KAYTUS BMC

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2221-003-D102
Version: 2.7
8 January 2025

KAYTUS SYSTEMS PTE. LTD.
150 Beach Road, #14-05/08, Gateway West,
Singapore 189720

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 6, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 7, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	KAYTUS BMC Security Target
ST Version:	2.7
ST Date:	8 January 2025

1.3 TOE REFERENCE

TOE Identification:	KAYTUS Server Baseboard Management Controller 7.11.00
TOE Developer:	KAYTUS SYSTEMS PTE. LTD.
TOE Type:	Remote Management Firmware

1.4 TOE OVERVIEW

The KAYTUS Server Baseboard Management Controller (BMC) 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 BMC uses an integrated System-on-Chip microprocessor for the remote monitoring/control system. The BMC co-exists on the system board with the managed server. The BMC functions independently of the server's state of operation, and the state of the server itself is transmitted to BMC through the internal hardware interface. This allows the BMC to function provided that the server is plugged into a power source, even if the server is not powered on.

The BMC can be used in the following situations:

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

Remote administration communication is protected using cryptography. The BMC offers WEB GUI and Redfish API management interfaces protected by HTTPS/TLS, and command line console access (SMASH CLP CLI) protected by SSH v2.

The TOE is a combined firmware and hardware TOE.

1.4.1 TOE Environment

Figure 1 - TOE Environment shows the evaluated configuration. An administrator terminal which is a Windows 10 x64 general purpose computer is required to manage the TOE.

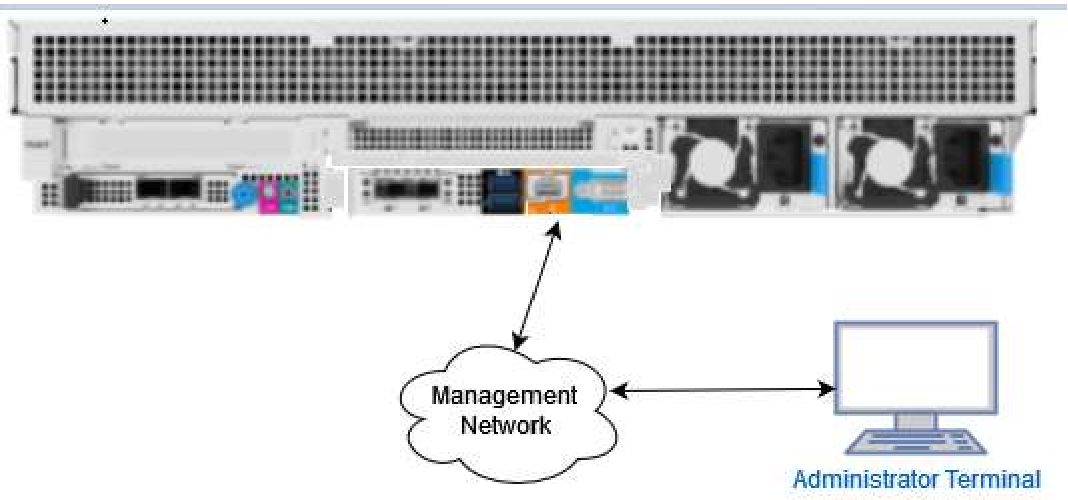

Figure 1 - TOE Environment

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:

- OpenWebStart version 1.10.1
- SSH Client: PuTTY Version 0.76+
- Redfish API Client: Postman Version 7+
- Web browsers: Google Chrome 58+

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is shown in Figure 2 – Evaluated Configuration and consists of the BMC hardware, BMC firmware and the host. The BMC hardware with KAYTUS BMC firmware is preinstalled within the host’s chassis. The BMC hardware is an advanced RISC1 machine (ARM) and uses the AST2500 server management processor. The BMC is managed through external network interfaces, and it communicates with the host with internal circuit board connections. The KAYTUS M6 Rack and Multi-node servers are covered by this evaluation.

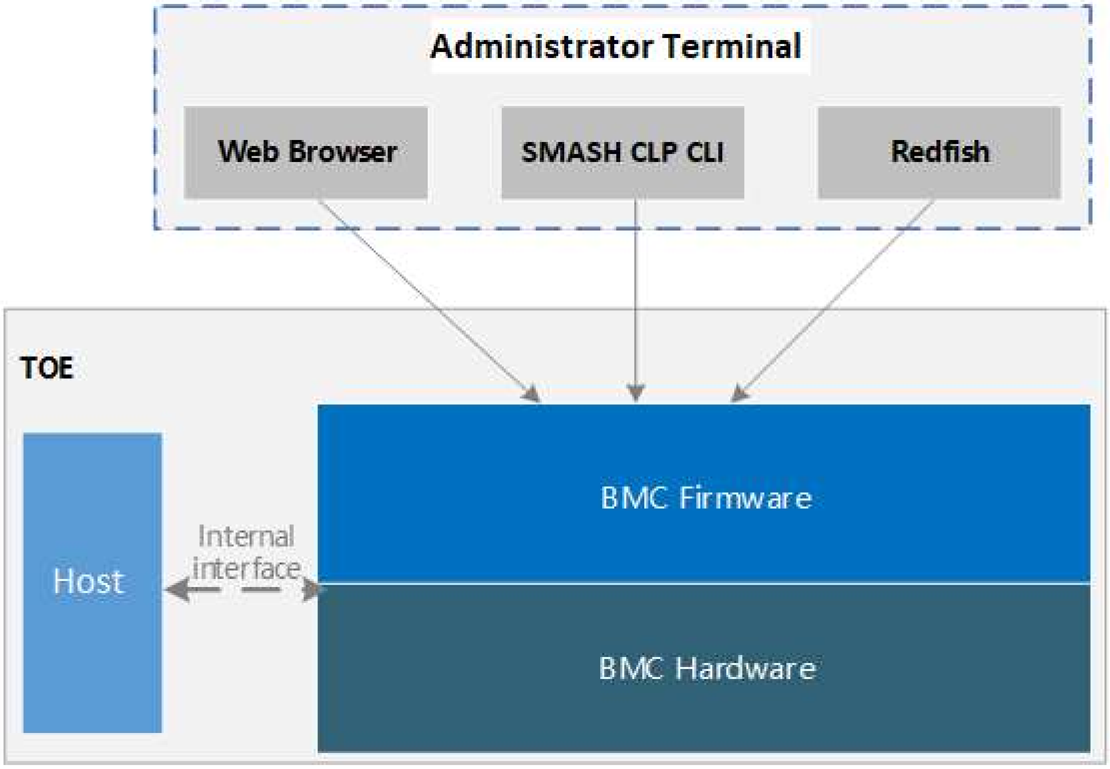

Figure 2 – Evaluated Configuration

The table below shows the KAYTUS server models.

Server Type	Operating System	Hardware
Rack Server	Not applicable	KAYTUS NF5180M6
		KAYTUS NF5280M6
		KAYTUS NF8260M6
		KAYTUS NF8480M6
		KAYTUS NF5266M6
		KAYTUS NF5466M6
Multi-Node Server	Not applicable	KAYTUS i24M6

Table 1 –KAYTUS Server Models

1.5.1.1 TOE Delivery

The TOE is shipped directly to customers with the firmware preinstalled. Alternatively, the evaluated version of the firmware and guidance documentation may be downloaded from the KAYTUS support site:

https://www.kaytus.com/. From there perform the following steps:

- Select “Support” -> “Documentation”
- Scroll down to the end of the product list then select “Click here for more product drivers, firmware and documentation”
- Select the desired server

The software and documentation will then be available for download.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation:

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

1.5.2 Logical Scope

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.
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 (TLS v1.2). 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 SSH v2 using the SMASH CLP CLI or the Redfish API using HTTPS. (TLS v1.2)

Functional Classes	Description
Protection of the TSF	The TOE provides time stamps for the audit records and its own use.
TOE Access	The TOE provides both TSE and user initiated termination and also enforces restrictions on session establishment.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using HTTPS (TLS v1.2) and SSH v2.

Table 2 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

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

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP; therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 3 lists the threats addressed by the TOE. Potential threat agents are unauthorized users and authorized users. The unauthorized users are considered to possess public knowledge of how the TOE operates, and the skills and resources to alter TOE configuration settings, or parameters, or both. The unauthorized users are not granted physical or logical access to the TOE. Authorized users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters but are assumed not to be wilfully hostile.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.CONFIG	An authorized user could improperly gain access to TSF functionality if the TOE is misconfigured or does not enforce proper roles and permissions.
T.UNAUTH	An unauthorized user may gain access to TOE data or TOE functionally that is restricted to authorized users.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed in the operational environment. Table 4 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.CRYPTO	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information, which is transferred between the TOE and administrators.
P.MANAGE	The TOE shall be managed only by authorized users.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Assumptions	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT	The TOE must record time stamped audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. The TOE must also protect stored audit records.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE and restrict these functions and facilities from unauthorized use.
O.I&A	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.PROTECT	The TOE must protect against unauthorized access to interactive management sessions and must provide a means of controlling and restricting access to TOE services and ports. The TOE must ensure the confidentiality and integrity of interactive administrative sessions.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.PERSONNEL	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.CONFIG	T.UNAUTH	P.CRYPTO	P.MANAGE	A.LOCATE	A.MANAGE
O.ACCESS		X		X		
O.ADMIN	X	X		X		
O.AUDIT	X					
O.I&A	X	X				
O.PROTECT	X	X	X			
OE.PERSONNEL						X
OE.PHYSICAL					X	

Table 8 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.CONFIG**	An authorized user could improperly gain access to TSF functionality if the TOE is misconfigured or does not enforce proper roles and permissions.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE and restrict these functions and facilities from unauthorized use.
	O.AUDIT	The TOE must record audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. The TOE must also protect stored audit records.
	O.I&A	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE
	O.PROTECT	The TOE must protect against unauthorized access to interactive management sessions and must provide a means of controlling and restricting access to TOE services and ports. The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.ADMIN helps to mitigate this threat by ensuring the TOE has the proper environment in which to operate. O.AUDIT allows for the review of configuration changes thus helping to ensure that configuration changes are authorized and have been made correctly. O.I&A helps to mitigate the threat by ensuring that users are identified and authorized before they can access to TOE security functions. O.PROTECT ensures that interactive management sessions can't be inadvertently accessed and ensures that they are protected.	

Threat: **T.UNAUTH**	An unauthorized user may gain access to TOE data or TOE functionally that is restricted to authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE and restrict these functions and facilities from unauthorized use.

	O.I&A	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.PROTECT	The TOE must protect against unauthorized access to interactive management sessions and must provide a means of controlling and restricting access to TOE services and ports. The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.ACCESS helps to mitigate this threat by limiting an authorized user's access to appropriate TOE functions and data. O.I&A helps to mitigate the threat by ensuring that users are identified and authorized before they can access to TOE security functions. O.ADMIN helps to mitigate this threat by ensuring the TOE has the proper environment in which to operate. O.PROTECT helps to mitigate this threat by protecting the confidentiality and integrity of management sessions.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **P.CRYPTO**	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure or modification of sensitive information, which is transferred between the TOE and administrators.	
Objectives:	O.PROTECT	The TOE must protect against unauthorized access to interactive management sessions and must provide a means of controlling and restricting access to TOE services and ports. The TOE must ensure the confidentiality and integrity of interactive administrative sessions.
Rationale:	O.PROTECT ensures that the confidentiality and integrity of the TOE communications is maintained.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the

		TOE and restrict these functions and facilities from unauthorized use.
Rationale:	O.ACCESS ensures that only authorized users manage the TOE. O.ADMIN ensures that the operational environment is adequate for the operation of the TOE.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.PERSONNEL	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.PERSONNEL supports this assumption by ensuring that trained individuals are in place to manage the TOE.	

5 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

5.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

5.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and are summarized in Table 9.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of audit data loss
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets

Class	Identifier	Name
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.1(1)	TSF-initiated session locking (WEB GUI and SMASH CLP CLI)
	FTA_SSL.1(2)	TSF-initiated session locking (Redfish API)
	FTA_SSL.4	User-initiated termination
	FTA_TSE.1	TOE session establishment
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [

- *Login and logout*
- *Account management actions*
- *All changes to password policy*
- *All changes to roles*
- *Enabling and disabling of BMC system services and service port assignment changes*
- *All changes to BMC firewall rules*
- *Powering on/off the host*
- *KVM configuration change*
- *Open/Close KVM Window*

- *BMC firmware update, host BIOS update, CPLD Firmware update, and BMC Factory reset*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

5.2.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*users who have been assigned the Administrator role*] with the capability to read [*all audit logs*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [filtering] of audit data based on [*date*].

5.2.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

5.2.1.6 FAU_STG.3 Action in case of audit data loss

Hierarchical to: No other components

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [replace previously saved audit trail backup file with the current audit trail file and clear all records inside the current audit trail file] if the audit trail **file** exceeds [200 KB in size].

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in table below*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in table below*] and cryptographic key sizes [*cryptographic key sizes specified in table below*] that meet the following: [*standards listed in table below*].

Cryptographic Operation	Algorithm	Key Size or Digest (bits)	Standard	CAVP Certificate Numbers
Encryption and Decryption	AES (CBC, CTR and GCM mode)	128, 256	FIPS PUB 197 (AES), NIST SP 800-38A and NIST SP 800-38C	A4791
Cryptographic Signature Services	RSA Digital Signature Algorithm (RSASSA-PKCS-v1_5 using SHA-256 and SHA-512)	Signature Verification 1024, 2048, 3072, 4096 Signature Generation 2048, 3072, 4096	PKCS #1.5	A4791
Hashing	SHA-256	256	FIPS PUB 180-4	A4791
	SHA-384	384		
	SHA-512	512		
Keyed Hash	HMAC-SHA-256	8 - 524288 key 256 digest	FIPS PUB 198	A4791
	HMAC-SHA2-384	8 - 524288 key 384 digest		

Cryptographic Operation	Algorithm	Key Size or Digest (bits)	Standard	CAVP Certificate Numbers
	HMAC-SHA2- 512	8 - 524288 key 512 digest		
Random Bit Generation	CTR_DRBG	256	NIST SP800-90A	A4791

Table 10 - Cryptographic Algorithms

Note: The cryptographic operations are implemented in the KAYTUS Server Baseboard Management Controller Cryptographic Library 7.11.00.

5.2.3 User Data Protection (FDP)

5.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Security Management Access Control SFP*] on [

a) Subjects: authorized users
b) Objects: TOE configuration
c) Operations: view, modify

].

5.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Security Management Access Control SFP*] to objects based on the following: [

a) Subjects: authorized users
b) Subject attributes: role and associated permissions
c) Objects: TOE configuration
d) *Object attributes: none*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*users can perform the actions determined by the user's role and the role's permissions.*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

5.2.4 Identification and Authentication (FIA)

5.2.4.1 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) Username
b) User roles

].

5.2.4.2 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

a) *a configurable minimum length of 8 to 16 characters,*
b) *passwords must contain at least three of the following character types:*
   - *uppercase letters,*
   - *lowercase letters,*
   - *numbers, and*
   - *special characters*

c) *configurable number of historical passwords must not be reusable*].

5.2.4.3 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.4 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Security Management (FMT)

5.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Security Management Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*role*] to [*users who have been assigned the Administrator role*].

5.2.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Security Management Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users who have been assigned the Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) User management
b) Service settings
c) Firewall settings
d) Audit management
e) Power control
f) Remote control
g) System maintenance

].

5.2.5.4 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator, Operator, User*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.7 TOA Access (FTA)

5.2.7.1 FTA_SSL.1 (1) TSF-initiated session locking (WEB GUI and SMASH CLP CLI)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

FTA_SSL.1.1(1) The TSF shall lock an interactive session after [*a time interval of user inactivity that has been configured by a user with the Administrator or Operator role using the WEB GUI or Redfish API*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2(1) The TSF shall require the following events to occur prior to unlocking the session: [*re-authentication*].

5.2.7.2 FTA_SSL.1 (2) TSF-initiated session locking (Redfish API)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1(2) The TSF shall lock an interactive session after [*a time interval of user inactivity that has been configured by the session owner during session establishment or based on a global setting configured by a user with the Administrator or Operator role*] by **invalidating the session specific X-Auth-Token**.

FTA_SSL.1.2(2) The TSF shall require the following events to occur prior to unlocking the session: [*re-authentication*].

5.2.7.3 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.2.7.4 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*session establishment request source IP, source MAC address, and TOE port number*].

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*administration of the TOE*]].

5.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 11.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	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
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 11 – Security Assurance Requirements

5.4 SECURITY REQUIREMENTS RATIONALE

5.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.I&A	O.PROTECT
FAU_GEN.1			X		
FAU_SAR.1			X		
FAU_SAR.2			X		
FAU_SAR.3			X		
FAU_STG.1			X		
FAU_STG.3			X		
FCS_COP.1					X
FDP_ACC.1		X			
FDP_ACF.1		X			
FIA_ATD.1	X				
FIA_SOS.1				X	
FIA_UAU.2	X			X	
FIA_UID.2	X			X	
FMT_MSA.1		X			
FMT_MSA.3		X			
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_STM.1			X		
FTA_SSL.1(1)					X
FTA_SSL.1(2)					X
FTA_SSL.4					X
FTA_TSE.1					X

	O.ACCESS	O.ADMIN	O.AUDIT	O.I&A	O.PROTECT
FTP_TRP.1					X

Table 12 – Mapping of SFRs to Security Objectives

5.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must only allow authorized users to access appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FIA_ATD.1	User attribute definition
Rationale:	FIA_UAU.2 requires that any user be authenticated prior to being able to access TOE functionality. FIA_UID.2 requires that any user be identified prior to being able to access TOE functionality. FIA_ATD.1 states that the TSF maintains a list of user attributes that allow or deny access to TOE functionality.	

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the TOE and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Rationale:	FMT_MSA.1 and FMT_MSA.3 restrict specified management activities to users assigned the Administrator role and ensure that appropriate default values are used.	

	FMT_SMF.1 defines the management activities that an authorized user can perform. FMT_SMR.1 defines the three user roles which are Administrator, Operator, and User. FDP_ACC.1 enforces the security functional policy imposed on specific objects and roles. FDP_ACF.1 the security functional policy is enforced by the TSF. It explicitly allows access of TOE security functionality to users with appropriate privilege and denies access to users without appropriate privilege.

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions. Audit records must be readable by authorized administrators and administrators must be able to filter records for ease of viewing. The TOE must also protect stored audit records.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selected Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of audit data loss
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 allows the administrator to view audit events. FAU_SAR.2 restricts the audit log review to users who have been assigned the Administrator role. FAU_SAR.3 allows a user who has been assigned the Administrator role to search the audit logs using filters. FAU_STG.1 does not allow unauthorised modifications or deletions of the audit logs. FAU_STG.3 saves a copy of the audit logs when the size limit is reached. This copy overwrites the previously saved copy. This ensures that recent audit data is preserved. FPT_STM.1 ensures that there is a time stamp for the audit records.	

Objective: **O.I&A**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
	FIA_SOS.1	Specification of secrets

Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_SOS.1 specifies the password rules that are enforced by the TOE. FIA_UAU.2 requires that any user be authenticated prior to being able to access TOE functionality. FIA_UID.2 requires that any user be identified prior to being able to access TOE functionality.	

Objective: **O.PROTECT**	The TOE must protect against unauthorized access to interactive management sessions and must provide a means of controlling and restricting access to TOE services and ports. The TOE must ensure the confidentiality and integrity of interactive administrative sessions.	
Security Functional Requirements:	FCS_COP.1	Cryptographic operation
	FTA_SSL.1(1)	TSF-initiated session locking (WEB GUI and SMASH CLP CLI)
	FTA_SSL.1(2)	TSF-initiated session locking (Redfish API)
	FTA_SSL.4	User-initiated termination
	FTA_TSE.1	TOE session establishment
	FTP_TRP.1	Trusted Path
Rationale:	FCS_COP.1 ensures that the TOE uses validated cryptography. FTA_SSL.1(1), FTA_SSl.1(2), and FTA_SSL.4 ensure that inactive sessions automatically lock and that users can logout. FTA_TSE.1 ensures that interactive management sessions can be restricted based on origin and destination information. FTP_TRP.1 protects the management sessions from disclosure using TLS v1.2 or SSH v2.	

5.4.3 Dependency Rationale

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.3	FAU_STG.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	FCS_CKM.1 is considered satisfied as per Canadian Common Criteria Scheme guidance.
	FCS_CKM.4	✓	FCS_CKM.4 is considered satisfied as per Canadian Common Criteria Scheme guidance.
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	None	N/A	
FIA_SOS.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	
FTA_SSL.1(1)	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.

SFR	Dependency	Dependency Satisfied	Rationale
FTA_SSL.1(2)	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FTA_SSL.4	None	N/A	
FTA_TSE.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 13 – Functional Requirement Dependencies

5.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the augmentation since there are several areas where current practices and procedures exceed the minimum requirements for EAL 2.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 SECURITY AUDIT

The BMC locally records the audit logs of various configuration and management operations of TOE. The logs include the following events:

- Login and logout
- Account management actions
- All changes to password policy
- All changes to roles
- Enabling and disabling of BMC system services and service port assignment changes
- All changes to BMC firewall rules
- Powering on/off the host
- KVM configuration change
- Open/Close KVM Window
- BMC firmware update, host BIOS update, CPLD Firmware update, and BMC Factory reset.

Account management actions consist of creation, modification, deletion, disabling and password change. Each event contains the following information if is applicable: date/time, software interface, username, IP address or hardware interface, and event description (event type, event information, event outcome).

A user with the Administrator role who logs in to BMC web interface, SMASH CLP CLI, or uses the Redfish API can read all audit information and can query audit information. Logs can be filtered by date. Audit log records are protected from modification.

The BMC audit log is stored in the BMC flash storage media and unaffected by system power loss. 200KB disk space is dedicated to the storage of current Audit Log file. When BMC detects that the Audit log file is reaching 200K in size, the file will be saved as a backup Audit log file and a new empty Audit log file will be used to store the upcoming log records. The previously saved backup Audit log file is removed from the storage each time a new backup file is created. The backup audit log file can be downloaded through the WEB GUI.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3.

6.2 CRYPTOGRAPHIC SUPPORT

The TOE uses the CMVP validated KAYTUS Server Baseboard Management Controller Cryptographic Library 7.11.00. TLS and SSH are implemented in this library. TLS v1.2 is used to protect the BMC web interface and Redfish API connections while SSH v2 is used to protect the SMASH CLI CLP connection. No communication with a remote user is possible without using one of these methods, ensuring that validated cryptography is used for all trusted path / channels functionality. Assured identification of the TLS/SSH server is achieved using public key certificates. Cryptographic operations are performed in accordance with the details provided in Section 5.2.2.1.

TOE Security Functional Requirements addressed: FCS_COP.1.

6.3 USER DATA PROTECTION

The TOE provides controlled access to the administrative functions that support the BMC remote management functionality, including:

- User management
- Service settings
- Firewall settings
- Audit management
- Power control
- Remote control
- System maintenance

Access to these functions is controlled through the security management access control SFP, which allows users to perform functions according to assigned roles.

The mapping between the roles and permissions are shown in the following table. These apply to WEB GUI and Redfish API users unless otherwise indicated.

Role	Permission
Administrator	Full access to • User management including, ○ Account creation, modification, deletion, disablement, and password change ○ Password policy management; and, ○ Role and Privilege Management • Service settings • Firewall settings • Audit management (Query of audit records only) • Power control • (Host) Remote control (Configure and Access Host KVM) • System maintenance
Operator	Full access to

Role	Permission
	• User management including: ○ Password policy management ○ Read access to role and privilege management • Service settings • Firewall settings • Power control • (Host) Remote control (Configure and Access Host KVM) • System maintenance
User	Read Access to, • User management (Password policy management and Role and Privilege Management only) • Service settings • Firewall settings • Power control (Host Power Status) • (Host) Remote control (Access of Host KVM) • System maintenance

Table 14 - Mapping Between Roles and Permissions

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1.

6.4 IDENTIFICATION AND AUTHENTICATION

The TOE supports user identification and authentication based on username and password. The TSF does not allow any TSF mediated actions before a user has been authenticated.

The TOE enforces password complexity that is configured by the administrator. The minimum password length can be configured to be from 8 to 16 characters and the character type can be set to require three or more arbitrary combinations of uppercase letters, lowercase letters, numbers, and special characters.

Additionally, the number of times the historical password cannot be reused can be set. New records of historical passwords are only stored when a user changes their password after the number of times the historical password cannot be reused is increased. The stored historical passwords are only erased if the limit is decreased or if a user is deleted.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2.

6.5 SECURITY MANAGEMENT

BMC provides three default user roles, and they are Administrator, Operator and User which are assigned to user accounts. The BMC has a default Administrator role account which cannot be deleted. A newly created user account is automatically assigned the user role. All accounts can only be created or modified by a user who has been assigned the Administrator role and these users are responsible for:

- User management using the WEB GUI or Redfish API consisting of account management, password policy management, role management, and privilege management.
- BMC system service management using the WEB GUI Redfish API, or SMASH CLP CLI
- BMC firewall rule management using the WEB GUI
- Reviewing audit records using the WEB GUI, Redfish API, or SMASH CLP CLI
- Power control of the host using the WEB GUI Redfish API, or SMASH CLP CLI
- Remote control and management of the host using the WEB GUI or Redfish API
- System maintenance of the host and BMC using the WEB GUI Redfish API, or SMASH CLP CLI

Security Management Function	Details
System Service Management	Network service ports and ports using insecure protocols and unused network service ports are closed. A session limit can also be set for each service.
Firewall Rule Management	Firewall rules can be created to filter network traffic based on IP address, port, and MAC address.
Remote Control and Management of the Host	Remote Control redirects the console of the server system to the connected WEB GUI or Redfish API session allowing the remote viewing of the host's display and control of the host's keyboard/mouse.
System Maintenance of the Host	The host's firmware can be updated using the WEB GUI Redfish API, or SMASH CLP CLI.

Table 15 - System Management Function Details

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

6.6 PROTECTION OF THE TSF

When plugged in, the KAYTUS server runs the Intel Management Engine (ME) which is an embedded microcontroller running a lightweight microkernel operating system. When the BMC powers on it requests the time from the ME and synchronizes its time with the ME hourly. The BMC's time is used to provide reliable time stamp services for the BMC audit function and TSF initiated session locking.

TOE Security Functional Requirements addressed: FPT_STM.1.

6.7 TOE ACCESS

Remote Management of the BMC is provided through the WEB GUI, Redfish API, and SMASH CLP CLI interfaces. After the configured session timeout has passed, the WEB GUI, and SMASH CLP CLI user sessions will become invalid, and the system will automatically terminate the connection. The user needs to log in again in order to perform any operations. The session timeout can be configured by a user with the Administrator or Operator role using the WEB GUI or Redfish API interfaces.

Upon successful authentication at the Redfish API interface, a X-Auth-Token is issued to the user. The X-Auth-Token can be attached to subsequent Redfish API requests from the same user, replacing user credentials, allowing those requests to be executed with the same user privilege. A user with the Administrator or Operator role can configure a session timeout. Once the configured timeout has passed, the X-Auth-Token is no longer accepted by BMC and new Redfish API requests issued with the X-Auth-Token will be rejected. The user needs to provide username and password again at the Redfish API interface to obtain a new X-Auth-Token. All Redfish API users have the option to specify an alternative session time out value during the initial authentication request to overwrite the administrator configured X-Auth-Token session timeout. Alternatively, Redfish API users may choose to use basic HTTP authentication instead. In this case, the user provides credentials with each Redfish API request, and each Redfish API request is regarded as an individual user session.

The TOE allows users to actively end sessions. After the session ends, the user will need to log in again to perform any BMC operations.

The TOE allows users with the Administrator or Operator role to disable services to ensure that only the services being used are available. Users assigned to the Operator role can configure the port number on which the service is available.

Additionally, the TOE supports connection control based on source IP address, MAC address, and TOE port number requested. Rules can be configured by a user with the Administrator or Operator role to allow or deny connections from corresponding sources.

TOE Security Functional Requirements addressed: FTA_SSL.1(1), FTA_SSL.1(2), FTA_SSL.4, FTA_TSE.1.

6.8 TRUSTED PATH / CHANNELS

When the BMC web interface or Redfish API interface is used, the connection between BMC and the remote user’s session is protected from modification and disclosure using TLS v1.2. The SMASH CLP CLI is protected by SSH v2. These connections are logically distinct from other communication channels. Identification and authentication are required before any TSF actions can be performed.

TOE Security Functional Requirements addressed: FTC_TRP.1.

7 TERMINOLOGY AND ACRONYMS

7.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Security Policy	The term security policy is used in this ST to describe the policies implemented within the TOE to enforce the claimed functionality. It does not refer to the specific policies enforced by the User Data Protection SFRs.

Table 16 – Terminology

7.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
CLI	Command Line Interface
CPLD	Complex Programmable Logic Device
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPMI	Intelligent Platform Management Interface
ME	(Intel) Management Engine
NTP	Network Time Protocol
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SMASH CLP	System Management Architecture for Server Hardware Command Line Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation

Acronym	Definition
TSF	TOE Security Functionality

Table 17 – Acronyms