



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR **CYBER SECURITY**

COMMON CRITERIA CERTIFICATION REPORT

KAYTUS Server Baseboard Management Controller 7.11.00

8 January 2025

597-EWA

V1.1

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)



OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).



TABLE OF CONTENTS

EXECUTIVE SUMMARY	6
1 Identification of Target of Evaluation	7
1.1 Common Criteria Conformance	7
1.2 TOE Description.....	7
1.3 TOE Architecture	7
2 Security Policy	8
2.1 Cryptographic Functionality	8
3 Assumptions and Clarification of Scope	9
3.1 Usage and Environmental Assumptions.....	9
3.2 Clarification of Scope	9
4 Evaluated Configuration	10
4.1 Documentation.....	10
5 Evaluation Analysis Activities	11
5.1 Development	11
5.2 Guidance Documents.....	11
5.3 Life-Cycle Support	11
6 Testing Activities	12
6.1 Assessment of Developer tests.....	12
6.2 Conduct of Testing	12
6.3 Independent Testing.....	12
6.3.1 Independent Testing Results	12
6.4 Vulnerability Analysis	13
6.4.1 Vulnerability Analysis Results.....	13
7 Results of the Evaluation	14
7.1 Recommendations/Comments	14
8 Supporting Content	15
8.1 List of Abbreviations.....	15



8.2 References.....15

LIST OF FIGURES

Figure 1: TOE Architecture..... 7

LIST OF TABLES

Table 1: TOE Identification 7

Table 2: Cryptographic Implementation(s)..... 8



EXECUTIVE SUMMARY

KAYTUS Server Baseboard Management Controller 7.11.00 (hereafter referred to as the Target of Evaluation, or TOE), from **KAYTUS SYSTEMS PTE. LTD.**, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **8 January 2025** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	KAYTUS Server Baseboard Management Controller 7.11.00
Developer	KAYTUS SYSTEMS PTE. LTD.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL2+ with ALC_FLR.2

1.2 TOE DESCRIPTION

The TOE, KAYTUS Server Baseboard Management Controller 7.11.00, is an embedded system located in an KAYTUS M6 Server that provides remote management capabilities, including hardware asset management, health status monitoring, fault analysis and remote control. The TOE co-exists on the system board with the managed server but functions independently of the server's state of operation and communicates with the server through the internal hardware interface. Externally, the TOE offers WEB GUI and Redfish API management interfaces and command line console access (SMASH CLP CLI) via a dedicated management port.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

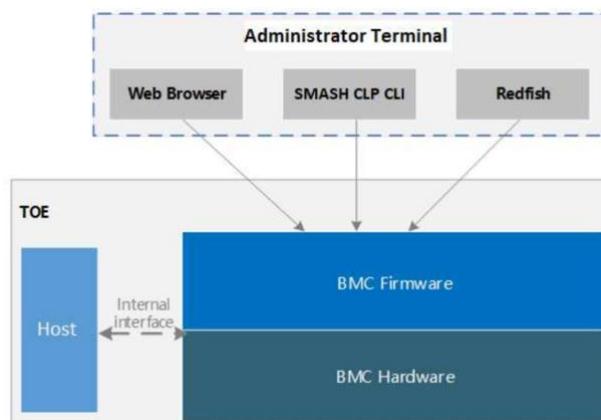


Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP/CMVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Implementation	Certificate Number
KAYTUS Server Baseboard Management Controller Cryptographic Library 7.11.00	A4791

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There are one or more competent individuals assigned to manage the TOE.

3.2 CLARIFICATION OF SCOPE

The following features are excluded from this evaluation:

- IPMI
- NTP
- SNMP
- Remote authentication such as LDAP/AD or Radius
- VNC

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Hardware	<p>KAYTUS Server Baseboard Management Controller 7.11.00</p> <p>on the following rack servers:</p> <ul style="list-style-type: none">• KAYTUS NF5180M6• KAYTUS NF5280M6• KAYTUS NF8260M6• KAYTUS NF8480M6• KAYTUS NF5266M6• KAYTUS NF5466M6 <p>and the following multi-node server:</p> <ul style="list-style-type: none">• KAYTUS i24M6
---------------------	---

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a) KAYTUS Server Baseboard Management Controller 7.11.00 Common Criteria Guidance Supplement, version 1.3
- b) KAYTUS Server BMC User Manual V1.0
- c) KAYTUS Server BMC Configuration Manual V1.0
- d) KAYTUS Server BMC Update Manual V1.0
- e) KAYTUS Server Redfish User Manual V1.1

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.



6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

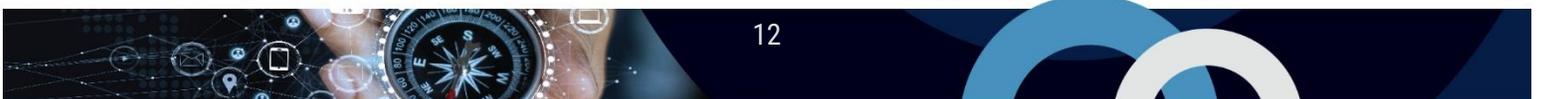
During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

- a. Repeat of Developer's Tests
- b. Independent Testing

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.



6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Evaluation team generated (Type 3)
- Technical community sources (Type 2)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **5 November 2024** and included the following search terms:

openssl version 1.0.2u	Busybox version 1_21_1	Linux Kernel
openssh version 7.9p1	jQuery version 2.1.1	KAYTUS
Bootstrap version 3.2.0	lighttpd version 1.4.45	AST2500
OpenWebStart 1.10.01	MegaRAC	

Vulnerability searches were conducted using the following sources:

NIST National Vulnerability Database https://nvd.nist.gov	KAYTUS Security Bulletins https://www.kaytus.com/en/2745970/index.html
CISA – Known exploited vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.



8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
KAYTUS BMC Security Target, Version 2.7, 8 January 2025
Evaluation Technical Report for Common Criteria Evaluation of KAYTUS KAYTUS Server Baseboard Management Controller 7.11, Version 1.2, 8 January 2025