Reference: 2018-54-INF-3132-v1
Target: Público
Date: 11.06.2020

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

CERTIFICATION REPORT

Dossier #	**2018-54**
TOE	**TZ v2.4**
Applicant	**B82193210 - Tecnobit S.L.U.**
References	

[EXT-4404] Certification request

[EXT-5898] Evaluation Technical Report vM0

Certification report of the product TZ v2.4, as requested in [EXT-4404] dated 20/11/2018, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5898] received on 24/04/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product TZ v2.4.

The Target of Evaluation (TOE) is a cryptographic module that secures communications between different deployed units for a mission and it implements endorsed cryptographic security functions to protect the confidentiality of user data according to a security policy of an IT system.

The TOE uses, manages and protects the cryptographic keys and missions for these endorsed cryptographic security functions.

Developer/manufacturer: Tecnobit S.L.U.

Sponsor: Tecnobit S.L.U..

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

ITSEF: Applus Laboratories

Security Target: TZ Security Target, Version 008, February 28, 2020.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2+ (ALC_FLR.1)

Evaluation end date: 25/05/2020

Expiration Date[1]: 12/06/2025

All the assurance components required by the evaluation level EAL2+ (ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2+ (ALC_FLR.1), as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product TZ v2.4, a positive resolution is proposed.

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

TOE SUMMARY

TZ is a portable, light and very small size cryptographic module for protecting data communications.

The Target of Evaluation (TOE) is a cryptographic module that secures communications between different deployed units for a mission and it also implements endorsed cryptographic security functions to protect the confidentiality of user data according to a security policy of an IT system.

The TOE uses, manages and protects the cryptographic keys and missions for these endorsed cryptographic security functions.

A mission consists in a set of TOE devices, configured within a data transmission mode and how that transmission is cryptographically protected.

Cryptographic keys involved in TOE communication provide integrity and confidentiality protection during data transmission.

TOE protects communication data as follows:

- Data: Information is secured following the IPSec protocol according to [RFC4301]. Both, transport and tunnel IPSec modes are able to be configured.

TOE is composed by two physical isolated zones: the red one encrypts and decrypts data sent or to be received by the end user; and the black one manages the delivery of these protected data to one or several endpoints through communication channel.

Devices used by the end user such as computers, which create and process clear data, are connected to the red zone of the TOE.

The media devices that transmit the protected data, such us Tactical IP radios (HARRIS 7800, PR4G, Spearnet, etc.) or network devices such as switches, are connected to the black zone of the TOE.

TOE has two working configurations managed by the role that the user using TOE owns. These roles can be: operator (S.OPERATOR) or management role (S.MANAGEMENT). When the user using the TOE is an operator role, TOE is able to transmit data in several modes for protecting data information:

- Unicast: one target communication
- Multicast: several targets communication

Management role is capable of getting audit files and to update software, cryptographic keys and missions.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE: Security Target Evaluation	ASE_INT.1. ST Introduction ASE.CCL.1. Conformance claims ASE_SPD.1. Security problem definition ASE_OBJ.2. Security objectives ASE_ECD.1. Extended component definition ASE_REQ.2. Derived security requirements ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture ADV_FSP.2. Functional specification ADV_TDS.1. TOE design
AGD: Guidance documents	AGD_OPE.1. Operational user guidance AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities ALC_CMS.2. CM Scope ALC_DEL.1. Delivery ALC_FLR.1. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage ATE_FUN.1. Functional tests ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS	
FAU_GEN.1	FMT_MOF.1/TrustedUpdate
FAU_SAR.1	FMT_MSA.1/CONFIG
FAU_STG.2	FMT_MSA.1/RED-BLACK
FAU_STG.4	FMT_MSA.1/SERVICES

FCS_CKM.2	FMT_MSA.3/CONFIG
FCS_CKM.4	FMT_MSA.3/RED-BLACK
FCS_COP.1	FMT_MSA.3/SERVICES
FDP_ACC.2/CONFIG	FMT_MTD.1
FDP_ACC.2/SERVICES	FMT_SMF.1
FDP_ACF.1/CONFIG	FMT_SMR.1
FDP_ACF.1/SERVICES	FPT_FLS.1
FDP_IFC.2	FPT_PHP.1
FDP_IFF.1	FPT_PHP.3
FDP_ITC.1	FPT_PHP.4
FDP_ITC.2	FPT_STM.1
FDP_UCT.1	FPT_TDC.1
FDP_UIT.1	FPT_TOS.1
FIA_509.1	FPT_TST.2
FIA_509.2	FTP_ITC.1
FIA_AFL.1	FTP_ITC.2
FIA_UAU.1	FTP_TRP.1
FMT_MOF.1/AdminAct	

IDENTIFICATION

Product: TZ v2.4

Security Target: TZ Security Target, Version 008, February 28, 2020.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2+ (ALC_FLR.1).

SECURITY POLICIES

The use of the product TZ v2.4 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.4 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.5 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.3 (Threats) do not suppose a risk for the product TZ v2.4, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

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 detailed in [ST], chapter 4.2 (Security Objectives for the Operational Environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The security functions provided by this TOE are:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

PHYSICAL ARCHITECTURE

The physical boundary of the TOE is the TZ device.

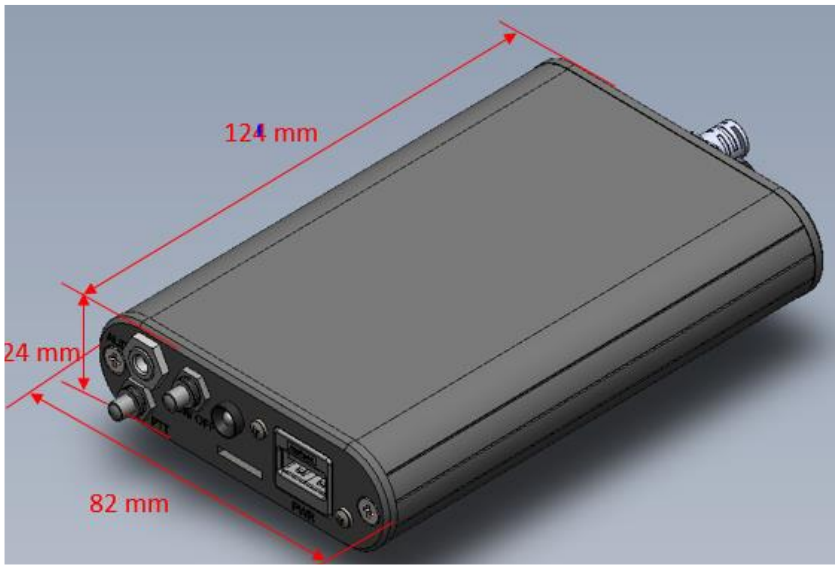

Figure 1. TZ device

DOCUMENTS

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

DOCUMENT	FORMAT
T0074000ILS008-MT-507 **Manual de Empleo y Mantenimiento de 1er Escalón** **Version 008**	PDF
T90421000CFG008 **Configuración del TZ** **Version 008**	PDF
T90421000ERR001 **Mensajes de Error** **Date 06/06/2019**	XLS
T90421000PRE009 **Manual de configuración del entorno operacional** **Version 008**	PDF

PRODUCT TESTING

The developer has executed test for all the security functions, prioritizing the functionality of the security measures of the TOE that have a great impact in the overall security of the TSF. All the tests have been performed by the developer in its premises, with a satisfactory result.

In addition, to verify the results of the developer tests and to gain more assurance of the proper implementation of the TOE, the evaluator has also repeated all the developer functional tests in the developer premises, verifying that the obtained results are consistent with the results obtained by the developer.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic has been successful in the TOE's operational environment as defined in the security target when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined as a set of hardware, software and firmware contained within a secured boundary. The boundary provides physical countermeasures to protect stored data from information disclosures or integrity breaches.

The evaluated configuration setup where it has been evaluated comprises of:

- TZ v2.4 devices.
- A Management Centre (CMAP) laptop.
- A switch to interconnect CMAP to the TZ devices.
- A virtualized workstation to capture all the traffic between CMAP and TZ devices.
- Virtualized workstations acting as information providers to TZ devices.

The TOE also includes the documents identified in section "DOCUMENTS" of this certification report that shall be distributed and made available together to the users of the evaluated version.

EVALUATION RESULTS

The product TZ v2.4 has been evaluated against the Security Target: TZ Security Target, Version 008, February 28, 2020.

All the assurance components required by the evaluation level EAL2+ (ALC_FLR.1) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**"

VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2+ (ALC_FLR.1), as defined by the Common Criteria v3.1 release 5 and the Common Methodology for Information Technology Security Evaluation version 3.1 release 5..

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

There is no additional recommendation from the evaluation team in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

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

The certifier strongly recommends to the TOE consumer to strictly follow the guidance that can be found on section DOCUMENTS of this certification report as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

The certifier remarks the following point that should be observed by potential consumers:

- The two anti-tampering labels leave traces when they are removed so it is very important to look for any trace of labels manipulation or any evidence of labels removal before to operate the TOE.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IPSec Internet Protocol security

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.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: TZ Security Target, Version 008, February 28, 2020.

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.

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.