Reference: 2025-12-INF-4669- v1
Target: Limitada al expediente
Date: 27.01.2026

Created by: I008
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2025-12**
TOE	**KAYTUS Server Baseboard Management Controller version 4.04.04**
Applicant	**202237717R - Kaytus Systems PTE. Ltd.**
References	

[EXT-9463] 20250205_2025-12_solicitud_certificacion

[EXT-9893] 2025-09-24_2025-12_ETR_v1.2

Certification report of the product KAYTUS Server Baseboard Management Controller version 4.04.04, as requested in [EXT-9463] dated 05/02/2025, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9893] received on 24/09/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KAYTUS Server Baseboard Management Controller version 4.04.04.

The KAYTUS Server Baseboard Management Controller 4.04.04 is an out-of-band management firmware running on a System-on-Chip microprocessor located in a KAYTUS V3 server, which provides remote management capabilities including hardware asset management, product 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.

Evaluation Level: Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022, EAL 2 + ALC_FLR.

Evaluation end date: 04/11/2025.

Expiration Date[1]: 18/12/2030

All the assurance components required by the evaluation level EAL 2 + ALC_FLR 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 EAL 2 + ALC_FLR, as defined by the CC:2022 r1 and the CEM:2022.

Considering the obtained evidences during the instruction of the certification request of the product KAYTUS Server Baseboard Management Controller version 4.04.04, a positive resolution is proposed.

TOE SUMMARY

The KAYTUS Server Baseboard Management Controller (BMC) is an out-of-band management firmware running on a System-on-Chip (SoC) microprocessor integrated into KAYTUS V3 servers. Its purpose is to provide remote server management capabilities, such as hardware administration, status monitoring, fault analysis, and remote control, operating independently from the main system.

[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 TOE allows:

- Real-time monitoring of the server hardware status and operation through a graphical interface.
- Remote management of startup, shutdown, firmware deployment, and updates.
- Automated large-scale maintenance using the Redfish API.

Remote administration communications are cryptographically protected using HTTPS/TLS v1.2 and v1.3 and SSHv2. Access is controlled, and administrator actions are audited.

The main security functionalities of the TOE include:

- Auditing: generation and secure storage of logs with timestamps and review capability.
- Cryptographic operations: protection of communications and firmware integrity verification using digital signatures.
- Access control: enforcement of role-based access policies.
- Identification and authentication: user validation before granting access.
- Security management: administrative functions available according to the user's role, through the web interface (HTTPS), CLI (SSHv2), or Redfish API.
- TSF protection: recovery after failures, firmware integrity verification, and security actions following errors.
- Session management: establishment, locking, and secure termination of sessions.
- Trusted path/channel: secure communications ensuring confidentiality, integrity, and authentication.

In summary, the TOE provides a secure remote management platform that protects communications, enforces access control, maintains firmware integrity, and ensures full traceability of administrative actions within the KAYTUS V3 server environment.

SECURITY ASSURANCE REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v2022 r1.

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)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)

Development (ADV)	Security-enforcing functional specification (ADV_FSP.2)
	Security Architecture Description (ADV_ARC.1)
	Basic Design (ADV_TDS.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Lifecycle support (ALC)	Use of a CM system (ALC_CMC.2)
	Parts of the TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
	Flaw Reporting Procedures (ALC_FLR.2)
Tests (ATE)	Independent Testing – sample (ATE_IND.2)
	Functional testing (ATE_FUN.1)
	Evidence of coverage (ATE_COV.1)
Vulnerability evaluation (AVA)	Vulnerability Analysis (AVA_VAN.2)

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v2022 r1.

Requirement Class	Security Functional Requirement
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_UID.2
	FIA_UAU.2
	FIA_ATD.1
	FIA_SOS.1

Requirement Class	Security Functional Requirement
Security Management (FMT)	FMT_SMF.1
	FMT_SMR.1
	FMT_MSA.1
	FMT_MSA.3
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 Paths (FTP)	FTP_TRP.1

IDENTIFICATION

Product: KAYTUS Server Baseboard Management Controller version 4.04.04

Security Target: KAYTUS Server Baseboard Management Controller Security Target, v.1.1, 30/04/2025.

Evaluation Level: Common Criteria version 2022 release 1. EAL 2 + ALC_FLR

SECURITY POLICIES

The use of the product KAYTUS Server Baseboard Management Controller version 4.04.04 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 version 4.04.04, 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.

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 TOE supports a large range of security functionalities to facilitate various IT systems integration, yet not all these functionalities are in the scope of the ST. As some of them are obsolete and may not be secure enough, or rarely used in most scenarios, they are preserved for legacy purposes on old IT systems which still did not migrate to state-of-art technologies. Nonetheless, they shall not be enabled in this certified configuration. The next table shows the list of secure functionalities/protocols and the ones that should be enabled in the evaluated configuration of the TOE.

Security Functional Specification		Enabled in TOE
TOE management	WebUI (Web User Interface)	Y
	SMASH CLP CLI (Command Line Interface)	Y
	Redfish API	Y
	IPMI	N
	SNMP	N
User	Password	Y

Security Functional Specification		Enabled in TOE
authentication mechanism	LDAP/AD server	N
	Kerberos server	N
	Two Factor Authentication (by certificates)	Y
Security protocols	TLS1.3/1.2	Y
	TLS1.1/1.0	N
	SSH V2	Y

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
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.
TOE 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 (BMC_B_BirchStream_4.04.04_StandardK_KAYTUS_20250427_enc)	4.04.04	HPM	670D3A4325CAFBEF902D648752A8067BE8349F78A6B3B2AFDCE3B585

The TOE includes the following guidance documentation, which can be downloaded by the user from the KAYTUS website:

Document	Version	Format	SHA256 digest
BMC User Manual for KAYTUS V3 Series Servers V1.2	1.2	PDF	E9BA4560BD06DF6DFC1FA7CBAE49B55C597884206DAA1088F102DF25064D01F
BMC Configuration Manual for KAYTUS V3 Series Servers V1.1	1.1	PDF	530AC56206779F6AC759E6D89694379D41B820A1C97A4D82041C
BMC Update Manual for KAYTUS V3 Series Servers V1.3	1.3	PDF	F64A201285E4397ED5466CF28EBB46F6557E5CBA0DEA42A0A7092075
Redfish User Manual for KAYTUS V3 Series Servers V1.1	1.1	PDF	55DE5FF6D6C38ABA664AC6153B38B79103996E67C501A3C91D80AE2949896
Kaytus Server BMC Common Criteria Guidance Supplement V1.3	1.3	PDF	20CC3F66E57D2D684350F03DA05943DA15130FFAE7CAB814DBF15083139C58

DOCUMENTS

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

- [GS13] KAYTUS Server Baseboard Management Controller Common Criteria Guidance Supplement, v.1.3, 04/08/2025
- [UPM13] BMC Update Manual for KAYTUS V3 Series Servers. V.1.3, 22/05/2025
- [UM12] BMC User Manual for KAYTUS V3 Series Servers, v.1.2, 07/03/2025
- [ST11] KAYTUS Server Baseboard Management Controller Security Target, v.1.1, 30/04/2025

PRODUCT TESTING

The developer has executed test 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.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated about 25% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function 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 evaluated configuration is shown in Figure 1 - Evaluated Configuration and consists of the TOE, the microprocessor and the Host hardware.

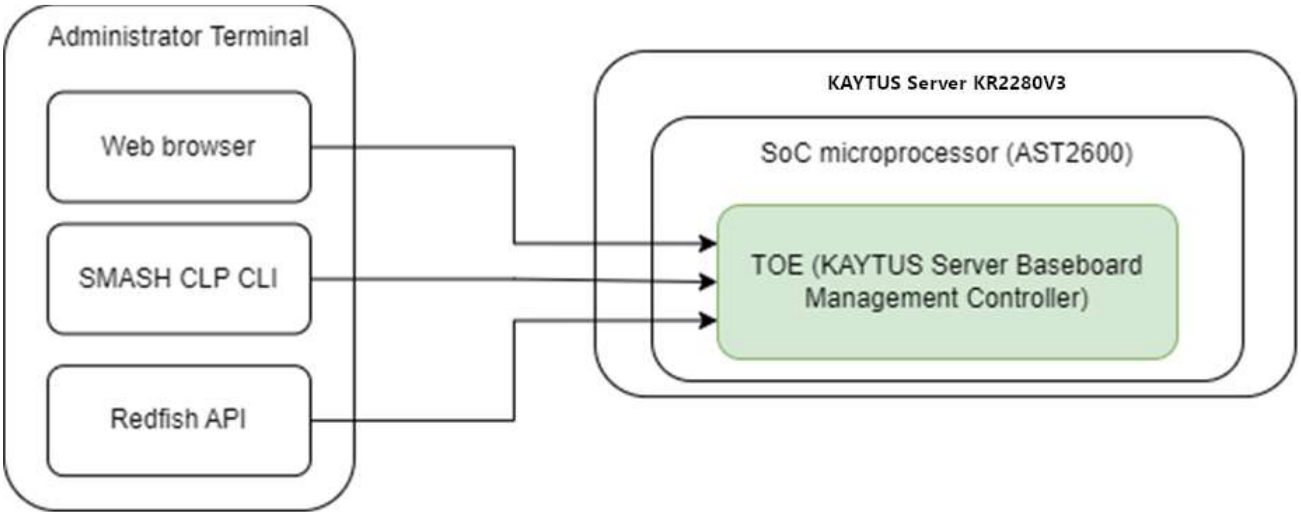

Figure 1 - Evaluated Configuration

The microprocessor with the TOE is preinstalled within the Host's chassis. The microprocessor hardware is an advanced RISC1 machine (ARM) and uses the AST2600 server management processor. The microprocessor is managed through external network interfaces, and it communicates with the host through internal circuit board connections.

EVALUATION RESULTS

The product KAYTUS Server Baseboard Management Controller version 4.04.04 has been evaluated against the Security Target KAYTUS Server Baseboard Management Controller Security Target, v.1.1, 30/04/2025.

All the assurance components defined in the Security Target and in Common Criteria version 2022 revision 1, and 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 v2022, revision 1.

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 TOE user must read and understand the user guides in order to operate the TOE properly in accordance with the Security Target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product KAYTUS Server Baseboard Management Controller version 4.04.04, 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
ST	Security Target
OE	Operational Environment

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC2022p1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model Revision 1, November 2022.
[CC2022p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Revision 1, November 2022.
[CC2022p3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components Revision 1, November 2022.
[CC2022p4]	Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities Revision 1, November 2022.
[CC2022p5]	Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements Revision 1, November 2022.

[CEM2022]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 2022 Revision 1, November 2022.
[CCAdd]	CC and CEM addenda. Exact Conformance, Selection-Based SFRs, Optional SFRs, version 0.5, May 2017.
[ST11]	KAYTUS Server Baseboard Management Controller Security Target, v.1.1, 30/04/2025

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.