National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Microsoft Windows 10 (Anniversary Update)

Report Number: CCEVS-VR-10752-2017
Dated: April 12, 2017
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

Stelios Melachrinoudis
Jean Petty

Common Criteria Testing Laboratory

Leidos, 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 to determine 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, as well as this Validation Report (VR), which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration, to help in that determination. Prospective users should carefully read 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 Microsoft Windows 10 Mobile (Anniversary Update) and Windows 10 (Anniversary Update) with Microsoft Surface Book, Microsoft Surface Pro 4, Microsoft Surface Pro 3, Microsoft Surface 3, Microsoft Surface 3 with LTE, Microsoft Lumia 950, Microsoft Lumia 950 XL, Microsoft Lumia 650, HP Elite x3, and Dell Latitude 5580. 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 Microsoft Windows 10 Mobile (Anniversary Update) and Windows 10 (Anniversary Update) with Microsoft Surface Book, Microsoft Surface Pro 4, Microsoft Surface Pro 3, Microsoft Surface 3, Microsoft Surface 3 with LTE, Microsoft Lumia 950, Microsoft Lumia 950 XL, Microsoft Lumia 650, HP Elite x3, and Dell Latitude 5580 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in April 2017. 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 the assurance activities specified in the *Protection Profile for Mobility Device Fundamentals,* version 2.0. 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 Microsoft Windows 10 Mobile (Anniversary Update) and Windows 10 (Anniversary Update) with Microsoft Surface Book, Microsoft Surface Pro 4, Microsoft Surface Pro 3, Microsoft Surface 3, Microsoft Surface 3 with LTE, Microsoft Lumia 950, Microsoft Lumia 950 XL, Microsoft Lumia 650, HP Elite x3, and Dell Latitude 5580 is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of Microsoft Windows 10 Mobile (Anniversary Update) and Windows 10 (Anniversary Update) editions running on the following devices:

- Microsoft Surface Book, Windows 10 Enterprise and Windows 10 Pro
- Microsoft Surface Pro 4, Windows 10 Enterprise and Pro
- Microsoft Surface Pro 3, Windows 10 Enterprise and Windows 10 Pro
- Microsoft Surface 3, Windows 10 Enterprise and Windows 10 Pro
- Microsoft Surface 3 with LTE, Windows 10 Enterprise and Windows 10 Pro
- Microsoft Lumia 950, Windows 10 Mobile
- Microsoft Lumia 950 XL, Windows 10 Mobile

- Microsoft Lumia 650, Windows 10 Mobile
- HP Elite x3, Windows 10 Mobile
- Dell Latitude 5580, Windows 10 Enterprise and Pro

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 PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as 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 10 (Anniversary Update) Pro Edition (64-bit version) Microsoft Windows 10 (Anniversary Update) Enterprise Edition (64-bit version) Microsoft Windows 10 Mobile (Anniversary Update)
Sponsor & Developer	Michael Grimm Microsoft Corporation
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	April 2017
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 2.0
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Microsoft Windows 10 (Anniversary Update) mobile devices by any agency of the U.S. Government and no warranty of Microsoft Windows 10 mobile devices is either expressed or implied.
Evaluation Personnel	Gregory Beaver Gary Grainger Kevin Steiner

Item	Identifier
Validation Personnel	Stelios Melachrinoudis, Lead Validator Jean Petty, Senior Validator

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 Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Microsoft Windows 10 (Anniversary Update) and Windows 10 Mobile (Anniversary Update) Security Target
ST Version	0.08
Publication Date	March 24, 2017
Vendor and ST Author	Microsoft
TOE Reference	Microsoft Windows 10 (Anniversary Update)
TOE Hardware Models	Microsoft Surface Book, Windows 10 Enterprise and Windows 10 Pro Microsoft Surface Pro 4, Windows 10 Enterprise and Pro Microsoft Surface Pro 3, Windows 10 Enterprise and Windows 10 Pro Microsoft Surface 3, Windows 10 Enterprise and Windows 10 Pro Microsoft Surface 3 with LTE, Windows 10 Enterprise and Windows 10 Pro Microsoft Lumia 950, Windows 10 Mobile Microsoft Lumia 950 XL, Windows 10 Mobile Microsoft Lumia 650, Windows 10 Mobile HP Elite x3, Windows 10 Mobile Dell Latitude 5580, Windows 10 Enterprise and Pro
TOE Software Version	Microsoft Windows 10 (Anniversary Update) Pro Edition (64-bit version) Microsoft Windows 10 (Anniversary Update) Enterprise Edition (64-bit version) Microsoft Windows 10 Mobile (Anniversary Update)
Keywords	Mobility Device

2.1 Threats

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

- If positioned on a wireless communications channel or elsewhere on the network, attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.

- An attacker may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints.
- Loss of confidentiality of user data and credentials may be a result of an attacker gaining physical access to a Mobile Device.
- Malicious or exploitable code could be used knowingly or unknowingly by a developer, possibly resulting in the capability of attacks against the platform's system software.
- An attacker gains and continues to have access the device, resulting it loss of integrity and possible control by both an adversary and 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 Microsoft Windows 10 (Anniversary Update) Operating System editions running on the following devices:

- **Microsoft Surface Book**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Core i7, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface Pro 4**, Windows 10 Enterprise and Pro, 64-bit, Intel Core i7 , Marvell 8897, IEEE 801.11 Wi-Fi b/g/n adapter, Intel TPM 2.0, Bluetooth 4.0
- **Microsoft Surface Pro 3**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Core i7, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface 3**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Atom Z8700, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface 3 with LTE**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Atom Z8700, LTE, Marvell 8897 Wi-Fi a/b/g/n adapter, 3G/4G Mobile Broadband (GSM, HSPA and LTE protocol support), Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0 [one variant for Verizon networks, one variant which is SIM-unlocked]
- **Microsoft Lumia 950**, Windows 10 Mobile, Qualcomm Snapdragon 808, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi a/b/g/n adapter, Qualcomm TPM 2.0, Bluetooth 4.1
- **Microsoft Lumia 950 XL**, Windows 10 Mobile, Qualcomm Snapdragon 810, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi a/b/g/n adapter, Qualcomm TPM 2.0, Bluetooth 4.1
- **Microsoft Lumia 650**, Windows 10 Mobile, Qualcomm Snapdragon 210, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi b/g/n adapter, Qualcomm TPM 2.0
- **HP Elite x3**, Windows 10 Mobile, Qualcomm Snapdragon 820, GSM, WCDMA, LTE, Qualcomm MSM8996, IEEE 801.11 Wi-Fi a/c adapter, Qualcomm TPM 2.0
- **Dell Latitude 5580**, Windows 10 Enterprise and Pro, 64-bit, Intel Core i7, Intel 8265 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Nuvoton TPM 2.0

The Microsoft Windows 10 Mobile (Anniversary Update) and Microsoft Windows 10 (Anniversary Update) editions 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. Microsoft Windows 10 Mobile (Anniversary Update) and Microsoft Windows 10 (Anniversary Update) also referred to as “Windows”, expands 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 the following variants of Windows:

- Microsoft Windows 10 (Anniversary Update) Pro Edition (64-bit version)
- Microsoft Windows 10 (Anniversary Update) Enterprise Edition (64-bit version)
- Microsoft Windows 10 Mobile (Anniversary Update)

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.

The Security Functional Requirements were evaluated with respect to the TOE configurations listed above; however, there are a few variations in requirement specifics and applicability between the Windows 10 Mobile (Anniversary Update) Edition-based TOEs (Mobile Edition) and the Windows 10 Pro and Enterprise Edition-based (Anniversary Update) TOEs. These differences are summarized in the following table:

SFR	**Windows 10 Mobile**	**Windows 10 Enterprise and Pro**
FAU_GEN.1	Was not included in this evaluation.	Was included in this evaluation.
FAR_SAR.1	Was not included in this evaluation.	Was included in this evaluation.
FAU_SEL.1	Was not included in this evaluation.	Was included in this evaluation.
FAU_STG.1	Was not included in this evaluation.	Was included in this evaluation.
FAU_STG.4	Was not included in this evaluation.	Was included in this evaluation.
FCS_COP.1(PBKD)	The iteration count is 3,300.	The iteration count is 8,000.
FDP_DAR_EXT.1	Data at rest encryption uses AES-CBC.	Data at rest encryption can use either AES-CBC or AES-XTS.
FDP_DAR_EXT.2	Was included in this evaluation.	Was not included in this evaluation.
FMT_SMF_EXT.2	Will offer to wipe protected data when being unenrolled, in addition to alerting the administrator and removing Enterprise applications.	Only alerts the administrator and removes Enterprise applications upon unenrollment.

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 clarification. 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, operating system editions, and software versions identified in this document, and not any earlier or later versions released or in process. For example, functionality that is offered in Windows 10 Home edition was not evaluated.
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. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. Accordingly, the functionality offered by applications outside the Windows Store was not tested. The MDFPP has requirements it places on TOE system services that applications can leverage and this evaluation used only apps from the Windows Store to comply with those requirements. In particular, users and administrators should install applications from the Windows Store or via an MDM; otherwise the device will be outside the evaluated configuration.
5. Windows implements IPsec however it was not included in the Mobile Device Fundamentals PP evaluation because there is a separate protection profile for IPsec VPN clients. The native IPsec functionality provided by Windows 10 (Anniversary Update) has been evaluated against the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (VID10753).
6. Device manufacturers, OS developers, and mobile carriers provide many applications that provide capabilities outside of what is required in the MDF PP. AVA_VAN.1 in Section 6.6 of MDFPP V2.0 limits the scope of vulnerability search activities. Hence, identifying and inspecting data collected and transmitted by applications is beyond the scope of MDFPP V2.0.
7. 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 Security Audit

Windows 10 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. In the context of this evaluation, the protection profile requirements cover generating audit events, selecting which events should be audited, and providing secure storage for audit event entries.

5.2 Cryptographic Support

Windows provides CAVP 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 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 to authenticate users and machines as well as protect both user and system data in transit.

- *Software-based disk encryption:* Windows implements BitLocker to provide encrypted data storage for fixed and removable volumes and protects the disk volume's encryption key with one or more intermediate keys and authorization factor
- *IPsec:* Windows implements IPsec to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.[1]

5.3 User Data Protection

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

5.4 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 TLS and authenticates the user to their mobile device.

5.5 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.

[1] Windows implements IPsec however it was not included in the Mobile Device Fundamentals PP evaluation because there is a separate protection profile for IPsec VPN clients.

5.6 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. 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.

5.7 TOE Access

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.

5.8 Trusted Path/Channels

Windows uses a 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 Common Criteria Evaluation Microsoft Windows 10 (Anniversary Update) Mobile Device Operational Guidance*, Version 1.0, March 16, 2017.

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 Security Target used is:

- *Microsoft Windows 10 (Anniversary Update) and Windows 10 Mobile (Anniversary Update) Security Target*, Version 0.08, March 24, 2017.

7 Independent Testing

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

- *Windows 10 Anniversary Update Common Criteria Test Report and Procedures for Mobility Device Fundamentals PP*, Version 1.1, March 8, 2017

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- *Microsoft Windows 10 Anniversary Update with Microsoft Surface Book, Surface Pro 4, Surface Pro 3, Surface 3, Surface 3 with LTE, Lumia 950, Lumia 950 XL, Lumia 650, HP Elite x3, and Dell Latitude 5580 Common Criteria Assurance Activities Report*, Version 1.1 March 31, 2017

The purpose of the testing 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 PP MDF v2.0.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in PP MDF. 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.

Testing of the TOE was performed from August 29, 2016 through September 2, 2016 and January 9, 2017 through January 13, 2017 on developer site in Redmond, WA and July 14, 2016 through January 20, 2017 at the Leidos CCTL in Columbia, MD. During the onsite the evaluator was given full access to the TOE and developer test tools to use throughout testing.

Prior to testing, the evaluation team performed an onsite evaluation per NIAP Labgram #078/Valgram #098: CCTL Evaluation Test Requirements. The vendor site controlled access to the test facility. Only the employees who were involved in testing were allowed in the testing facility. The testing was performed on an isolated network to prevent tampering. The test environment was verified to be functioning properly before being used as part of testing.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE 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 PP MDF v2.0 were fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE consists of the following software and hardware device combinations.

TOE Software Identification: The following Windows Operating System editions are included in the evaluation:

- Microsoft Windows 10 AU Pro edition (64-bit version) on Microsoft Surface book
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Microsoft Surface Book
- Microsoft Windows 10 AU Pro edition (64-bit version) on Microsoft Surface Pro 4
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Microsoft Surface Pro 4
- Microsoft Windows 10 AU Pro edition (64-bit version) on Microsoft Surface Pro 3
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Microsoft Surface Pro 3
- Microsoft Windows 10 AU Pro edition (64-bit version) on Microsoft Surface 3
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Microsoft Surface 3
- Microsoft Windows 10 AU Pro edition (64-bit version) on Microsoft Surface 3 with LTE
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Microsoft Surface 3 with LTE
- Microsoft Windows 10 AU Mobile on Microsoft Lumia 950
- Microsoft Windows 10 AU Mobile on Microsoft Lumia 950 XL
- Microsoft Windows 10 AU Mobile on Microsoft Lumia 650
- Microsoft Windows 10 AU Mobile on HP Elite x3
- Microsoft Windows 10 AU Pro edition (64-bit version) on Dell Latitude 5580
- Microsoft Windows 10 AU Enterprise edition (64-bit version) on Dell Latitude 5580

The following security updates must be applied to the above Windows 10 products:

- All critical updates as of December 31, 2016.

TOE Hardware Identification: The following hardware devices and components are included in the evaluation:

- **Microsoft Surface Book**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Core i7, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface Pro 4**, Windows 10 Enterprise and Pro, 64-bit, Intel Core i7 , Marvell 8897, IEEE 801.11 Wi-Fi b/g/n adapter, Bluetooth 4.0 Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface Pro 3**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Core i7, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface 3**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Atom Z8700, Marvell 8897 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0
- **Microsoft Surface 3 with LTE**, Windows 10 Enterprise and Windows 10 Pro, 64-bit, Intel Atom Z8700, GSM, LTE, HSPA, Marvell 8897 Wi-Fi a/b/g/n adapter, , Bluetooth 4.0, Bluetooth LE, Intel TPM 2.0 [one variant for Verizon networks, one variant which is SIM-unlocked]
- **Microsoft Lumia 950,** Windows 10 Mobile, Qualcomm Snapdragon 808, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi a/b/g/n adapter, Qualcomm TPM 2.0, Bluetooth 4.1

- **Microsoft Lumia 950 XL,** Windows 10 Mobile, Qualcomm Snapdragon 810, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi a/b/g/n adapter, Qualcomm TPM 2.0, Bluetooth 4.1
- **Microsoft Lumia 650,** Windows 10 Mobile, Qualcomm Snapdragon 212, GSM, WCDMA, LTE, Qualcomm WCN3620, IEEE 801.11 Wi-Fi b/g/n adapter, Qualcomm TPM 2.0, Bluetooth 4.1
- **HP Elite x3,** Windows 10 Mobile, Qualcomm Snapdragon 820, GSM, WCDMA, LTE, Qualcomm MSM8996, IEEE 801.11 Wi-Fi a/c adapter, Qualcomm TPM 2.0
- **Dell Latitude 5580,** Windows 10 Enterprise and Pro, 64-bit, Intel Core i7, Intel 8265 Wi-Fi a/b/g/n adapter, Bluetooth 4.0, Nuvoton TPM 2.0

The TOE must be deployed as described in Section 4 Assumptions of this document and be configured in accordance with the *Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 (Anniversary Update) Mobile Device Operational Guidance,* Version 1.0, March 16, 2017.

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Mobility Device Fundamentals,* Version 2.0, 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. The security assurance requirements are listed in the following table.

Table 3: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.1	Security objectives for the operational environment
ASE_REQ.1	Stated security requirements
ASE_SPD.1	Security Problem Definition
ASE_TSS.1	TOE summary specification
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
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the Microsoft Windows 10 Mobile (Anniversary Update) and Microsoft Windows 10 (Anniversary Update), to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

For all Microsoft Surface, Surface Pro, and Surface Book devices, as well as the Latitude 5580, evaluators discovered that Windows displays the following warning when the user is about to surpass the policy for failed authentication attempts:

> "If you keep entering the wrong password, you'll be locked out to help protect your data. To unlock, you'll need a BitLocker recovery key."

It is important for users, customers, and sponsors to understand that until an update is issued to modify this warning to one that better reflects the evaluated configuration, the warning must be disregarded as of the completion of this evaluation. There is no BitLocker recovery key created, utilized, or transmitted anywhere when Windows 10 is in its evaluated configuration, including as a recovery mechanism. Consequently, when the maximum number of unsuccessful authentication attempts has been surpassed, the user is not "locked out" but instead the user and organizational data on the device is wiped.

According to the Operational Guidance, the cipher suite selection and priority may be configured on the server side of a connection. Cipher suite selection is made according to the default order for Windows 10. Additionally, Windows 10 devices may be configured to trust a Certificate Authority by using policy pushed to the device by an MDM. The TOE comes preloaded with root certificates for various Certificate Authorities. Additional Certificate Authorities may be managed on the Windows 10 device using workplace enrollment and an MDM.

While there is traditionally an option to disable or enable location services on an MDM system or by a local Windows 10 administrator on a Windows 10 device, the Surface Book, Surface Pro 4, Surface Pro 3, Surface 3 (LTE), and Latitude 5580 do not have a GPS radio. Instead, they determine the location from available network information. In addition, the Surface Book, Surface Pro 4, Surface Pro 3, Surface 3 (LTE), and Latitude 5580 do not have the ability to initiate or receive phone calls and so the devices do not contain a dialer or any USSD or MMI codes. As such, GPS and telephony capabilities are out of scope.

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Microsoft Windows 10 (Anniversary Update) and Windows 10 Mobile Security Target
ST Version	0.08
Publication Date	March 24, 2017

13 Abbreviations and Acronyms

ACE	Access Control Entry
ACL	Access Control List
ACP	Access Control Policy
AD	Active Directory
ADAM	Active Directory Application Mode
AES	Advanced Encryption Standard
AGD	Administrator Guidance Document
AH	Authentication Header
ALPC	Advanced Local Process Communication
ANSI	American National Standards Institute
API	Application Programming Interface
APIC	Advanced Programmable Interrupt Controller
BTG	BitLocker To Go
CA	Certificate Authority
CBAC	Claims Basic Access Control, see DYN
CBC	Cipher Block Chaining
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CIFS	Common Internet File System
CIMCPP	Certificate Issuing and Management Components For Basic Robustness Environments Protection Profile, Version 1.0, April 27, 2009
CM	Configuration Management; Control Management
COM	Component Object Model
CP	Content Provider
CPU	Central Processing Unit
CRL	Certificate Revocation List
CryptoAPI	Cryptographic API
CSP	Cryptographic Service Provider
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DC	Domain Controller
DEP	Data Execution Prevention
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DFS	Distributed File System
DMA	Direct Memory Access
DNS	Domain Name System
DS	Directory Service
DSA	Digital Signature Algorithm
DYN	Dynamic Access Control
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EFS	Encrypting File System
ESP	Encapsulating Security Protocol
FEK	File Encryption Key
FIPS	Federal Information Processing Standard

FRS	File Replication Service
FSMO	Flexible Single Master Operation
FTP	File Transfer Protocol
FVE	Full Volume Encryption
GB	Gigabyte
GC	Global Catalog
GHz	Gigahertz
GPC	Group Policy Container
GPO	Group Policy Object
GPOSPP	US Government Protection Profile for General-Purpose Operating System in a Networked Environment
GPT	Group Policy Template
GPT	GUID Partition Table
GUI	Graphical User Interface
GUID	Globally Unique Identifiers
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
I/O	Input / Output
I&A	Identification and Authentication
IA	Information Assurance
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
ID	Identification
IDE	Integrated Drive Electronics
IETF	Internet Engineering Task Force
IFS	Installable File System
IIS	Internet Information Services
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IPC	Inter-process Communication
IPI	Inter-process Interrupt
IPsec	IP Security
ISAPI	Internet Server API
IT	Information Technology
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPC	Local Procedure Call
LSA	Local Security Authority
LSASS	LSA Subsystem Service
LUA	Least-privilege User Account
MAC	Message Authentication Code
MB	Megabyte
MMC	Microsoft Management Console
MSR	Model Specific Register
NAC	(Cisco) Network Admission Control
NAP	Network Access Protection

NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NLB	Network Load Balancing
NMI	Non-maskable Interrupt
NTFS	New Technology File System
NTLM	New Technology LAN Manager
OS	Operating System
PAE	Physical Address Extension
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RADIUS	Remote Authentication Dial In Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RAS	Remote Access Service
RC4	Rivest’s Cipher 4
RID	Relative Identifier
RNG	Random Number Generator
RPC	Remote Procedure Call
RSA	Rivest, Shamir and Adleman
RSASSA	RSA Signature Scheme with Appendix
SA	Security Association
SACL	System Access Control List
SAM	Security Assurance Measure
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SAS	Secure Attention Sequence
SD	Security Descriptor
SHA	Secure Hash Algorithm
SID	Security Identifier
SIP	Session Initiation Protocol
SIPI	Startup IPI
SF	Security Functions
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SMI	System Management Interrupt
SMTP	Simple Mail Transport Protocol
SP	Service Pack
SPI	Security Parameters Index
SPI	Stateful Packet Inspection
SRM	Security Reference Monitor
SSL	Secure Sockets Layer
SSP	Security Support Providers
SSPI	Security Support Provider Interface
ST	Security Target
SYSVOL	System Volume

TCP	Transmission Control Protocol
TDI	Transport Driver Interface
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSS	TOE Summary Specification
UART	Universal Asynchronous Receiver / Transmitter
UI	User Interface
UID	User Identifier
UNC	Universal Naming Convention
US	United States
UPN	User Principal Name
URL	Uniform Resource Locator
USB	Universal Serial Bus
USN	Update Sequence Number
v5	Version 5
VDS	Virtual Disk Service
VPN	Virtual Private Network
VSS	Volume Shadow Copy Service
WAN	Wide Area Network
WCF	Windows Communications Framework
WebDAV	Web Document Authoring and Versioning
WebSSO	Web Single Sign On
WDM	Windows Driver Model
WIF	Windows Identity Framework
WMI	Windows Management Instrumentation
WSC	Windows Security Center
WU	Windows Update
WSDL	Web Service Description Language
WWW	World-Wide Web
X64	A 64-bit instruction set architecture
X86	A 32-bit instruction set architecture

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] *Protection Profile for Mobile Device Fundamentals,* Version 2.0, 17 September 2014.

[6] *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013.

[7] *Microsoft Windows 10 (Anniversary Update) and Windows 10 Mobile (Anniversary Update) Security Target,* Version 0.08, March 24, 2017

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

[9] *Evaluation Technical Report for Microsoft Windows 10 Anniversary Update with Microsoft Surface Book, Surface Pro 4, Surface Pro 3, Surface 3, Surface 3 with LTE, Lumia 950, Lumia 950 XL, Lumia 650, HP Elite x3, and Dell Latitude 5580,* Version 1.1, March 31, 2017

[10] *Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 (Anniversary Update) Mobile Device Operational Guidance*, Version 1.0, March 16, 2017.

[11] *Microsoft Windows 10 Anniversary Update with Microsoft Surface Book, Surface Pro 4, Surface Pro 3, Surface 3, Surface 3 with LTE, Lumia 950, Lumia 950 XL, Lumia 650, HP Elite x3, and Dell Latitude 5580 Common Criteria Assurance Activities Report,* Version 1.1 March 31, 2017