Reference: 2023-8-INF-4178- v1
Target: Pública
Date: 16.01.2024

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

CERTIFICATION REPORT

Dossier #	**2023-8**
TOE	**Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge**
Applicant	**600413485 - Microsoft Corporation**

References

[EXT-8307] Certification request

[EXT-8676] Evaluation Technical Report

Certification report of the product Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge, as requested in [EXT-8307] dated 22/02/2023, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8676] received on 01/09/2023.

CONTENTS

EXECUTIVE SUMMARY

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

Windows Operating Systems (OS):

- Microsoft Windows 11 version 22H2 Enterprise edition
- Microsoft Windows 11 version 22H2 Pro edition
- Microsoft Windows 11 version 22H2 Education edition
- Microsoft Windows 11 version 22H2 IoT Enterprise edition
- Microsoft Windows 10 version 22H2 Pro edition
- Microsoft Windows 10 version 22H2 Enterprise edition
- Microsoft Windows Server 2022 Standard edition [1]
- Microsoft Windows Server 2022 Datacenter edition [2]
- Microsoft Windows Server Datacenter: Azure Edition [3]
- Microsoft Azure Stack HCIv2 version 22H2
- Microsoft Azure Stack Hub
- Microsoft Azure Stack Edge

TOE Versions:

- Microsoft Windows 11 build 10.0.22621.1 (also known as version 22H2)
- Microsoft Windows 10 build 10.0.19045.2006 (also known as version 22H2)
- Microsoft Windows Server 2022 10.0.20348.587
- Microsoft Windows Server Datacenter: Azure Edition build 10.0.20348.1006
- Microsoft Azure Stack HCIv2 version 10.0.20349.1129
- Microsoft Azure Stack Hub and Edge build 10.0.17784.1068

The following security updates must be applied for:

- Windows 11, Windows 10, Windows Server and Azure Stack: all critical updates as of June 1, 2023.

[1] With December 13, 2022 cumulative update.

[2] With December 13, 2022 cumulative update.

[3] December 2022 virtual machine image from Azure Marketplace.

The TOE includes the Windows 11 operating system; Windows 10 operating system; the Windows Server operating system; Azure Stack Hub, Edge and HCI; 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 Corporation.

Sponsor: Microsoft Corporation.

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

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profiles:

The ST and the Windows 10 and 11 editions (TOEs) claims exact conformance to:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
- PP-Module for WLAN Clients, version 1.0, March 31, 2022
- PP-Module for Virtual Private Network (VPN) Clients, version 2.4, March 31, 2022
- PP-Module for Bluetooth, version 1.0, April 15, 2021

The ST, the Windows Server and the Azure Stack editions (TOEs) claims exact conformance to:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
- PP-Module for Virtual Private Network (VPN) Clients, version 2.4, March 31, 2022
- PP-Module for Bluetooth, version 1.0, April 15, 2021

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module]).

Evaluation end date: 15/09/2023

Expiration Date[4]: 17/01/2029

All the assurance components required by the evaluation level of [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module] have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module] assurance level packages, as defined by the Common Criteria version 3.1 release 5, the [GPOSPP],

[4] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

[WLAN_Client_Module], [VPN_Client_Module], [Bluetooth_Module] and the Common Criteria Evaluation Methodology version 3.1 release 5.

Considering the obtained evidences during the instruction of the certification request of the TOE, a positive resolution is proposed.

TOE SUMMARY

The TOE includes the Windows 11 operating system; Windows 10 operating system; the Windows Server operating system; Azure Stack Hub, Edge and HCI; 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.

All Windows 11, Windows 10, Windows Server editions, plus the Windows operating systems in Azure Stack products, collectively called "Windows", are pre-emptive 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 Security Services

- **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. The TOE also provides extensive auditing support of cryptographic operations 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.

- TLS: Windows implements Transport Layer Security to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.
- IPsec: Windows implements IPsec to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.
- Wi-Fi: Windows implements IEEE 802.11 wireless networking to provide protected, authenticated, confidential, and tamper-proof networking between Windows clients and Wi-Fi access points.
- Bluetooth: Windows implements Bluetooth version 5.1 wireless networking protocols to provide protected, authenticated, confidential, and tamper-proof networking between Windows operating systems and Bluetooth peer devices.

Although Windows provides the ability to replace cryptographic functions and random number generators with alternative implementations, this functionality has not been evaluated and therefore is not covered by this certificate.

- **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. Windows provides the ability to use, store, and protect X.509 certificates that are used for IPsec VPN sessions.
- **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 TLS, HTTPS, DTLS, EAP-TLS, and IPsec 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 version 3.1 release 5. The TOE meets the following SARs:

Requirement Class	**Requirement Component**
Security Target (ASE)	ST Introduction (ASE_INT.1)
	Conformance Claims (ASE_CCL.1)
	Security Objectives (ASE_OBJ.2)
	Extended Components Definition (ASE_ECD.1)
	Stated Security Requirements (ASE_REQ.2)
	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)

SECURITY FUNCTIONAL REQUIREMENTS

The Windows 10 and Windows 11 editions satisfy functional requirements according to the Common Criteria version 3.1 release 5, [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module].

The Windows Server and Azure Stack editions satisfy functional requirements according to the Common Criteria version 3.1 release 5, [GPOSPP], [VPN_Client_Module] and [Bluetooth_Module].

All of them are listed in the tables below:

TOE Security Functional Requirements for [GPOSPP]

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.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)
	TLS Client Protocol (FCS_TLSC_EXT.2)
	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)
	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)
	Specification of Management Functions for OS (FMT_SMF_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)
	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)
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))

TOE Security Functional Requirements for [WLAN_Client_Module]

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation for Wireless LAN (FAU_GEN.1 (WLAN))
Cryptographic Support (FCS)	Cryptographic Key Generation for Symmetric Keys for WPA2/WPA3Connections (FCS_CKM.1(WPA))
	Cryptographic Key Distribution for Symmetric Keys for WPA2/WPA3Connections (FCS_CKM.2(WLAN))
	Extensible Authentication Protocol-Transport Layer Security (FCS_TLSC_EXT.1(WLAN))
	TLS Client Support for Supported Groups Extension (EAP-TLS for WLAN) (FCS_TLSC_EXT.2(WLAN))
	Supported WPA Versions (FCS_WPA_EXT.1)
Identification & Authentication (FIA)	X.509 Certificate Validation (FIA_X509_EXT.1(WLAN))
	X.509 Certificate Authentication EAP-TLS for WLAN (FIA_X509_EXT.2(WLAN))
	Certificate Storage and Management (FIA_X509_EXT.6)
Security Management (FMT)	Specification of Management Functions for Wi-Fi (FMT_SMF.1(WLAN))
Protection of the TSF (FPT)	TSF Cryptographic Functionality Testing (FPT_TST_EXT.3 (WLAN))
TOE Access (FTA)	Wireless Network Access (FTA_WSE_EXT.1)
Trusted Path/Channels (FTP)	Trusted Channel Communication (FTP_ITC_EXT.1 (WLAN))

TOE Security Functional Requirements for [VPN_Client_Module]

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation (FAU_GEN.1)
	Selective Audit (FAU_SEL.1)
Cryptographic Support (FCS)	Cryptographic Key Generation (FCS_CKM.1 (VPN))
	Cryptographic Key Storage (FCS_CKM_EXT.2)
	EAP-TLS (FCS_EAP_EXT.1)
	IPsec (FCS_IPSEC_EXT.1)
User Data Protection (FDP)	Split Tunnel Prevention (FDP_VPN_EXT.1)
	Full Residual Information Protection (FDP_RIP.2)
Identification & Authentication (FIA)	Pre-Shared Key Composition (FIA_PSK_EXT.1)
	Generated Pre-Shared Keys (FIA_PSK_EXT.2)
	X.509 Certificate Use and Management (FIA_X509_EXT.3)
Security Management (FMT)	Specification of Management Functions for VPN (FMT_SMF.1(VPN))
Protection of the TSF (FPT)	Self-Test for IPsec (FPT_TST_EXT.1 (VPN))
Trusted Path/Channels (FTP)	Inter-TSF Trusted Channel (FTP_ITC.1(VPN))

TOE Security Functional Requirements for [Bluetooth_Module]

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation (FAU_GEN.1(BT))
Cryptographic Support (FCS)	Bluetooth Key Generation (FCS_CKM_EXT.8)
Identification & Authentication (FIA)	Bluetooth User Authorization (FIA_BLT_EXT.1)
	Bluetooth Mutual Authentication (FIA_BLT_EXT.2)
	Rejection of Duplicate Bluetooth Connections (FIA_BLT_EXT.3)
	Secure Simple Pairing (FIA_BLT_EXT.4)
	Trusted Bluetooth Device User Authorization (FIA_BLT_EXT.6)
	Untrusted Bluetooth Device User Authorization (FIA_BLT_EXT.7)
Security Management (FMT)	Management of Security Functions Behavior for Bluetooth (FMT_MOF_EXT.1(BT))
	Specification of Management Functions for VPN (FMT_SMF_EXT.1(BT))
Trusted Path/Channels (FTP)	Bluetooth Encryption (FTP_BLT_EXT.1)
	Persistence of Bluetooth Encryption (FTP_BLT_EXT.2)
	Bluetooth Encryption Parameters (BR/EDR) (FTP_BLT_EXT.3(BR))
	Bluetooth Encryption Parameters (LE) (FTP_BLT_EXT.3(LE))

IDENTIFICATION

Product:

Windows Operating Systems (OS):

- Microsoft Windows 11 version 22H2 Enterprise edition
- Microsoft Windows 11 version 22H2 Pro edition
- Microsoft Windows 11 version 22H2 Education edition
- Microsoft Windows 11 version 22H2 IoT Enterprise edition
- Microsoft Windows 10 version 22H2 Pro edition
- Microsoft Windows 10 version 22H2 Enterprise edition
- Microsoft Windows Server 2022 Standard edition [5]
- Microsoft Windows Server 2022 Datacenter edition [6]
- Microsoft Windows Server Datacenter: Azure Edition [7]

[5] With December 13, 2022 cumulative update.

[6] With December 13, 2022 cumulative update.

[7] December 2022 virtual machine image from Azure Marketplace.

- Microsoft Azure Stack HCIv2 version 22H2
- Microsoft Azure Stack Hub
- Microsoft Azure Stack Edge

TOE Versions:

- Microsoft Windows 11 build 10.0.22621.1 (also known as version 22H2)
- Microsoft Windows 10 build 10.0.19045.2006 (also known as version 22H2)
- Microsoft Windows Server 2022 10.0.20348.587
- Microsoft Windows Server Datacenter: Azure Edition build 10.0.20348.1006
- Microsoft Azure Stack HCIv2 version 10.0.20349.1129
- Microsoft Azure Stack Hub and Edge build 10.0.17784.1068

The following security updates must be applied for:

- Windows 11, Windows 10, Windows Server and Azure Stack: all critical updates as of June 1, 2023.

Security Target:

Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge Security Target (version 0.04, 03/07/2023).

Protection Profile:

The ST and the Windows editions (TOEs) claims exact conformance to:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
- PP-Module for WLAN Clients, version 1.0, March 31, 2022
- PP-Module for Virtual Private Network (VPN) Clients, version 2.4, March 31, 2022
- PP-Module for Bluetooth, version 1.0, April 15, 2021

The ST, the Windows Server editions and the Azure Stack editions (TOEs) claims exact conformance to:

- Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019
- PP-Module for Virtual Private Network (VPN) Clients, version 2.4, March 31, 2022
- PP-Module for Bluetooth, version 1.0, April 15, 2021

Evaluation Level:

Common Criteria version 3.1 release 5 (assurance packages according to [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module]).

SECURITY POLICIES

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

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following 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 detail of these assumptions is documented in the Security Target, section 3.3 (“Secure usage assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.1 (“Threats to security”) do not suppose a risk for the TOE, based on conformance to [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module].

For any other threat not included in the [ST], the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

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 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

Conceptually the TOE can be thought of as a collection of the following security services which the [ST] describes with increasing detail:

- 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.
- Windows OS Resume which reloads an image of the executing operating system from a hibernation file as part of resuming from a hibernated state.
- 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 IPsec module in user-mode.
- The IKE and AuthIP Keying Modules service which hosts the IKE and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec).
- The Remote Access Service device driver in the kernel, which is used primarily for ad hoc or user-defined VPN connections; known as the "RAS IPsec VPN" or "RAS VPN".
- The IPsec Policy Agent service which enforces IPsec policies.
- The Key Isolation Service which protects secret and private keys.
- 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.
- 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.
- The Windows Trusted Installer which installs updates to the Windows operating system.

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 (x64) or AMD (x64) along with peripherals for input/output (keyboard, mouse, display, and network).

The TOE was tested on the physical and virtual computer platforms listed in the Security Target, in the section 1.4.2.2.

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 in .pdf format:

- *Operational and Administrative Guidance* version 8.0, July 3, 2023 (along with all the documents web resources referenced therein).
    - *Hash SHA-256: F8F513302F551798D10438AB77F449F89169D9FA97EAEA500EA3BD86DF8932B6*

PRODUCT TESTING

The tests performed by the evaluator are based on the assurance activities defined for the ATE activity in the [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module] 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], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module] 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], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module], the vulnerability analysis scope has taken into account the public vulnerabilities affecting to all the operating system versions.

- The evaluator has performed a search of public sources to discover known vulnerabilities of the TOE.

- Using the obtained results, the evaluator has performed a sampling approach to verify if exists applicable public exploits for any of the identified public vulnerabilities and verify whether the security updates published by the vendor are effective.

- The evaluator has checked that all the public vulnerabilities published between October 18, 2022 to August 8, 2023 have been fixed by the vendor, since there are security updates available for the evaluated TOEs. The range of applicable security updates selected is based in the following criteria: the start date is the oldest release date of TOEs evaluated. In this case, Windows 11 22H2, which was released in October 18, 2022. For the final date, August 8, 2023 was selected, since this date is when the vendor provided the latest security updates for the TOEs during the evaluation period. The evaluator has ensured that for all the public vulnerabilities identified in vulnerability assessment report belonging to the period from June 8, 2021 to July 12, 2022, the vendor has published the corresponding update fixing the vulnerabilities.

- In order to demonstrate that the vendor was addressing correctly the issues, the evaluator executed in the TOE some public exploits and proof of concepts (PoC).

Therefore, the evaluator concluded that there were not exploitable vulnerabilities in the TOE operational environment according to the scope of this evaluation.

EVALUATED CONFIGURATION

The TOE under evaluation is composed of the following Windows Operating Systems (OS):

- Microsoft Windows 11 version 22H2 Enterprise edition
- Microsoft Windows 11 version 22H2 Pro edition
- Microsoft Windows 11 version 22H2 Education edition
- Microsoft Windows 11 version 22H2 IoT Enterprise edition
- Microsoft Windows 10 version 22H2 Pro edition
- Microsoft Windows 10 version 22H2 Enterprise edition
- Microsoft Windows Server 2022 Standard edition [8]
- Microsoft Windows Server 2022 Datacenter edition [9]
- Microsoft Windows Server Datacenter: Azure Edition [10]

[8] With December 13, 2022 cumulative update.

[9] With December 13, 2022 cumulative update.

- Microsoft Azure Stack HCIv2 version 22H2
- Microsoft Azure Stack Hub
- Microsoft Azure Stack Edge

TOE Versions:

- Microsoft Windows 11 build 10.0.22621.1 (also known as version 22H2)
- Microsoft Windows 10 build 10.0.19045.2006 (also known as version 22H2)
- Microsoft Windows Server 2022 10.0.20348.587
- Microsoft Windows Server Datacenter: Azure Edition build 10.0.20348.1006
- Microsoft Azure Stack HCIv2 version 10.0.20349.1129
- Microsoft Azure Stack Hub and Edge build 10.0.17784.1068

The following security updates must be applied for:

- Windows 11, Windows 10, Windows Server and Azure Stack: all critical updates as of June 1, 2023.

They have been tested in the following platforms:

- Microsoft Surface Laptop 5
- Microsoft Surface Pro 9
- Microsoft Surface Pro 9 5G (Qualcomm)
- Surface Studio 2+
- Microsoft Surface Laptop Go 2
- Microsoft Surface Go 3
- Microsoft Surface Laptop Studio
- Microsoft Surface Laptop 4 (AMD)
- Microsoft Surface Laptop 4 (Intel)
- Dell Latitude 7420
- Dell Latitude 9520
- HP EliteBook 840 G10
- Lenovo ThinkPad Z13 (AMD)
- Panasonic CF-33

[10] December 2022 virtual machine image from Azure Marketplace.

- Panasonic FZ-55 Toughbook
- Zebra L10ax / RTL 10C1
- Zebra ET80Z Tablet
- Microsoft Windows Server 2022 Hyper-V
- Microsoft Windows Server 2019 Hyper-V
- Dell PowerEdge R640
- Dell PowerEdge R6625
- Dell PowerEdge R760xp
- Dell PowerEdge R840
- HPE Edgeline EL8000 / ProLiant e910 Server Blade
- Voyager Klaas Telecom

The next list summarizes the combination between hardware platforms and operating system editions used for the testing:

- Microsoft Surface Laptop 5 with Windows 11 22H2 Enterprise (build 10.0.22621.1)
- Microsoft Surface Pro 9 Windows 10 22H2 Enterprise (build 10.0.19045.2)
- Dell PowerEdge R6625 with Windows Server 2022 Datacenter (21H2, build 10.0.20348.587)
- Dell PowerEdge R6625 with Windows Server Azure Datacenter Edition (21H2, build 10.0.20348.1006)
- Dell PowerEdge R6625 with Azure Stack HCIv2 version 21H2 (build 10.0.20349.1129)
- Dell PowerEdge R6625 with Azure Stack Hub (20H2, build 10.0.17784.1068)
- Dell PowerEdge R6625 with Azure Stack Edge (20H2, build 10.0.17784.1068)
- Microsoft Windows Server 2022 Hyper-V with Windows Azure Datacenter edition (21H2, build 20348.1006)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (10.0.19045.2)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (21H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- HPE Edgeline EL 8000 with Windows Server 2022 Standard edition (21H2, build 10.0.20348.587)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 21H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (21H2, build 10.0.20348.587)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HP EliteBook 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad T14 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2)

EVALUATION RESULTS

The TOE has been evaluated against the Security Target:

- Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge Security Target (version 0.04, 03/07/2023).

All the assurance components defined in the [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module] and [Bluetooth_Module] have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the assurances packages defined, according to the Common Criteria v3.1 release 5, the [GPOSPP], [WLAN_Client_Module], [VPN_Client_Module], [Bluetooth_Module] 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.

COMMENTS & RECOMMENDATIONS FROM THE CERTIFIER

Considering the obtained evidences during the instruction of the certification request of the product Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge, 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

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] Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 22, 2019

[WLAN_Client_Module] PP-Module for WLAN Clients, version 1.0, March 31, 2022

[VPN_Client_Module] PP-Module for Virtual Private Network (VPN) Clients, version 2.4, March 31, 2022

[Bluetooth_Module] PP-Module for Bluetooth, version 1.0, April 15, 2021

[ST] Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge Security Target (version 0.04, 03/07/2023).

SECURITY TARGET

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 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge Security Target (version 0.04, 03/07/2023).
    - Hash SHA-256: 4272FD4974EA5D611E3B3525E1673F8EDCC237D640BF75439A865EA5BF84A3A5

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 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge Security Target (version 0.04, 03/07/2023).
    - Hash SHA-256: 690CB9452C249E2109EC96F0C3CFEF85C52472699F8412B78655DF4EE7057C4B

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.

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

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.