National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Microsoft Windows 8.1 and Windows 8.1 Phone

Report Number:	**CCEVS-VR-VID10592-2015**
Dated:	**March 16, 2015**
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

Members from

The Aerospace Corporation,
The Mitre Corporation,
National Security Agency

Common Criteria Testing Laboratory

Kevin Micciche
Kevin Steiner
Gary Grainger

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Windows 8.1 and Windows Phone 8.1 Mobility Devices. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Windows 8.1 and Windows Phone 8.1 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in March 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Mobility Device Fundamentals, version 1.1. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www,niap-ccevs.org).

The Leidos evaluation team determined that Windows 8.1 and Windows Phone 8.1 are conformant to the claimed Protection Profiles (PPs) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Windows 8.1 and Windows Phone 8.1 Operating Systems, running on the following devices:

- **Microsoft Surface Pro 2**, Windows 8.1 Pro, 64-bit, Intel i5, Marvell AVASTAR 350N Wi-Fi a/b/g/n adapter, Intel TPM 1.2
- **Microsoft Lumia 520**, Windows Phone 8.1, Qualcomm Snapdragon S4 Plus MSM8227, LTE, Qualcomm WCN3620 Wi-Fi b/g/n adapter, Qualcomm TPM 2.0
- **Lenovo X1 Carbon**, Windows 8.1 Enterprise, 64-bit, Intel i7, Intel Dual Band Wireless 7260 Wi-Fi n adapter, Intel TPM 1.2
- **HP Pro x2 410 G1 Notebook PC**, Windows 8.1 Enterprise, 64-bit, Intel i5, Intel Dual Band Wireless 7260 Wi-Fi b/g/n adapter. Intel TPM 1.2
- **Dell Venue 8 Pro Tablet**, Windows 8.1, 32-bit, Intel Atom (64-bit), Dell Wireless 1538 Dual-Band 2x2 Wi-Fi b/g/n adapter, Intel TPM 2.0

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Microsoft Windows 8.1 and Windows Phone 8.1
Sponsor & Developer	Michael Grimm Microsoft Corporation
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	February 2015
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Protection Profile for Mobility Device Fundamentals*, Version 1.1
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Windows 8.1 and Windows Phone 8.1 by any agency of the U.S. Government and no warranty of Windows 8.1 and Windows Phone 8.1 is either expressed or implied.
Evaluation Personnel	Kevin Micciche Kevin Steiner Gary Grainger
Validation Body	National Information Assurance Partnership, CCEVS

2 Identification

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	**Description**
ST Title	Microsoft Windows Common Criteria Evaluation for Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Security Target
ST Version	1.0
Publication Date	March 6, 2015
Vendor and ST Author	Microsoft
TOE Reference	Windows 8.1 and Windows Phone 8.1
TOE Hardware Models	Microsoft Surface Pro 2 (Windows 8.1 Pro) Microsoft Lumia 520 (Windows Phone 8.1) Lenovo X1 Carbon (Windows 8.1 Enterprise) HP Pro x2 410 G1 Notebook PC (Windows 8.1 Enterprise) Dell Venue 8 Pro Tablet (Windows 8.1 Pro)
TOE Software Version	Windows 8.1 (Pro/Enterprise) and Windows Phone 8.1
Keywords	Mobility Device

2.1 Threats

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

- An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.
- An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software update of any applications or system software on the device. These attacks also include malicious web pages or email attachments which are usually delivered to devices over the network.
- The loss or theft of the Mobile Device may give rise to loss of confidentiality of user data including credentials. These physical access threats may involve attacks which attempt to access the device through external hardware ports, through its user interface, and also through direct and possibly destructive access to its storage media. The goal of such attacks is to access data from a lost or stolen device which is not expected to return to its user.
- Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally by its developer or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have

access. They may also conduct attacks against the platform‘s system software which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

- Persistent access to a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat in itself. In this case the device and its data may be controlled by an adversary at least as well as by its legitimate owner.

2.2 Organizational Security Policies

There are no Organizational Security Policies for the Mobile Device protection profile.

3 Architectural Information

The TOE is a hardware and software solution that consists of the Windows 8.1 and Windows Phone 8.1 Operating Systems, running on the following devices:

- **Microsoft Surface Pro 2**, Windows 8.1 Pro, 64-bit, Intel i5, Marvell AVASTAR 350N Wi-Fi a/b/g/n adapter, Intel TPM 1.2
- **Microsoft Lumia 520**, Windows Phone 8.1, Qualcomm Snapdragon S4 Plus MSM8227, LTE, Qualcomm WCN3620 Wi-Fi b/g/n adapter, Qualcomm TPM 2.0
- **Lenovo X1 Carbon**, Windows 8.1 Enterprise, 64-bit, Intel i7, Intel Dual Band Wireless 7260 Wi-Fi n adapter, Intel TPM 1.2
- **HP Pro x2 410 G1 Notebook PC**, Windows 8.1 Enterprise, 64-bit, Intel i5, Intel Dual Band Wireless 7260 Wi-Fi b/g/n adapter. Intel TPM 1.2
- **Dell Venue 8 Pro Tablet**, Windows 8.1, 32-bit, Intel Atom (64-bit), Dell Wireless 1538 Dual-Band 2x2 Wi-Fi b/g/n adapter, Intel TPM 2.0

Windows 8.1 and Windows Phone 8.1 are preemptive multitasking, multiprocessor, and multi-user operating systems. In general, operating systems provide users with a convenient interface to manage underlying hardware. They control the allocation and manage computing resources such as processors, memory, and Input/Output (I/O) devices. Windows 8.1and Windows Phone 8.1, collectively referred to as Windows, expand these basic operating system capabilities to controlling the allocation and managing higher level IT resources such as security principals (user or machine accounts), files, printing objects, services, window station, desktops, cryptographic keys, network ports traffic, directory objects, and web content. Multi-user operating systems such as Windows keep track of which user is using which resource, grant resource requests, account for resource usage, and mediate conflicting requests from different programs and users.

The TOE includes three product variants of Windows 8.1 and Windows Phone:

- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows Phone 8.1

Windows 8.1 is suited for business desktops, notebook, and convertible computers. It is the workstation product and while it can be used by itself, it is also designed to serve as a client within Windows domains.

Windows Phone 8.1 is based on the same core operating system as Windows 8.1 and provides a simplified user interface that makes Windows Phone a communications hub for voice, text, and web access.

The TOE includes both physical and logical boundaries. Its operational environment is that of a networked environment with IEEE 802.11 (Wi-Fi), mobile broadband networks (3G/4G and LTE) and Bluetooth networks

4 Assumptions

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

- It is assumed that the TOE‘s security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
- It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.
- It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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 Security Policy

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

5.1 Cryptographic Support

Windows provides NIST CAVP-validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, 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, 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 protect both user and system data in transit.

5.2 User Data Protection

In the context of this evaluation Windows protects user data at rest and provides secure storage of X.509v3 certificates.

5.3 Identification and Authentication

In the context of this evaluation, Windows provides the ability to use, store, and protect X.509 certificates that are used for IPsec and authenticates the user to their mobile device.

5.4 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.

5.5 Protection of the TSF

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.

Like TSF processes, user processes also are provided a private address space and process context, and therefore are protected from each other. Additionally, the TSF has the added ability to protect memory pages using Data Execution Prevention (DEP) which marks memory pages in a process as non-executable unless the location explicitly contains executable code. When the processor is asked to execute instructions from a page marked as data, the processor will raise an exception for the OS to handle.

The Windows kernel, user-mode applications, and all Windows Store Applications implement Address Space Layout Randomization (ASLR) in order to load executable code at unpredictable base addresses. The base address is generated using a pseudo-random number generator that is seeded by high quality entropy sources that provides at least 8 random bits for memory mapping.

5.6 Session Locking

Windows provides the ability for a user to lock their session either immediately or after a defined interval. Windows constantly monitors the mouse, keyboard, and touch display for activity and locks the computer after a set period of inactivity. Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialog.

5.7 Trusted Path/Channels

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 in addition to providing protected communications for HTTPS and TLS.

6 Documentation

Microsoft offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

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

- Microsoft Windows 8.1 and Windows Phone 8.1 Common Criteria Supplemental Admin Guidance, Version 1.0

The above document is considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The supplemental guidance document can be obtained by request from wincc@microsoft.com or from a customer’s local technical account manager.

The Security Target used is:

- Microsoft Windows Common Criteria Evaluation for Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Security Target, Version 1.0, March 6, 2015

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Microsoft Mobility Device PP Test Report and Procedures, March 16, 2015.

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to MDFPP v1.1.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in MDFPP. 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 team test report listed above.

Independent testing took place at the CCTL location in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in three distinct but representative configurations) in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for MDFPP v1.1 were fulfilled.

8 Evaluated Configuration

The following Windows Operating Systems (OS):

- Microsoft Windows 8.1 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 8.1 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Phone 8.1

The following security updates and patches must be applied to the above Windows 8.1 products:

- All critical updates as of July 31, 2014

The following security updates must be applied to the above Windows Phone 8.1 products:

- All critical updates as of July 31, 2014

TOE Hardware Identification: The following hardware platforms and components are included in the evaluated configuration:

- **Microsoft Surface Pro 2**, Windows 8.1 Pro, 64-bit, Intel i5, Marvell AVASTAR 350N Wi-Fi a/b/g/n adapter, Intel TPM 1.2
- **Microsoft Lumia 520**, Windows Phone 8.1, Qualcomm Snapdragon S4 Plus MSM8227, LTE, Qualcomm WCN3620 Wi-Fi b/g/n adapter, Qualcomm TPM 2.0
- **Lenovo X1 Carbon**, Windows 8.1 Enterprise, 64-bit, Intel i7, Intel Dual Band Wireless 7260 Wi-Fi n adapter, Intel TPM 1.2
- **HP Pro x2 410 G1 Notebook PC**, Windows 8.1 Enterprise, 64-bit, Intel i5, Intel Dual Band Wireless 7260 Wi-Fi b/g/n adapter. Intel TPM 1.2
- **Dell Venue 8 Pro Tablet**, Windows 8.1 Pro, 32-bit, Intel Atom (64-bit), Dell Wireless 1538 Dual-Band 2x2 Wi-Fi b/g/n adapter, Intel TPM 2.0

All devices include IEEE 802.11 Wi-Fi and Bluetooth 4.0, the Surface Pro 2 includes Bluetooth LE.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Mobility Device Fundamentals Version 1.1, 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 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 claimed PPs, 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 Leidos CCTL. A summary of the assessment is contained in the *Microsoft Windows Common Criteria Evaluation Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Assurance Activities Report, version 1.3, March 10, 2015*. The security assurance requirements are listed in the following table.

Table 3: 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

This section contains observations, recommendations, and caveats formulated by the validation team during the course of the evaluation and validation effort.

- The editions of Windows 8.1 that are included in this evaluation are also used on server, desktop, and laptop platforms as well. Users may expect that functionality present in those configurations is allowed in the configurations covered by this evaluation. However, the applications that may be loaded and used in an evaluated configuration of one of the TOE configurations listed in Section 8 are limited to applications from the Windows Apps Store. The MDFPP has requirements it places on TOE system services that applications can leverage, and this evaluation used only apps from the Windows App Store to comply with those requirements.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Microsoft Windows Common Criteria Evaluation for Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Security Target
ST Version	1.0
Publication Date	March 6, 2015

13 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
AAR	Assurance Activities Report
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CC Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CLI	Command Line Interface
EP	Extended Package
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IOS	Inter-network Operating System
IPsec	Internet Protocol security
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
USB	Universal Serial Bus
VPN	Virtual Private Network
VR	Validation Report
WAN	Wide Area Network

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Microsoft Windows Common Criteria Evaluation for Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Security Target, version 1.0, March 6, 2015

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report for Microsoft Windows 8.1 and Windows Phone 8.1, February 11, 2015, Version 1.0

[8] Microsoft Windows 8.1 and Windows Phone 8.1 Common Criteria Supplemental Admin Guidance, Version 1.0

[9] Microsoft Windows Common Criteria Evaluation Microsoft Windows 8.1, Microsoft Windows Phone 8.1 Assurance Activities Report, version 1.3, March 10, 2015.

[10] Microsoft Windows 8.1 Common Criteria Test Report and Procedures for Mobility Device PP (Proprietary), Report Version 1.0, 11 March 2015.