Reference: 2018-25-INF-2642-v1
Target: Público
Date: 20.12.2018

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-25**
TOE	**Windows 10 and Windows Server: build 10.0.17134 (also known as version 1803)**
Applicant	**600413485 - Microsoft Corp.**

References

[EXT-4196] Certification request

[EXT-4505] Evaluation Technical Report v1.0

Certification report of the product Windows 10 and Windows Server: build 10.0.17134 (also known as version 1803), as requested in [EXT-4196] dated 03/08/2018, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4505] received on 19/11/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product:

Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (April 2018 Update) (32-bit version)
- Microsoft Windows 10 Pro Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows 10 Enterprise Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows Server Standard Core, version 1803
- Microsoft Windows Server Datacenter Core, version 1803

TOE Versions:

- Windows 10: build 10.0.17134 (also known as version 1803)
- Windows Server: build 10.0.17134 (also known as version 1803)

The following security updates must be applied for:

- Windows 10 and Windows Server: all critical updates as of July 30, 2018

The certified TOE includes the Windows 10 operating system, the Windows Server operating system, and those applications necessary to manage, support and configure the operating system. Windows 10 and Windows Server can be delivered preinstalled on a new computer or downloaded from the Microsoft website.

Developer/manufacturer: Microsoft Corp.

Sponsor: Microsoft Corp..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profiles:

- General Purpose Operating Systems Protection Profile, Version 4.1, March 9, 2016 ([GPOSPP]).
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, version 1.0, February 8, 2016 ([GPOSPP-WLAN-EP]).

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to the [GPOSPP] and [GPOSPP-WLAN-EP].

Evaluation end date: 19/11/2018.

All the assurance components required by the evaluation level of the [GPOSPP] and [GPOSPP-WLAN-EP] have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [GPOSPP] and [GPOSPP-WLAN-EP] assurance level packages, as defined by the Common Criteria version 3.1 release 5, the [GPOSPP], the [GPOSPP-WLAN-EP] and the Common Criteria Evaluation Methodology version 3.1 release 5.

Considering the obtained evidences during the instruction of the certification request of the product Windows 10 and Windows Server: build 10.0.17134 (also known as version 1803), a positive resolution is proposed.

TOE SUMMARY

All Windows 10 and Windows Server editions, collectively called "Windows", 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 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.

TOE major security features

The major security features implemented by the TOE and subject to evaluation (no assurance can be supposed to any other

- **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. 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.
- **Cryptographic Support**: Windows provides FIPS 140-2 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.

- **User Data Protection**: In the context of this evaluation Windows protects user data and provides virtual private networking capabilities.
- **Identification and Authentication**: Each Windows user must be identified and authenticated based on administrator-defined policy prior to performing any TSF-mediated functions. An interactive user invokes a trusted path in order to protect his I&A information. Windows maintains databases of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows account policy functions include the ability to define the minimum password length, the number of failed logon attempts, the duration of lockout, and password age.
- **Protection of the TOE 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.
- **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.
- **TOE Access**: Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialog.
- **Trusted Path for Communications**: Windows uses HTTPS, TLS, DTLS, and EAP-TLS to provide a trusted path for communications.

- **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.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance packages defined in [GPOSPP], according to Common Criteria v3.1 release 5. The TOE meet the following SARs:

Requirement Class	Requirement Component
Security Target (ASE)	ST Introduction (ASE_INT.1) Conformance Claims (ASE_CCL.1) Security Objectives (ASE_OBJ.1) Extended Components Definition (ASE_ECD.1) Stated Security Requirements (ASE_REQ.1) Security Problem Definition (ASE_SPD.1) TOE Summary Specification (ASE_TSS.1)
Design (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance (AGD)	Operational User Guidance (AGD_OPE.1) Preparative Procedures (AGD_PRE.1)
Lifecycle (ALC)	Labeling of the TOE (ALC_CMC.1) TOE CM Coverage (ALC_CMS.1) Timely Security Updates (ALC_TSU_EXT.1)
Testing (ATE)	Independent Testing – Conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

The detailed specification of the SARs can be found in the Security Target, section 5.2.

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 release 5:

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation (FAU_GEN.1) Audit Data Generation (FAU_GEN.1 (WLAN))
Cryptographic Support (FCS)	Cryptographic Key Generation for (FCS_CKM.1) Cryptographic Key Generation for WPA2 Connections (FCS_CKM.1(WLAN)) Cryptographic Key Establishment (FCS_CKM.2(1) Cryptographic Key Distribution for GTK (FCS_CKM.2(WLAN)) Cryptographic Key Destruction (FCS_CKM.4) Cryptographic Operation for Data Encryption/Decryption (FCS_COP.1(SYM)) Cryptographic Operation for Hashing (FCS_COP.1(HASH)) Cryptographic Operation for Signing (FCS_COP.1(SIGN)) Cryptographic Operation for Keyed Hash Algorithms (FCS_COP.1(HMAC)) Random Bit Generation (FCS_RBG_EXT.1) Storage of Sensitive Data (FCS_STO_EXT.1) TLS Client Protocol (FCS_TLSC_EXT.1) Extended: Extensible Authentication Protocol-Transport Layer Security (FCS_TLSC_EXT.1(WLAN)) TLS Client Protocol (FCS_TLSC_EXT.2) Extended: TLS Client Protocol (FCS_TLSC_EXT.2(WLAN)) TLS Client Protocol (FCS_TLSC_EXT.3) TLS Client Protocol (FCS_TLSC_EXT.4) DTLS Implementation (FCS_DTLS_EXT.1)
User Data Protection (FDP)	Access Controls for Protecting User Data (FDP_ACF_EXT.1) Information Flow Control (FDP_IFC_EXT.1)

Identification & Authentication (FIA)	Authorization Failure Handling (FIA_AFL.1) Extended: Port Access Entity Authentication (FIA_PAE_EXT.1) Multiple Authentication Mechanisms (FIA_UAU.5) X.509 Certification Validation (FIA_X509_EXT.1) X.509 Certificate Authentication (FIA_X509_EXT.2) Extended: X.509 Certificate Authentication (EAP-TLS) (FIA_X509_EXT.2(WLAN)) Extended: Certificate Storage and Management (FIA_X509_EXT.4)
Security Management (FMT)	Management of Security Functions Behavior (FMT_MOF_EXT.1) Specification of Management Functions (FMT_SMF_EXT.1) Extended: Specification of Management Functions (FMT_SMF_EXT.1(WLAN))
Protection of the TSF (FPT)	Access Controls (FPT_ACF_EXT.1) Address Space Layout Randomization (FPT_ASLR_EXT.1) Stack Buffer Overflow Protection (FPT_SBOP_EXT.1) Software Restriction Policies (FPT_SRP_EXT.1) Boot Integrity (FPT_TST_EXT.1) Extended: TSF Cryptographic Functionality Testing (FPT_TST_EXT.1 (WLAN)) Trusted Update (FPT_TUD_EXT.1) Trusted Update for Application Software (FPT_TUD_EXT.2)
TOE Access (FTA)	Default TOE Access Banners (FTA_TAB.1) Extended: Wireless Network Access (FTA_WSE_EXT.1)
Trusted Path/Channels (FTP)	Trusted Path (FTP_TRP.1) Trusted Channel Communication (FTP_ITC_EXT.1(TLS)) Trusted Channel Communication (FTP_ITC_EXT.1(DTLS)) Extended: Trusted Channel Communication (FTP_ITC_EXT.1 (WLAN))

The detailed specification of the SFRs can be found in the Security Target, section 5.1.

IDENTIFICATION

Product:

Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (April 2018 Update) (32-bit version)
- Microsoft Windows 10 Pro Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows 10 Enterprise Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows Server Standard Core, version 1803
- Microsoft Windows Server Datacenter Core, version 1803

TOE Versions:

- Windows 10: build 10.0.17134 (also known as version 1803)
- Windows Server: build 10.0.17134 (also known as version 1803)

The following security updates must be applied for:

- Windows 10 and Windows Server: all critical updates as of July 30, 2018

Security Target: Microsoft Windows 10, Windows Server (April 2018 Update) Security Target. Version: version 0.03, October 11, 2018.

Protection Profiles:

- General Purpose Operating Systems Protection Profile, Version 4.1, March 9, 2016 ([GPOSPP]).
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, version 1.0, February 8, 2016 ([GPOSPP-WLAN-EP]).

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to the [GPOSPP] and [GPOSPP-WLAN-EP].

SECURITY POLICIES

There are no Organizational Security Policies for the protection profile or extended package.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The complete list of assumptions can be found in the Security Target, section 3.3

CLARIFICATIONS ON NON-COVERED THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment as defined in the protection profiles [GPOSPP] and [GPOSPP-WLAN-EP] and included in the Security Target. They can be foun in the Security Target, section 3.1

The threats covered by the security properties of the TOE are categorized in the Security Target, section 3.1.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized in the Security Target, in the section 4.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

Conceptually the Windows TOE can be thought of as a collection of the following security services which the security target describes with increasing detail in the remainder of this document:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the TOE Security Functions
- Access to the TOE
- Trusted Path and Channels

These services are primarily provided by Windows components:

- The Boot Manager, which is invoked by the computer's bootstrapping code.
- The Windows Loader which loads the operating system into the computer's memory.
- The Windows Kernel which contains device drivers for the Windows NT File System, full volume encryption, the crash dump filter, and the kernel-mode cryptographic library.
- The IPv4 / IPv6 network stack in the kernel.
- The Windows Trusted Installer which installs updates to the Windows operating system.
- The Local Security Authority Subsystem which identifies and authenticates users prior to log on and generates events for the security audit log.
- FIPS-Approved cryptographic algorithms to protect user and system data.
- The Key Isolation Service which protects secret and private keys.
- Local and remote administrative interfaces for security management.
- Windows Explorer which can be used to manage the OS and check the integrity of Windows files and updates.

PHYSICAL ARCHITECTURE

Each instance of the general purpose OS TOE runs on a tablet, convertible, workstation or server computer. The TOE executes on processors from Intel (x86 and x64) or AMD (x86 and x64) along with peripherals for input/output (keyboard, mouse, display, and network).

The TOE does not include any hardware or network infrastructure components between the computers that comprise the distributed TOE. The security target assumes that any network connections, equipment, peripherals and cables are appropriately protected in the TOE security environment.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- *Microsoft Windows 10 and Windows Server (version 1803) GP OS Operational and Administrative Guidance* along with all the documents referenced therein.

PRODUCT TESTING

The tests performed by the evaluator are based on the assurance activities defined for the ATE activity in the [GPOSPP] and [GPOSPP-WLAN-EP] for each SFR that is included in the [ST].

The evaluator has performed an installation and configuration of the TOEs and their operational environment following the steps included in the installation and operation manual. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST].

The independent testing has covered 100% of SFRs of the [ST] and assurance activities defined in the [GPOSPP] and [GPOSPP-WLAN-EP] for each SFR. There has not been any deviation from the expected results under the environment defined in security target [ST].

PENETRATION TESTING

According to the [GPOSPP] and [GPOSPP-WLAN-EP], the vulnerability analysis scope has taken into account the public vulnerabilities affecting to all the operating system versions. The lab has performed a search on public sources to discover known vulnerabilities of the TOE belonging to the period from July 30, 2018 to October 10, 2018.

The lab has checked that all the public vulnerabilities previously published have been fixed as the TOE has been configured with all critical updates until July 30, 2018.

EVALUATED CONFIGURATION

The TOE under evaluation includes five product variants of Windows (build 10.0.17134):

- Microsoft Windows 10 Home Edition (April 2018 Update) (32-bit version)
- Microsoft Windows 10 Pro Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows 10 Enterprise Edition (April 2018 Update) (64-bit versions)
- Microsoft Windows Server Standard Core, version 1803
- Microsoft Windows Server Datacenter Core, version 1803

The following real and virtualized hardware platforms, corresponding firmware, and components are included in the evaluated configuration:

- Microsoft Surface Book 2
- Microsoft Surface Pro LTE
- Microsoft Surface Laptop
- Microsoft Surface Go
- Dell Latitude 5290
- Dell Latitude 12 Rugged Tablet

- Dell PowerEdge R740[1] (representing the 14th generation of PowerEdge servers.)
- Microsoft Windows Server Hyper-V
- Microsoft Windows Server 2016 Hyper-V

EVALUATION RESULTS

The TOE has been evaluated against the Security Target: Microsoft Windows 10, Windows Server (April 2018 Update) Security Target. Version: version 0.03, October 11, 2018.

All the assurance components defined in the [GPOSPP] and [GPOSPP-WLAN-EP] have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the assurances packages defined in the [GPOSPP] and [GPOSPP-WLAN-EP] and included in the [ST], as defined by the Common Criteria v3.1 release 5, the [GPOSPP], [GPOSPP-WLAN-EP] and the CEM v3.1 release 5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Epoche & Espri S.L.U., a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

[1] The Dell PowerEdge R440, R540, R640, , R740XD, T440, T640, R940, R940xa, R840, M640, M640p, FC640, MX740c, MX840c, C6420, C4140, XR2, and Dell Precision 7920 Rack all use the same processor, memory, chipset, and TPM and could be considered equivalent.

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[GPOSPP] General Purpose Operating Systems Protection Profile, Version 4.1, March 9, 2016.

[GPOSPP-WLAN-EP] General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, version 1.0, February 8, 2016.

[ST] Microsoft Windows 10, Windows Server (April 2018 Update) Security Target. Version: version 0.03, October 11, 2018.

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Microsoft Windows 10, Windows Server (April 2018 Update) Security Target. Version: version 0.03, October 11, 2018.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Microsoft Windows 10, Windows Server (April 2018 Update) Security Target. Version: version 0.04, October 11, 2018.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of

certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.