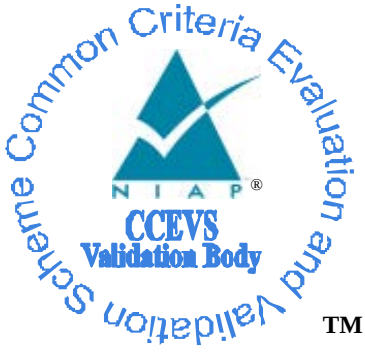
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client

Report Number: CCEVS-VR-VID10529-2013
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

Validation Team

Ken Elliott

The Aerospace Corporation

Jim Donndelinger

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Microsoft Windows 8, Microsoft Windows RT, and Microsoft Windows Server 2012 IPsec VPN Client product was performed by 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 evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, 30 December 2012. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is conformant to the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, 30 December 2012. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The focus of this evaluation is on the IPsec Virtual Private Network (VPN) client that is part of the Windows operating system. There are two mechanisms covered by this evaluation that invoke the IPsec VPN client: the Remote Access Service (RAS) interface, and the (raw) IPsec interface.

The IPsec interface is a part of the core networking stack and can be used to create IPsec security associations over both local and remote networks.

Remote Access Service (RAS) provides remote access capabilities to client applications on computers running Windows. Historically RAS was used for dial-up and point-to-point networking connections. However it can also be used to establish IPsec virtual private network sessions.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Windows 8, Windows RT, Windows Server 2012
Sponsor:	Microsoft Corporation
Developer:	Microsoft Corporation
CCTL:	Leidos (formerly SAIC) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	22 February 2013
Completion Date:	31 January 2014

CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 4, September 2012.
Evaluation Class:	None
Description:	The TOE provides capabilities for establishing IPsec security associations over both local and remote networks.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, 30 December 2012
Evaluation Personnel:	Leidos (formerly SAIC): Anthony J. Apted James L. Arnold, jr Tammy Compton Cornelius Haley
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. 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.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its operational environment are intended to fulfill:

- The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operability with other network equipment using the same protocols.
- The TOE must provide the capability to configure security-relevant aspects of its operation.

2 Identification

The evaluated product is **Microsoft Windows 8, Microsoft Windows RT, and Microsoft Windows Server 2012**, with focus on the IPsec Virtual Private Network (VPN) client that is part of these Windows operating systems.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the security policy has been derived from the Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target and Final ETR.*

3.1 Security Audit

Windows has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event-specific data. Authorized administrators can review audit logs and have the ability to search and sort audit records. Authorized administrators can also configure the audit system to include or exclude potentially auditable events to be audited based on a wide range of characteristics.

3.2 Cryptographic Protection

Windows provides FIPS-140-2 validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement (which is not studied in this evaluation), and random number generation. The TOE additionally provides support for public keys, credential management and certificate validation functions and provides support for the National Security Agency's Suite B cryptographic algorithms. Windows also provides extensive auditing support of cryptographic operations, the ability to replace cryptographic functions and random number generators with alternative implementations,[1] and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to using cryptography for its own security functions, Windows offers access to the cryptographic support functions for user-mode and kernel-mode programs. Public key certificates generated and used by Windows authenticate users and machines as well as user protect and system data in transit.

[1] This option is not included in the Windows Common Criteria evaluation.

- **IPsec:** Windows implements IPsec to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.

3.3 User Data Protection

In this context of this evaluation, Windows provides object and subject residual information protection.

3.4 Identification & Authentication

In the context of this evaluation, Windows provides the ability to use, store, and protect X.509 certificates that are used for IPsec. Windows also has the ability to use pre-shared keys for IPsec.

3.5 Security Management

Windows includes several functions to manage security policies. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

3.6 Protection of the TOE's Security Functions

Windows provides a number of features to ensure the protection of TOE security functions. Windows protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPsec, IKE, and ISAKMP. Windows ensures process isolation security for all processes through private virtual address spaces, execution context, and security context. The Windows data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. Windows includes self-testing features that ensure the integrity of executable program images and its cryptographic functions. Finally, Windows provides a trusted update mechanism to update Windows binaries itself.

3.7 Trusted Path for Communication

Windows uses the IPsec suite of protocols to provide a Virtual Private Network Connection (VPN) between itself, acting as a VPN client, and a VPN gateway.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients and performed by the evaluation team).

2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

The logical boundary of the TOE includes:

- The **IPv4 / IPv6 network stack** in the kernel.
- The **IPsec** module in user-mode.
- The **IKE and AuthIP Keying Modules** service which hosts the IKE and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec).
- The **Remote Access Service** device driver in the kernel, which is used primarily for ad hoc or user-defined VPN connections; known as the "RAS IPsec VPN" or "RAS VPN".
- The **IPsec Policy Agent** service which enforces IPsec policies.
- The **Cryptographic Services** module which confirms the signatures of Windows program files.
- **Windows Explorer** which can be used to create VPN connections and check the integrity of Windows files and updates.
- The **Certificates** MMC snap-in which is used when the authorized administrator needs to add a certificate, such as a root CA or machine certificate, to their certificate store.[2]
- The **Computer Configuration** MMC snap-in which can be used to set the auditing policy for the computer.
- The **Event Viewer** MMC snap-in which is used to view entries in the audit log.
- The **IP Security Monitor** MMC snap-in which can be used to view active IPsec security associations.
- The **IP Security Policies** MMC snap-in which is used to configure IPsec policies.
- The Windows **Registry** to manually set certain properties for the RAS interface.
- The **netsh** command line application which can be used to manage IPsec settings.
- The **auditpol** command line application which can be used to set the auditing policy for the computer.
- The **sfc** command line application which can be used to check the integrity and repair Windows files.

[2] For common deployment scenarios manually adding these certificates should not be necessary.

- The **Get-Authenticode PowerShell Cmdlet** which can be used to confirm the signatures of Windows program files.
- The following **PowerShell Cmdlets** to manage IPsec:
  - **Get-NetIPsecMainModeSA**
  - **Get-NetIPsecQuickModeSA**
  - **New-NetIPsecAuthProposal**
  - **New-NetIPsecPhase1AuthSet**
  - **New-NetIPsecMainModeCryptoProposal**
  - **New-NetIPsecMainModeCryptoSet**
  - **New-NetIPsecMainModeRule**
  - **New-NetIPsecQuickModeCryptoProposal**
  - **New-NetIPsecQuickModeCryptoSet**
  - **New-NetIPsecRule**
  - **Set-NetIPsecMainModeCryptoSet**
  - **Set-NetIPsecQuickModeCryptoSet**.

Physically, each TOE tablet, workstation, or server consists of an ARMv7 Thumb-2, x86 or x64 computer. The TOE executes on processors from Intel (x86 and x64), AMD (x86 and x64), Qualcomm (ARM), or NVIDIA (ARM).

A set of devices may be attached as part of the TOE:

- Display Monitors
- Fixed Disk Drives (including disk drives and solid state drives)
- Removable Disk Drives (including USB storage)
- Network Adaptor
- Keyboard
- Mouse
- Printer
- Audio Adaptor
- CD-ROM Drive
- Smart Card Reader
- Trusted Platform Module (TPM) version 1.2 or 2.0.

While this set of devices is larger than is needed to evaluate IPsec, it is the same set of devices as the General Purpose Operating System Protection Profile evaluation. By using the same set of devices for both evaluations, consumers can gain assurance by using both core OS capabilities and IPsec in combination.

The TOE does not include any network infrastructure components.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Microsoft Windows 8, Microsoft Windows Server 2012, Microsoft Windows RT Common Criteria Supplemental Admin Guidance for IPsec VPN Clients
- On-line documentation referenced by the Supplemental Admin Guidance

7 Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the Microsoft Windows 8, Windows RT, Windows Server 2012 Test Report and Microsoft Windows 8, Windows RT, Windows Server 2012 Detailed Test Results.

Evaluation team testing was conducted at the Leidos (formerly SAIC) CCTL in Columbia, MD.

7.1 Developer Testing

The assurance activities in the Protection Profile for IPsec Virtual Private Network (VPN) Clients do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the Microsoft Windows 8, Windows RT, Windows Server 2012 IPsec VPN Client Test Report. Tests were executed on all platforms claimed in the ST, with the exception of Windows Server 2012 Datacenter Edition, for which an equivalence argument to the Windows Server 2012 Standard Edition was provided.

The testing demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerabilities applicable to the TOE in its evaluated configuration, but did identify a general vulnerability of IPsec VPN clients, related to unverified Common Name in X.509 certificates. The evaluation team determined the tests already specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients were sufficient to test for this vulnerability, and evaluation team testing demonstrated the TOE is not subject to the vulnerability.

8 Evaluated Configuration

The evaluated version of the TOE is Microsoft Windows 8, Microsoft Windows RT, and Microsoft Windows Server 2012.

The TOE is delivered by six product variants of Windows 8, Windows RT, and Windows Server 2012:

- Microsoft Windows 8 Edition (32-bit and 64-bit versions)
- Microsoft Windows 8 Pro Edition (32-bit and 64-bit versions)

- Microsoft Windows 8 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows RT
- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2012 Datacenter Edition

The following security updates and patches must be applied to the above Windows 8 products:

- All critical security updates published as of February 2013.

The following security updates must be applied to the above Windows RT products:

- All critical security updates published as of February 2013.

The following security updates must be applied to the above Windows Server 2012 products:

- All critical security updates published as of February 2013.

Physically, each TOE tablet, workstation, or server consists of an ARMv7 Thumb-2, x86 or x64 computer. The TOE executes on processors from Intel (x86 and x64), AMD (x86 and x64), Qualcomm (ARM), or NVIDIA (ARM).

Evaluation testing took place on the following hardware platforms:

- Microsoft Surface RT
- Microsoft Surface Pro
- ASUS VivoTab RT
- Dell XPS 10
- Dell OptiPlex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit.

The evaluation covered the following mechanisms that invoke the IPsec VPN Client: the Remote Access Service (RAS) interface; and the underlying (raw) IPsec interface.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators do not have any additional comments or recommendations regarding the TOE.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target, Version 1.0, January 23, 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004.
5. Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, 30 December 2012.
6. Microsoft Windows 8, Microsoft Windows RT, Microsoft Windows Server 2012 IPsec VPN Client Security Target, Version 1.0, January 23, 2014.