Reference: 2023-16-INF-4388- v1
Target: Pública
Date: 12.11.2024

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-16**
TOE	**Kaytus Server Baseboard Management Controller 1.49.07**
Applicant	**202237717R - Kaytus Systems PTE. Ltd.**
References	

[EXT-8605] 2023-05-19_2023-XX_solicitud_certificacion

[EXT-9164] 2024-07-19_2023-16_ETR_v1.3

Certification report of the product Kaytus Server Baseboard Management Controller 1.49.07, as requested in [EXT-8605] dated 19/05/2023, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9164] received on 19/07/2024.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 6
SECURITY POLICIES 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY 6
ARCHITECTURE 7
LOGICAL ARCHITECTURE 7
PHYSICAL ARCHITECTURE 7
DOCUMENTS 8
PRODUCT TESTING 9
EVALUATED CONFIGURATION 9
EVALUATION RESULTS 10
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 10
CERTIFIER RECOMMENDATIONS 10
GLOSSARY 10
BIBLIOGRAPHY 11
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 11
RECOGNITION AGREEMENTS 12
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 12
International Recognition of CC – Certificates (CCRA) 12

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Kaytus Server Baseboard Management Controller 1.49.07.

The TOE is an out-of-band management firmware running in a System-on-Chip microprocessor located in an KAYTUS V2 Server (hereinafter referred to as "host") that provides remote management capabilities, including hardware asset management, health status monitoring, fault analysis and remote control.

Developer/manufacturer: Kaytus Systems PTE. Ltd.

Sponsor: Kaytus Systems PTE. Ltd..

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

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

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL2 + ALC_FLR.2.

Evaluation end date: 28/08/2024

Expiration Date[1]: 08/11/2029

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) 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 EAL2 + ALC_FLR.2, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidence during the instruction of the certification request of the product Kaytus Server Baseboard Management Controller 1.49.07, a positive resolution is proposed.

TOE SUMMARY

The TOE runs on an integrated System-on-Chip microprocessor for the remote monitoring/control system. The microprocessor co-exists on the system board with the managed server. The TOE functions independently of the server’s state of operation, and the state of the server itself is transmitted to microprocessor through the internal hardware interface.

The TOE can be used in the following situations:

[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.

- The operation and health status of key hardware components in the host can be monitored through the TOE GUI in real time.
- Hosts can be remotely managed through TOE, for startup, shutdown, firmware deployment, and update operations.
- Automated large scale multi-server maintenance can be achieved utilizing Redfish API capability offered from the TOE.

Remote administration communication is protected using cryptography. The TOE offers WebUI (Web browser) and Redfish API management interfaces protected by HTTPS/TLS v1.2 and v1.3, and command line console access (SMASH CLP CLI) protected by SSHv2. The remote management functionality provided by the TOE is access controlled and administrator actions are audited.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidence required by the additional component ALC_FLR.2 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.2
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

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

CLASS	IDENTIFIER
Security Audit (FAU)	FAU_GEN.1
	FAU_GEN.2
	FAU_SAR.1
	FAU_SAR.2
	FAU_SAR.3
	FAU_STG.1
	FAU_STG.3
Cryptographic Support (FCS)	FCS_COP.1
User Data Protection (FDP)	FDP_ACC.1
	FDP_ACF.1
	FDP_UCT.1
Identification and Authentication (FIA)	FIA_ATD.1
	FIA_SOS.1
	FIA_UAU.2
	FIA_UID.2
Security Management (FMT)	FMT_MSA.1
	FMT_MSA.3
	FMT_SMF.1
	FMT_SMR.1
Protection of the TSF (FPT)	FPT_STM.1
	FPT_RCV.3
	FPT_FLS.1
TOE Access (FTA)	FTA_SSL.1
	FTA_SSL.3
	FTA_SSL.4
	FTA_TSE.1
Trusted path/channels (FTP)	FTP_TRP.1

IDENTIFICATION

Product: Kaytus Server Baseboard Management Controller 1.49.07

Security Target: KAYTUS Server Baseboard Management Controller Security Target, version 0.9 (17 July 2024).

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL2 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Kaytus Server Baseboard Management Controller 1.49.07 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.2 ("*Organizational Security Policies*").

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 ("*Assumptions*").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Kaytus Server Baseboard Management Controller 1.49.07, although the agents implementing attacks have the attack potential according to the Basic of EAL2 + ALC_FLR.2 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.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 ("*Threats*").

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 those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("*Security Objectives for the operational Environment*").

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical boundary of the TOE may be broken down by the security functions described below:

- Security Audit. Audit entries are generated for security related events. The audit logs are protected from unauthorized modification and deletion and may be reviewed by authorized administrators. Time stamp information is provided to support auditing.
- Cryptographic Support. Cryptographic functionality is provided to allow the communications links between the TOE and its remote administrators to be protected. Digital signature algorithms are also implemented for firmware integrity checks.
- User Data Protection. The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE.
- Identification and Authentication. Users must be identified and authenticated prior to gaining access to the TOE.
- Security Management. The TOE provides management capabilities via a Web-Based GUI, accessed via HTTPS (TLSv1.2 and TLSv1.3). Management functions allow the administrators to configure system and network settings, configure users and roles, and manage the host. The TOE can also be managed over SSHv2 using the SMASH CLP CLI or the Redfish API using HTTPS. (TLSv1.2 and v1.3).
- Protection of the TSF. The TOE provides time stamps for the audit records and its own use. The TOE implements actions after failures in the firmware integrity check.
- TOA Access. TOE can lock an interactive session and allow user-initiated termination of the user's own interactive session. A TOE administrator may configure to deny session establishment.
- Trusted Path/Channel. The communications links between the TOE and its remote administrators are protected using HTTPS (TLSv1.2 and v1.3) and SSHv2.

PHYSICAL ARCHITECTURE

The chassis contains the Host hardware, the microprocessor and the firmware (the TOE) that is shipped directly to customers. The TOE is pre-installed in KAYTUS premises and delivered to

customers after the installation. So, the TOE is already installed when the customers receive the chassis.

Alternatively, the evaluated version of the firmware and guidance documentation may be downloaded from the support site: https://www.kaytus.com/. From there select Support -> Documentation for the documentation or Support -> Drivers for the firmware, then select the desired KAYTUS server model.

TOE	Version	Format	SHA256 digest
KAYTUS Server Baseboard Management Controller (ISBMC_EagleStream_1.49.07_Standard_20240416.hpm)	1.49.07	HPM	3a4959015b1495b67cba6f2c873a9952a7b3ef51ffb8562dd0aa2bde98b15556

DOCUMENTS

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

Document	Version	Format	SHA256 digest
Kaytus Server BMC User Manual for KAYTUS V2 Series Servers_Powered by Intel Processors	1.4	PDF	5d4d59101807ec2809ece7f919d35f12b3d209d45fbca4be2e6b2124fd63d197
Kaytus Server BMC Configuration Manual for KAYTUS V2 Series Servers_Powered by Intel Processors	1.2	PDF	f20391d5a67d96a4c75f7ffcd530d493783278084d6a764bcf9b9fcb98074ad5
Kaytus Server BMC Update Manual for KAYTUS V2 Series Servers_Powered by Intel Processors	1.2	PDF	685ee0b4e1ab7f043f396bebeb40a776a54ae0e5949093959ddf043bd966066d
Redfish User Manual for KAYTUS V2 Series Servers_Powered by Intel Processors	1.2	PDF	9d989983ce90dc9de7e5e48059ccabdd7fa7730d4d394f15ac1109dc3d6242c2
KAYTUS Server Baseboard Management Controller Common Criteria Guidance Supplement	0.9	PDF	0ad438213e7edd22f9698a47bb9354baf80fd81a83f15d45fb9120c6916231a4

PRODUCT TESTING

The developer has executed tests for all the TSFIs. 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 has been identified and 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.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises in the testing platform implemented in the evaluation facility.

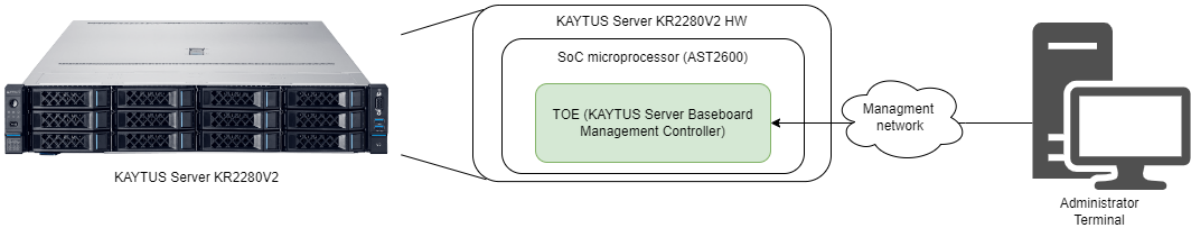
In addition, the lab has devised a test for each of the TSFi of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The board where the TOE is running is an advanced RISC1 machine (ARM) and uses the AST2600 server management processor. The hardware (KAYTUS V2 Server) where the microprocessor is installed is the item placed at the left of the figure below.

An administrator terminal (which is a Windows 10 x64 general purpose computer) is required to manage the TOE.



The administrator terminal is used to access the TOE's out-of-band management module through the management network using a web browser, Redfish API client, or SSH client. The following third-party software is required when interfacing with the TOE

- Java Runtime Environment: OpenJDK 1.8+

- SSH Client: PuTTY Version 0.76+
- Redfish API Client: Postman Version 7+
- Web browsers: Google Chrome 58+

EVALUATION RESULTS

The product Kaytus Server Baseboard Management Controller 1.49.07 has been evaluated against the Security Target KAYTUS Server Baseboard Management Controller Security Target, version 0.9 (17 July 2024).

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 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 evaluation level EAL2 + ALC_FLR.2, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

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 and the cumulative update 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.
- 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 evidence during the instruction of the certification request of the product Kaytus Server Baseboard Management Controller 1.49.07, 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.

[ST] KAYTUS Server Baseboard Management Controller Security Target, version 0.9 (17 July 2024).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

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

- KAYTUS Server Baseboard Management Controller Security Target, version 0.9 (17 July 2024).

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.eu.

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 CCRA for all assurance components selected.