Reference: 2017-25-INF-2751-v1
Target: Público
Date: 21.05.2019

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

CERTIFICATION REPORT

Dossier #	**2017-25**
TOE	**Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2**
Applicant	**1737565-0 - Bittium Wireless Oy**
References	
	[EXT-4852] ETR v2.0

Certification report of the product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2, as requested in [EXT-3462] dated 24/04/2019, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4852] received on 21/03/2019.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2.

The device is a Dual OS mobile handset running with two separate operating systems. Operating systems are normal operating system which is regular Android OS and Bittium Secure OS Secure operating system which base on Android 5.1.1 operating system with Bittium modifications. Only one operating system can be active at the time. Switching between two operating systems is done using menu under power key.

Developer/manufacturer: Bittium Wireless Oy

Sponsor: Bittium Wireless Oy.

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

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r4 - EAL2.

Evaluation end date: 21/03/2019.

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 r4 and the CEM v3.1 r4.

Considering the obtained evidences during the instruction of the certification request of the product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2, a positive resolution is proposed.

TOE SUMMARY

The TOE is a mobile handset running with Bittium Secure OS Secure operating system, which base on Android 5.1.1 operating system with Bittium modifications. Officials who are communicating sensitive information are intended to use device as reliable and secure mobile communication device for governmental.

TOE can be used, for example for voice and data communications applications using a trusted channel. The trusted channel is a VPN providing confidentially, integrity and end-points

authenticity. The TOE connects to the internet using either a mobile network or Wi-Fi networks, but in either case, the communication with trusted external entities is through trusted channels so that the IP traffic is sent and/or received using the trusted channel.

TOE also protects user sensitive data, protects from unauthorized access and external tampering.

Major security features of the TOE are:

- Security Audit – collects and stores security information of the TOE's to the data partition.
- Cryptographic Support – provides cryptographic operations. These functionalities are used for data and communication protection and integrity verification.
- User data protection – performs user data communication channel protection using VPN. Protects user data and corresponding keys from unauthorized access and in case of security integrity violation.
- Identification and authentication – perform user authorization and identification and restrict usage accordance security policies.
- Security Management – allows user manage security settings of the TOE, download trusted applications and perform emergency procedures in case of security violation. Allows MDM to configure security features of the TOE via secure connection.
- Protection of the TOE Security Functions – TOE protection is performed during boot and run time. TOE protection is performed using secure boot and integrity checking. Tamper handling protects TOE from external attacks and from OS manipulating. Trusted SW update includes protection of FOTA update and application updates.
- TOE Access – protect device by handling use session with different protection mechanisms. Such mechanisms are like two factor authentication (i.e. user credentials and HOTP from NFC dongle to login), session restrictions and timings.
- Trusted path/channels – Provide trusted communication channel for IP traffic using TLS (between TOE and MDM server) and IPsec (for VPN gateway).

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria v3.1 r4.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – simple
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 r4:

TOE Security Functional Requirements	**Description**
FAU_AUD_EXT.1	Audit data generation
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic Key Generation
FCS_COP.1	Cryptographic Operation
FCS_RBG_EXT.1	Extended – Random Bit Generation
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_DSK_EXT.1	Extended – Protection of Data on Disk
FDP_ZER_EXT.1	Extended – Zeroization
FIA_UAU.2	User Authentication before any action
FIA_AFL.1	Authentication failure handling
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FPT_FLS.1	Failure with preservation of secure state
FPT_SBT_EXT.1	Extended – Secure Boot and Operation continuity
FPT_STM.1	Reliable time stamps
FPT_TST_EXT.2	Extended – Integrity Test
FPT_TUD_EXT.1	Extended – Trusted Update
FPT_PHY_EXT.1	Extended – Passive detection of physical attack
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.2	User-initiated locking
FTP_ITC.1/VPN-tunnel	Inter-TSF Trusted Channel (Application communications)
FTP_ITC.1/REM-ADM	Inter-TSF Trusted Channel (remote administration)
FTP_ITC.1/AUDIT	Inter-TSF Trusted Channel

IDENTIFICATION

Product: Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2

Security Target: Bittium Tough Mobile C Security Target, version 4.0.2, 20/02/2019.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r4 EAL2.

SECURITY POLICIES

The use of the product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2 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 4.2 (Organisational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 4.3 (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 4.1 (Threats) do not suppose a risk for the product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2, although the agents implementing attacks have the attack potential according to the Basic of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, 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 5.2 (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 logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE is described in chapters 7 Security Requirements and in chapter 8 TOE Summary Specification in [ST].

The TOE includes the following functional sections:

- Security Audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Security updates

PHYSICAL ARCHITECTURE

TOE provides wireless connectivity including secure VPN connectivity. TOE could be used as a mobile device within an enterprise environment where the configuration of the device is managed through a compliant MDM.

MDM environment (i.e. Bittium Secure Suite and VPN Gateway) are out of the scope of the TOE, but it is used to support evaluation.

TOE is delivered in regular sales package including:

- Bittium Tough Mobile C HW and Bittium Secure OS Secure operating system
- Bittium Secure OS Secure operating system SW version is S2_BSOS_1.1.5C_MR22_sapphire2
- NFC dongle for two phase authentication
- Tough Mobile Quick start guide.

Note: NFC dongle and the Tough Mobile Quick start guide are part of the delivery but they are NOT part of the TOE on the common criteria evaluation.

The documentation listed in *DOCUMENTS* section of this Certification Report provide instructions for enterprise author how to perform initial provisioning and configuration of TOE via MDM, user and MDM administrator instructions of operations within enterprise environment.

DOCUMENTS

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

- Tough Mobile C Preparative procedures, version 2.0.0. Document number [121436EDC0162]
- Tough Mobile C Operational User Guidance, version 4.0.0. Document number [121436EDC0161].

PRODUCT TESTING

The developer has executed tests for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

EVALUATED CONFIGURATION

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals (see *DOCUMENTS* section of this certification report.

EVALUATION RESULTS

The product Bittium Tough Mobile C (BTMC). HW version: 9304809A03. SW version: Android 5.1.1. Kernel version: 3.4.0. Build: S2_BSOS_1.1.5C_MR22_sapphire2 has been evaluated against the Security Target: Bittium Tough Mobile C Security Target, version 4.0.2, 20/02/2019.

All the assurance components required by the evaluation level EAL2 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 evaluation level EAL2, as defined by the Common Criteria v3.1 r4 and the CEM v3.1 r4.

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.

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

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

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, September 2012.

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

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

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

[ST] Bittium Tough Mobile C Security Target, version 4.0.2, 20/02/2019.

SECURITY TARGET

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

- Bittium Tough Mobile C Security Target, version 4.0.2, 20/02/2019.

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:

- Bittium Tough Mobile C Security Target Lite, version 1.0.1, 17/05/2019.

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.