MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2015-27-INF-1539 v1	Created by: CERT10
Target: Público	Revised by: CALIDAD
Date: 06.04.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-27 Microsoft Windows 10 and Microsoft Windows Server 2012 R2

Applicant: MICROSOFT Microsoft Corp.

References:

[EXT-2825] Certification request of Microsoft Windows 10 and Microsoft Windows Server 2012 R2

[EXT-2952] Microsoft Windows Common Criteria Evaluation Microsoft Windows 10 & Microsoft Windows Server 2012 R2 Evaluation Technical Report, v 3.0, 21-03-201

The product documentation referenced in the above documents.

Certification report of the products

Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

TOE Build:

- Windows 10: build 10.0.10240
- Windows Server 2012 R2: build 6.3.9600

with all critical updates as of October 31, 2015

as requested in [EXT-2825] dated 20/11/2015, and evaluated by the laboratory Epoche & Espri S.L.U, as detailed in the Evaluation Technical Report [EXT-2952] received on 21/03/2016.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Microsoft Windows 10 and Microsoft Windows Server 2012 R2.

The TOE includes the Windows 10 operating system, the Windows Server 2012 R2 operating system, and those applications necessary to manage, support and configure the operating system. Windows 10 and Server 2012 R2 can run on any physical or virtual computer which is compatible with the x86 or x64 instruction set, such as processors from Intel or AMD.

The evaluation has been performed on the following TOE versions:

Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

TOE Build:

- Windows 10: build 10.0.10240
- Windows Server 2012 R2: build 6.3.9600

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 Profile: NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1 [GPOSPP]

Evaluation Level: Common Criteria v3.1 R4 (assurance packages according to the [GPOSPP]).

Evaluation end date: 21/03/2016.

All the assurance components required by the evaluation level of the [GPOSPP] 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] assurance level packages, as defined by the Common Criteria v3.1 R4, the [GPOSPP] and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product Microsoft Windows 10 and Microsoft Windows Server 2012 R2, a positive resolution is proposed.

TOE summary

Windows 10 and Windows Server 2012 R2, 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 functionality) to can be summarised as follows:

- 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 cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, and random number generation. 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 and 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 evidences required to fulfil the assurance packages defined in [GPOSPP], according to Common Criteria v3.1 R4.

Class	Family/Component

ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.1 Security objectives ASE_REQ.1 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labeling of the TOE ALC_CMS.1 TOE CM Coverage ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.1 Independent Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation (FAU_GEN.1)
Cryptographic Support (FCS)	Cryptographic Key Generation for (FCS_CKM.1)
	Cryptographic Key Establishment (FCS_CKM.2)
	Cryptographic Key Destruction (FCS_CKM_EXT.3)
	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)
	TLS Client Protocol (FCS_TLSC_EXT.2)
	TLS Client Protocol (FCS_TLSC_EXT.3)
	TLS Client Protocol (FCS_TLSC_EXT.4)

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)
	Multiple Authentication Mechanisms (FIA_UAU.5)
	X.509 Certification Validation (FIA_X509_EXT.1)
	X.509 Certificate Authentication (FIA_X509_EXT.2)
Security Management (FMT)	Management of Security Functions Behavior (FMT_MOF_EXT.1)
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)
	Integrity for Installation and Update (FPT_TUD_EXT.1)
	Integrity for Installation and Update of Application Software (FPT_TUD_EXT.2)
TOE Access (FTA)	Default TOE Access Banners (FTA_TAB.1)
Trusted Path/Channels (FTP)	Trusted Path (FTP_TRP.1)
	Trusted Channel Communication (FTP_ITC_EXT.1)

IDENTIFICATION

Product: Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

TOE Build:

- Windows 10: build 10.0.10240
- Windows Server 2012 R2: build 6.3.9600

with all critical updates as of October 31, 2015

Security Target: Microsoft Windows 10 Security Target version 1.0, March 17, 2016

Protection Profile: [GPOSPP]

Evaluation Level: Common Criteria v3.1 R4 (assurance packages according to the [GPOSPP]).

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation as there are not defined in the [GPOSPP].

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions specified in the [GPOSPP] and included in the [ST], are constraints to the conditions used to assure the security properties and functionalities compiled by the security target [ST]. 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.

Assumption	Description
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and

	uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment as defined in the [GPOSPP] and included in the [ST] are listed below.

Threat	Description
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

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 in the [GPOSPP] and included in the [ST] are categorized below.

Environment Objective	Description
OE.PLATFORM	The OS relies on being installed on trusted hardware.
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
OE.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise policy.

ARCHITECTURE

LOGICAL ARCHITECTURE

Logical boundaries

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.
- 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 for Windows 10 and Windows Server 2012 R2 which can be used to manage the OS and check the integrity of Windows files and updates.

PHYSICAL ARCHITECTURE

Physical boundaries

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 [ST] assumes that any network connections, equipment, peripherals and cables are appropriately protected in the TOE security environment.

DOCUMENTS

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

- Windows 10 and Server 2012 R2 GP OS Operational Guidance (January 13, 2016), version 0.09, 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] 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] 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], 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.

The lab has checked that all the public vulnerabilities published until October 31st have been fixed as the TOE has been configured with all critical updates until October 31.
For the public vulnerabilities identified for the period from November 1st to January 29th 2016, the vendor has published the corresponding update fixing the vulnerabilities.

EVALUATED CONFIGURATION

The TOE under evaluation is composed of the following operating system versions:

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

The build tested for all Windows 10 versions has been [version 10.0.10240] and for all Windows Server 2012 R2 versions [version 6.3.9600]. Before starting the testing all critical updates as of October 31, 2015 were applied in all operating systems.

The hardware platforms used during the evaluation are listed below:

- Microsoft Surface Pro 3
- Microsoft Surface 3
- Windows Server 2012 R2 Hyper-V
- HP Pro x612 Notebook PC
- Dell OptiPlex 755
- Microsoft Surface Book

The next table summarizes the combination between hardware platforms and operating system versions used for the testing:

Evaluated Testing Platforms	
Dell Optiplex 755 with Windows 10 x86 Pro Edition	
Dell Optiplex 755 with Windows 10 x86 Enterprise Edition	
Dell Optiplex 755 with Windows Server 2012 R2 Datacenter Edition	
HP Pro x2 612 with Windows 10 x64 Pro Edition	
Surface 3 with Windows 10 x64 Enterprise Edition	
Surface 3 Pro with Windows 10 x64 Enterprise Edition	
Surface Book with Windows 10 x64 Enterprise Edition	
Windows Server 2012 R2 Hyper-V with Windows 10 x86 Home Edition	
Windows Server 2012 R2 Hyper-V with Windows 10 x64 Enterprise Edition	
Windows Server 2012 R2 Hyper-V with Windows Server 2012 R2 Standard Edition	

EVALUATION RESULTS

The products

“Windows Operating Systems (OS):

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

TOE Build:

- Windows 10: build 10.0.10240
- Windows Server 2012 R2: build 6.3.9600

with all critical updates as of October 31, 2015” have been evaluated against the “Microsoft Windows 10 Security Target version 1.0, March 17, 2016”.

All the assurance components defined in the [GPOSPP] 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 included in the [ST], as defined by the Common Criteria v3.1 R4, the [GPOSPP] and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. The following usage recommendations are given:

- 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 evidences obtained during the instruction of the certification request of the product “Microsoft Windows 10 and Microsoft Windows Server 2012 R2”, 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
SFR	Security Functional Requirement
TOE	Target Of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

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, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[GPOSPP] NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1, 20160309

[ST] Microsoft Windows 10 Security Target version 1.0, March 17, 2016

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Microsoft Windows 10 Security Target version 1.0, March 17, 2016

A sanitized version of this ST will be published in the website of the certification body.