified By
FMT: Security Management	FMT_SMF.1/VPN: Specification of Management Functions (VPN)	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update) (as FMT_SMF.1(VPN))
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Self-Test	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update) (as FPT_TST_EXT.1(IPSEC))

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
The MOD_VPN_CLI_V2.1 does not define any additional optional requirements.		

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update) (as FAU_GEN.1(IPSEC))
	FAU_SEL.1: Selective Audit	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update)
FDP: User Data Protection	FDP_IFC_EXT.1: Subset Information Flow Control	Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server version 1909 (November 2019 Update) (as FDP_IFC_EXT.1(IPSEC))

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_GPOS_V4.2.1. The SARs defined in that PP are applicable to MOD_ VPN_CLI_V2.1 as well as CFG_GPOS-VPNC_V1.0 as a whole.

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 10: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	PP-Module evaluation
ACE_CCL.1	Pass	PP-Module evaluation
ACE_SPD.1	Pass	PP-Module evaluation
ACE_OBJ.1	Pass	PP-Module evaluation
ACE_ECD.1	Pass	PP-Module evaluation
ACE_REQ.1	Pass	PP-Module evaluation
ACE_MCO.1	Pass	PP-Module evaluation
ACE_CCO.1	Pass	PP-Module evaluation

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 Evaluation 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 Organizations. *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 Organizations. *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 Organizations. *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 Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

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

[6] Protection Profile for General Purpose Operating Systems, Version 4.2.1, 22 April 2019.

[7] PP-Configuration for General Purpose Operating Systems and Virtual Private Network (VPN) Clients, Version 1.0, 09 January 2020.

[8] Microsoft Windows Common Criteria Evaluation, Microsoft Windows 10 and Microsoft Windows Server version 1909 (November 2019 Update) Security Target, Version 0.04, 16 January 2020