National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1

Report Number: CCEVS-VR-PP-0004
Dated: 31 January 2014
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

Common Criteria Testing Laboratory

Base Requirements
Leidos (formerly SAIC)
Columbia, 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 Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1 (VPN Client PP). It presents a summary of the VPN Client PP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the VPN Client PP was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Microsoft Windows 8, Microsoft Windows Server 2012 capability (provided primarily by BitLocker). The evaluation was performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in April 2014. This evaluation addressed the base requirements as well as additional requirements in Appendix C of the VPN Client PP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the CCTL listed above.

The evaluation determined that the SWFDE is both **Common Criteria Part 2 Extended and Part 3 Conformant**. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). Because the ST contains only material drawn directly from the VPN Client PP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the VPN Client PP meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the VPN Client PP was performed concurrent with the first product evaluation against the PP. In this case the TOE

for this first product was the Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 capability. The evaluation was performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in January 2014.

The VPN Client PP contains a set of "base" requirements that all conformant STs must include, and in addition contain a set of "optional" requirements that may be included based on the selections made in the base requirements and the capabilities of the TOE. Because the optional requirements do not have to be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any optional requirements that are incorporated into the that initial ST. Subsequently, TOEs that are evaluated against the VPN Client PP that incorporate optional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and the appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP; it will be amended as subsequent evaluations address additional optional requirements in the VPN Client PP.

Protection Profile	*Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, 30 December 2012*
ST (Base)	Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target, Version 1.0, April 3, 2014
Evaluation Technical Report (Base)	Evaluation Technical Report for Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Part 2 (Microsoft Confidential), Version 1.0, 30 May 2013
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (Base and Additional)	Leidos (formerly SAIC), Columbia, MD
CCEVS Validators	Ken Elliott, The Aerospace Corporation

3 VPN Client PP Description

The VPN Client PP specifies Security Functional Requirements (SFRs) for a VPN Client. A VPN provides a protected transmission of private data between VPN Clients and VPN Gateways. The TOE defined by the PP is the VPN Client, a component executing on a remote access client, using a platform API that enables the VPN client application to interact with other applications and the client device platform (part of the Operational Environment of the TOE). The VPN Client is intended to be located outside or inside of a private network, and provides a secure tunnel to a VPN Gateway. The tunnel provides confidentiality, integrity, and data authentication for information

that travels across the public network. All VPN clients that comply with this document will support IPsec.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to 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: TOE Assumptions

Assumption	Description of Assumption
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 lists the threats addressed by the VPN Client and the operational environment. The assumed level of expertise of the attacker for all the threats identified below is unsophisticated.

Table 2: Threats

Threat	Description of Threat
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

4.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. There are no organizational security policies for the VPN Client PP.

4.4 Security Objectives for the TOE

Table 4: Security Objectives for the TOE

Objective	Objective Description
O.VPN_TUNNEL	The TOE will provide a network communication channel protected by encryption that ensures that the VPN client communicates with an authenticated VPN gateway.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Objective	Objective Description
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 operational environment.
OE.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5 Requirements

As indicated above, requirements in the VPN Client PP are comprised of the "base" requirements (appearing in Sections 4.1 and 4.2) and additional requirements appearing in Appendices B, C, and D of the VPN Client PP. The following are table contains the "base" requirements that were validated as part of the Microsoft Windows evaluation activity referenced above.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.1(2): Cryptographic Key Generation (for asymmetric keys - IKE)
	FCS_CKM_EXT.2: Cryptographic Key Storage
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_X509_EXT.1: Extended: X.509 Certificate Validation
	FIA_X509_EXT.2: Extended: X.509 Certificate Use and Management
FMT: Security management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel

The following table contains additional requirements contained in Appendices B, C, and D, 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.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Microsoft Windows 8, Windows RT, Server 2012, 23 January 2014
	FAU_SEL.1: Selective Audit	Microsoft Windows 8, Windows RT, Server 2012, 23 January 2014
FDP: User Data Protection	FDP_IFC_EXT.1: Extended: Subset Information Flow Control	
FIA: User Authentication	FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition	Microsoft Windows 8, Windows RT, Server 2012, 23 January 2014

6 Assurance Requirements

The following are the assurance requirements contained in the VPN Client PP:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.2	Pass

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 in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the VPN Client PP Assurance Activities to determine whether or not 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.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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 carried out by the CCEVS Validation Body leading to the issue 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 Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Part 2 (Microsoft Confidential)*, Version 1.0. 30 May 2013.

[7] Microsoft Corporation. *Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target*, Version 1.0, January 23, 2014

[8] *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.1, 30 December 2012