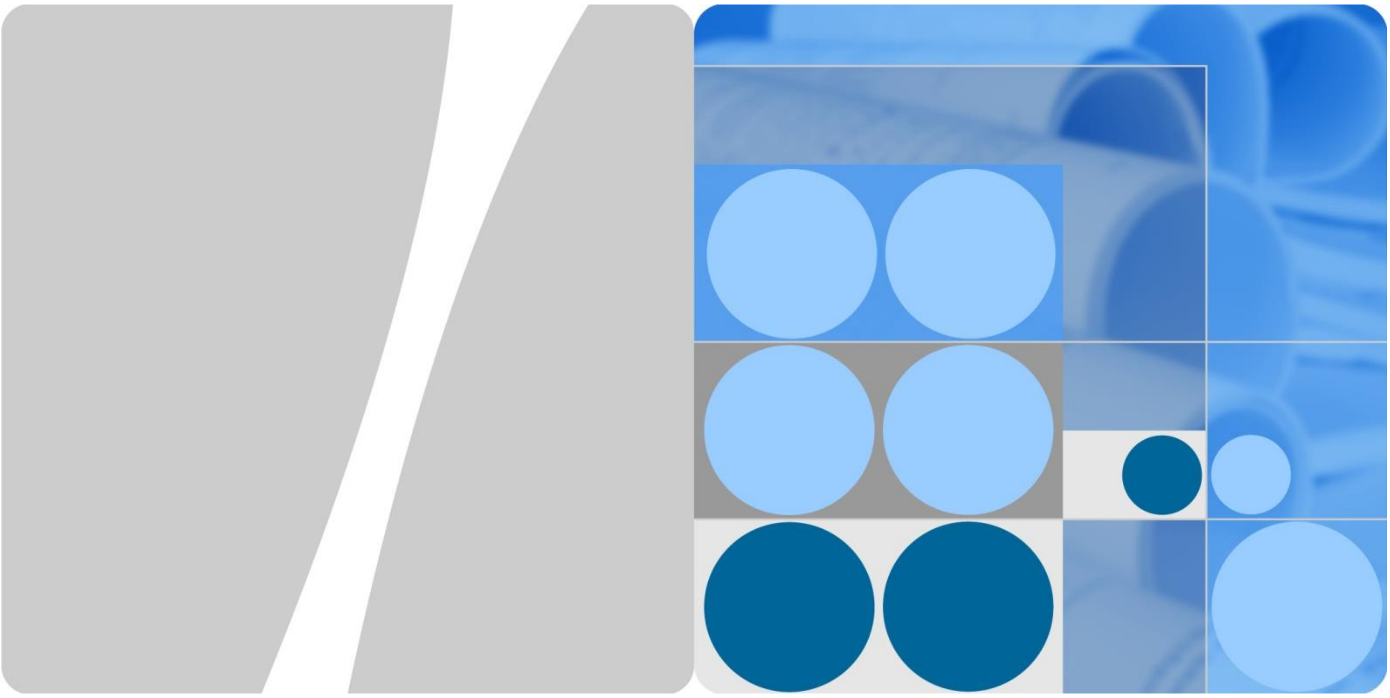

CC Security Target

for Huawei Server Management Software iBMC

Issue	1.8
Date	2020-08-03

HUAWEI TECHNOLOGIES CO., LTD

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Purpose

This Security Target is for the evaluation of Huawei server management software iBMC.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
📖 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Version	Change Description	Author
2019-10-30	0.1	Initial Draft	Huang Quanwei
2019-11-10	0.2	Update	Huang Quanwei

Date	Version	Change Description	Author
2019-11-18	0.3	Update	Huang Quanwei
2020-04-08	1.0	Update	Huang Quanwei
2020-04-26	1.1	Update	Huang Quanwei
2020-06-09	1.2	Update	Zhangli, Huang Quanwei
2020-06-28	1.3	Update	Zhangli, Huang Quanwei
2020-07-09	1.4	Update	Zhangli, Huang Quanwei
2020-07-20	1.5	Update the version description	Zhangli, Huang Quanwei
2020-07-21	1.6	Update the encryption mode in FTP_TRP.1	Huang Quanwei
2020-07-22	1.7	Update the version number	Huang Quanwei
2020-08-03	1.8	Update the version number	Huang Quanwei

Contents

Figures

Tables

1 Introduction

This Security Target is for the evaluation of Huawei Server management software iBMC (intelligent Baseboard Management Controller), which is an embedded, out of band management system optimized for server lifecycle management.

1.1 ST Identification

Title: Security Target for Huawei Server Management software iBMC

Version: 1.8

Date: 2020-08-03

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei Server management software iBMC

Version: V662/V3.01.12.02

Developer: Huawei Technologies Co., Ltd.

The TOE is part of the Huawei Server management software iBMC which is the software running on Huawei Server devices.

iBMC V662 and V3.01.12.02 are compatible with different iBMC chip, the hardware driver and OS is different, but the hardware adaptation layer (Platform Management Engine in Figure1-2) adapts to the differences, the adaptation layer interfaces presented externally are the same. Therefore, the difference does not affect the TSF and the changes occur only on SFR-non-interfering subsystems.

1.3 TOE overview

1.3.1 TOE usage

Huawei Server management software iBMC (intelligent Baseboard Management Controller) is an embedded, out of band management system optimized for server lifecycle management. It provides server management features such as hardware monitoring, dynamic energy management and saving, fault diagnosis and management, a variety of remote management tools, etc.

1.3.2 TOE type

The TOE type is a server management software, which is part of the Huawei server.

1.3.3 Non-TOE hardware and software

Non-TOE content includes:

1. iBMC Hardware including BMC chip and firmware storage media which the TOE runs on
2. Huawei server which is managed by iBMC
3. Web Browser, SSH Client and Redfish Client
4. NTP, Syslog and LDAP server

Huawei Server management software iBMC is an out of band management system optimized for server lifecycle management. It cooperates with other IT devices to perform management functions and service functions. The following figure presents an example of TOE deployment.

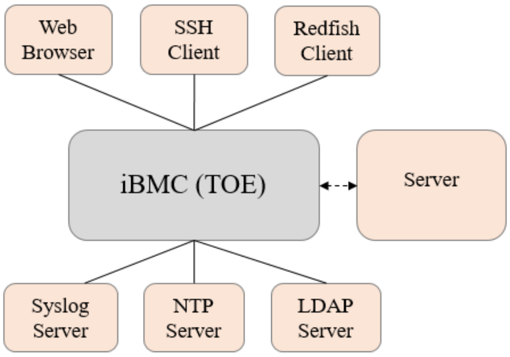

Figure 1-1 Deployment of the TOE

The syslog, NTP, and LDAP servers need to be deployed. The TOE functions as the client to communicate with all the servers, uploads logs to the syslog server, synchronizes the system time from the NTP server, and performs authentication on the LDAP server. TOE users can access the TOE through the web browser, SSH client, and Redfish client.

1.4 TOE Description

1.4.1 Physical Scope of the TOE

TOE consists of the Huawei server management software iBMC including underlying OS, product guidance and software signature file. The hardware that the TOE running on is not within the scope but a part of operational environment. The evaluated configuration of the TOE is listed as below.

Table 1-1 TOE Evaluated Configuration

Type	Delivery Item	Version
Software	iBMC-V662.zip iBMC-V3.01.12.02.zip	V662 V3.01.12.02
Software Signature File	iBMC-V662.zip.asc iBMC-V3.01.12.02.zip.asc	-
Product Guidance	Huawei Server Management Software iBMC AGD_OPE_V1.5.docx	V1.5
	Huawei Server Management Software iBMC AGD_PRE_Production_V1.4.docx	V1.4
	Huawei Server Management Software iBMC AGD_PRE_User_V1.5.docx	V1.5
Security Target	Huawei Server Management Software iBMC Security Target_V1.8.docx	V1.8

1.4.2 Logical scope of the TOE

The architecture of the iBMC is presented in Figure 1-2. It consists of the following parts:

- Interface Layer: The interface layer provides a variety of interfaces, including user interfaces (Web UI and SSH) and machine-machine interfaces (Redfish interface, SNMP and RMCP+).
- Application Layer: The application layer incorporates the security management features and service management features.
- Framework Layer: The framework layer consists of the platform management engine and driver.
- OS: iBMC underlying linux system.

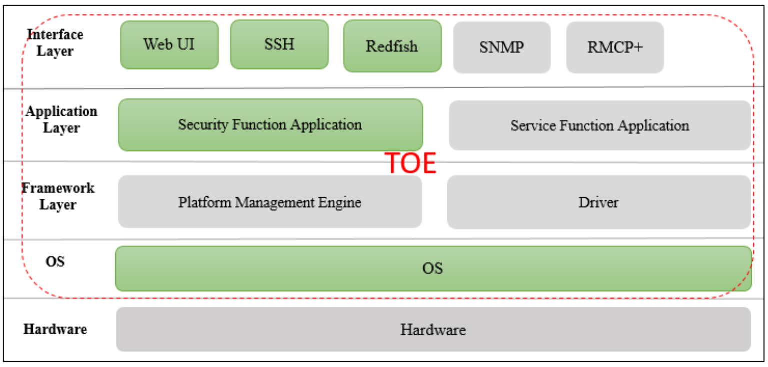

Figure 1-2 iBMC software architecture

Although Huawei Server management software iBMC provides many management and service functions, the TOE only address the security functions that secure the TOE itself as described in Logical scope of the TOE, these security functions are supported by components painted with green in the Figure 1-2. Other management functionalities shall be disabled to use the TOE in the certified configuration as described in Product Guidance.

The logical boundary of the TOE will be broken down into the following security classes, which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- TOE access
- Trusted Path/Channel

1.4.3 Summary of Security Features

1.4.3.1 Security Audit

The TOE generates security audit records for security relevant events. All audit records contain a timestamp, user name (if possible), IP address (if possible), etc.

Audit function is enabled by default and it can’t be disabled by any user. Audit records can be stored in local Flash or uploaded to syslog server. Only authorized user can view audit records.

1.4.3.2 Cryptographic Support

The TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (TLS, SSH) and authentication (Local user authentication, SSH public key authentication). The TOE is capable of generating the necessary keys (AES, RSA). For key generation, the TOE can use its own deterministic random number generator.

1.4.3.3 Identification and Authentication

The user and the upper-layer management system need to authenticate the access to the TOE through the Web, CLI and Redfish interfaces. The device management configuration and information query can be performed only after the authentication succeeds.

The TOE supports local authentication and Centralized authentication (LDAP). Both authentication can use mechanism of user name with password or SSH public key.

For local authentication, the account and password are saved on the local equipment and password complexity is required.

For LDAP centralized authentication, the account and password are stored on the remote LDAP servers, and password complexity policy is configured on LDAP server too.

1.4.3.4 Security Functionality Management

Security functionality management include not only authentication, authorization, access control, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

The functions mainly include:

- Management of user accounts, authentication data and role association
- Management of security banner, authentication failure policy

- Management of customized user role and its authorities
- Management of cypher suites
- Management of the security audit records, audit configuration
- Management of the session policy
- Management of the time, NTP configuration

1.4.3.5 TOE Access

The session timeout period can be configured on the TOE. If you do not perform any operation for a long time, the session will be automatically disconnected. You can also configure warning information on the TOE login page to prompt all login users. If a user fails to log in to the system for multiple times, the user is locked. The number of login failures and the locking duration are configurable.

The TOE supports configuration of security warning information. Before user authentication, warning information is displayed on the page. The warning information can be configured by users. The TOE supports the anti-brute force cracking mechanism, accounts can be locked based on consecutive login failures.

1.4.3.6 Trusted Path/Channel

The TOE supports HTTPS, TLS and SSH security protocols to secure communications with external entities including users and centralized authentication devices (i.e. LDAP server).

2 CC Conformance Claims

2.1 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The version of [CC] is 3.1R5.

The ST claims conformance to the EAL2 assurance package, augmented by ALC FLR.1.

No conformance to a Protection Profile is claimed.

3 TOE Security Problem Definition

3.1 Threats

3.1.1 Assets to be protected

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

1. TSF data such as Audit records, user account and authentication information, Critical security parameters used by cryptographic functions, etc.
2. Configuration data for the TOE

3.1.2 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment.

Assumed threat agents are classified into two classes:

Non-TOE users: who is not authorized to access the TOE, but obtains TOE knowledge through public channels, and attempts to access the TOE by hacking technologies such as brute force cracking

Non-administrator users: who is an authorized user to access the TOE with lower privileges than administrator, may obtain and utilize higher privileges to the TOE undeliberately. According to the assets to be protected, the following security threats are identified:

T.Unauthenticated

Threat agent: A subject who is not an authenticated user of the TOE

Asset: TSF data, Configuration data

Adverse action: the subject gains access to the TOE, views or modifies TOE configuration data, audit records, etc. without permission

T.Unauthorized

Threat agent: A user of the TOE authorized with low privileges

Asset: Configuration data

Adverse action: the user gains access to operations or information which is not authorized for. By that the user could modify TOE configuration data without permission.

T.Intercept

Threat agent: An attacker in the management network who is able to intercept traffic

Asset: TSF data

Adverse action: the attacker may modify and re-use sensitive information assets that are exchanged between the TOE and LDAP server or remote user, therefore compromises confidentiality and integrity of TSF data.

3.2 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

A.PhysicalProtection

It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals, such as a board, and SD card inserted in the transmission equipment) are protected against unauthorized physical access. It is also assumed that the local management sub-network, including the LDAP server, syslog server and NTP server together with all related communication cables are operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) need to be physically protected on the same level as the TOE. It is assumed that all RMTs as well as peripherals like LDAP server or syslog server are connected to the TOE via the same segregated management network (see also A.NetworkSegregation).

A.NetworkElements

It is assumed that the operational environment provides trustful devices (i.e. syslog servers, NTP servers and LDAP servers) that the TOE needs to cooperate with in the management sub-network, and these devices are configured and working correctly in the management sub-network.

The server managed by the TOE is controlled (authentication and permission management are required), and the operation (configure iBMC using the ipmi Command) from the Server to the TOE is secure.

A.NetworkSegregation

It is assumed that the operational environment provides segregation of networks by deploying the management interface of the TOE into an independent local network.

A.NoEvil

It is assumed that personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.CorrectHardware

It is assumed that the underlying hardware of iBMC, which is outside the scope of the TOE, works correctly. The hardware is reliable and runs according to the design specifications. There is no attack on the software from the hardware layer.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

O.Authentication

The TOE must provide identify and authenticate function. User must pass the system authentication before using the functions provided by the TOE. Multiple authentication methods must be supported, including local user authentication and remote centralized authentication. Security banner must be displayed before authentication. User accounts and passwords must be protected to prevent brute force cracking.

O.Authorization

The TOE shall implement different authorization levels that can be assigned to users in order to restrict the functionality that is available to individual users.

O.Communication

The TOE must implement logical protection measures for network communication between the TOE and Remote Management Terminal (RMT). These protection measures shall include device authentication and the use of a secure communication protocol.

O.Audit

The TOE shall provide functionality to generate audit records for security-relevant events.

O.SecurityManagement

The TOE shall provide functionality to manage security functions provided by the TOE. This includes:

- Management of user accounts, authentication data and role association
- Management of security banner, authentication failure policy
- Management of customized user role and its authorities
- Management of cypher suites
- Management of the security audit records, audit configuration
- Management of the session policy
- Management of the time, NTP configuration

4.2 Security Objectives for the Operational Environment

OE.PhysicalProtection

The TOE and its operational environment (i.e. the complete system including attached peripherals, such as a board, and CF card inserted in the transmission equipment) shall be protected against unauthorized physical access. The local management network, including the LDAP server, syslog server, and locally attached management terminals (LMT) together with all related communication lines shall be operated in the same physically secured environment as the TOE. Remote management terminals (RMTs) shall be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any RMT and the TOE are protected by cryptographic means and do not need any physical protection.

OE.NetworkElements

The operational environment shall provide secured and correctly working devices as resources that the TOE needs to cooperate with. The behavior of such devices provided by the operational environment shall be secure and correct.

OE.NetworkSegregation

The operational environment shall provide segregation of networks by deploying the management interface of the TOE into an independent local network. The network of the iBMC management system must be isolated from the network of the server service system.

OE.NoEvil

Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or willfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation.

OE.CorrectHardware

The underlying hardware of Huawei server, which is outside the scope of the TOE, shall work correctly. The hardware is reliable and runs according to the design specifications. There is no attack on the software from the hardware layer.

4.3 Rationale for Security Objectives

The following table provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat.

Table 4-1 Mapping objectives to threats and OSPs

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.Unauthenticated	O.Authentication O.Audit O.Communication O.SecurityManagement	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). Login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit). Secure communication protocols can prevent attackers from hijacking the active authentication communication between the TOE and users (O.Communication). Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement).
T.Unauthorized	O.Authorization O.Audit O.SecurityManagement	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit). Access control mechanisms (including user level) can be configured by users with sufficient user level (O.SecurityManagement).
T. Intercept	O.Communication O.SecurityManagement	The threat of intercept is countered by requiring communications security via HTTPS and SSH for communication between EMS and the TOE (O.Communication). Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement).

The following table provides a mapping of the objectives for the operational environment to assumptions, showing that each objective is covered exactly by one assumption. The objectives for the environment are mirrored by the assumptions. A Security Objective for the Operational Environment directly upholds the Assumption of the same name.

Table 4-2 Mapping objectives for the environment to assumptions

Environmental Objective	Threat /Assumption
OE.PhysicalProtection	A.PhysicalProtection

Environmental Objective	Threat /Assumption
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation
OE.NoEvil	A.NoEvil
OE.CorrectHardware	A.CorrectHardware

5 Extended Components Definition

There is no extended components for this TOE.

6 Security Requirements for the TOE

6.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

6.2 Security Functional Requirements

The following table lists the security functions of the TOE：

Table 6-1 TOE Security Functional Requirements

Name	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted Audit Review

FAU_STG.1	Protected Audit Trail Storage
FAU_STG.3	Action in Case of Possible Audit Data Loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of Security Functions Behavior
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination
FTA_TAB.1	Default TOE access banners
FTA_TSE.1	TOE session establishment
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

6.2.2 Security Audit (FAU)

6.2.2.1 FAU_GEN.1 Audit Data Generation

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

~~a) Start-up and shut-down of the audit functions~~

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

c) **The following auditable events:**

i. user activity

1. **login, logout**
2. **add, delete, modify users**
3. **user password change**
4. **user level change**
5. **user lock and unlock**

ii. system management

1. **perform security management functions which are defined in FMT_SMF.1 Specification of Management**
2. **Power on, power off, and restart the service system**

Application Note: Audit functionality is enabled by default during start-up of the device, and it cannot be shut down manually, therefore there's no start-up and shut-down of the audit functions events to be recorded.

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 ST, **Operation Type (if applicable)**, **Operation Object (if applicable)**, **Access IP Address (if applicable)**, **User Name (if applicable).**

Application Note: The term 'if applicable' shall be read as 'whenever an event can be associated with the specified information'. For example, if an event can be associated with a User Name, then the event shall be recorded and the audit information shall contain the User Name. If the event cannot be associated with the User Name, the event shall be recorded and the audit information shall not contain User Name information. If multiple conditional information can be associated with an event (e.g. interface and User Name can be associated with an event), all the conditional information shall be contained in the audit information when record the event.

6.2.2.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that causes the event.

6.2.2.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **Administrators** with the capability to read **all information** 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.

6.2.2.4 FAU_SAR.2 Restricted 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.

6.2.2.5 FAU_STG.1 Protected Audit Trail Storage

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

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorized modifications to the stored audit records in the audit trail.

6.2.2.6 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall **overwrite the oldest records** if the audit trail exceeds **the size of log files**.

Application Note: The audit trail is recorded in log file on the storage media (FLASH), the size of log file is fixed.

6.2.3 Cryptographic Support (FCS)

6.2.3.1 FCS_CKM.1/DH Cryptographic key generation

FCS_CKM.1.1/DH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **diffie-hellman-group14-sha1/diffie-hellman-group-exchange-sha256/ diffie-hellman-group-exchange-sha1** and specified cryptographic key sizes **128/256 bits** that meet the following: : **[NIST SP 800-56A], [RFC 4253], [RFC 3526], [RFC 4346], [RFC 5246], [PKCS#3] for SSH/TLS.**

Application Note: When establish SSH/TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption, and generation and verification of integrity protection information for SSH/TLS communication. The key generation is performed according to [RFC 4250], [RFC 4253], [RFC 3526].

When establish TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement use ECDHE_RSA/DHE_RSA algorithm. RSA private key sizes is 2048bit which used to exchange key used for encryption and decryption, and generation and verification of integrity protection information for TLS communication. The key generation is performed according to [RFC 4346], [RFC 5246].

6.2.3.2 FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **2048/ 4096 bits** that meet the following: **[FIPS 186-4], chap. 5.1, RSA key pairs for RSASSA-PKCS1-V1_5 using CRT, chap. 6.3.**

Application Note: The RSA Key Pair generation algorithm meets [FIPS 186-4], chap. 5.1 and adapts method in Appendix B.3.3. The TOE uses RSA keygen method to generate 'SSH host key' which is used as client key within the SSH protocol.

6.2.3.3 FCS_CKM.4/DH Cryptographic key destruction

FCS_CKM.4.1/DH The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with 0** that meets the following: **none.**

Application Note: Whenever a Trusted Channel is terminated for whatever reason, all temporary session keys are erased from the volatile memory by the post-processing routines associated with the Trusted Channel. These session keys are generated by FCS_CKM.1/DH

6.2.3.4 FCS_CKM.4/RSA Cryptographic key destruction

FCS_CKM.4.1/RSA The TSF shall destroy cryptographic (RSA) keys in accordance with a specified cryptographic key destruction method **overwriting with 0** that meets the following: **none**

Application Note: This SFR was refined to RSA keys in the non-volatile memory only. The RSA Keys will be stored in flash memory. The private key cannot be exported.

According to A.PhysicalProtection, the iBMC is deployed in a secured environment. Therefore, the key destruction mechanism for RSA keys in non-volatile memory is intended to be used when the TOE is leaving the secured area (e.g. when decommissioned) to destroy residual information. There is no destruction mechanism to selectively destroy RSA keys during regular use of the TOE.

6.2.3.5 FCS_COP.1/AES Cryptographic operation

FCS_COP.1.1/AES The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **AES,** with operating modes, key sizes and underlying standards as defined in the following table.

Table 6-2 AES operating modes supported by the TOE for symmetric encryption and decryption

AES operating mode	Cryptographic key sizes [bits]	Meeting the standards
GCM mode	128, 256	[FIPS 197], [NIST SP 800-38D]
CTR mode	128, 192, 256	[FIPS 197], [NIST SP 800-38A]

Application Note:

AES-128, 192, 256 in CTR mode is used for encryption and decryption within SSH communication.

AES-128/256 in GCM mode is used for encryption and decryption within SSH/TLS communication.

6.2.3.6 FCS_COP.1/RSA Cryptographic operation

FCS_COP.1.1/RSA The TSF shall perform **asymmetric authentication** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048 to 4096bits** that meet the following: **RSA Cryptography Standard ([PKCS#1 V2.1], RSASSA-PKCS1-v1_5 for SSH and TLS).**

Application Note: RSA with key size of 2048 according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 is used for asymmetric authentication for SSH according to chap. 6.6 of [RFC 4253], ssh-rsa as well as 'publickey' authentication of the TOE (as SFTP client) to the server for SSH according to chap. 7 of [RFC 4252].

RSA with key size of 2048 to 4096bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 is used for asymmetric authentication of TLS.

Certificates used by TLS are imported by users into the TOE. Therefore, the TOE does not provide path validation capabilities for X.509 certificates. It is assumed that the weak RSA key (size less than 2048 bits) and hashing algorithms will not to be imported into the TOE. If the hashing algorithms specified in the certificates are not supported by the TOE, the TLS communication will not be established successfully.

6.2.3.7 FCS_COP.1/HMAC-SHA2 Cryptographic operation

FCS_COP.1.1/HMAC-SHA2 The TSF shall perform **data integrity generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA2** and cryptographic key sizes **256/512 bits** that meet the following: [RFC 2104], [FIPS 198-1]

Application Note: HMAC-SHA2-256/ HMAC-SHA2-512 is used for integrity protection of SSH communication.

6.2.3.8 FCS_COP.1/SHA256 Cryptographic operation

FCS_COP.1.1/SHA256 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA256** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA256 is used in TLS communication.

6.2.3.9 FCS_COP.1/SHA384 Cryptographic operation

FCS_COP.1.1/SHA384 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA384** and cryptographic key sizes **None** that meet the following: **[FIPS 180-4].**

Application Note: SHA384 is used in TLS communication.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **5** (consecutive) unsuccessful authentication attempts occur related to **user logging in**.

Application Note: The TSF detects the number of times the user enters the wrong password continuously, and locks the user when the maximum number of settings is reached. The number of errors can be configured, default is 5 times.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall

1. lock the offending user

2. record the event in the security log

Application Note: When the defined number of unsuccessful authentication attempts is exceeded, the TSF terminates the user attempting to authenticate and locks the user account. The lock time can be configured, default is 5 minutes.

6.2.4.2 FIA_ATD.1 User Attribute Definition

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

1. user ID and user name

2. user validity period

3. user level

4. password

5. password validity period

6. the inactivity time after which an account is automatically logged out

7. Status of the account (locked/unlocked)

8. number of failed consecutive logins within certain period of time and timestamp of last successful login

6.2.4.3 FIA_UAU.2 User authentication before any action

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.

Application Note: Authentication is possible by username and password.

6.2.4.4 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide the following authentication mechanisms:

1. Remote authentication by LDAP

2. Local Authentication by local user name and password of TOE

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's identity according to the following:

1. For Remote authentication by LDAP

2. For local Authentication, the TSF will authenticate the users based on the configured Identification (including user name and password)

6.2.4.5 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only **bullets(•)** or **asterisks(*)** to the user while the authentication is in progress.

6.2.4.6 FIA_UID.2 User identification before any action

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.

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***modify the behavior, determine the behavior of*** the functions **defined in FMT_SMF.1** to **users with sufficient user level as defined in FMT_SMR.1**.

Application Note: Access control of the TOE works as follows: All user are assigned to user roles and scope. User roles are used to control the set of commands that can be executed, and scopes are used to control the set of operating objects. Users can only execute a command if their associated user roles match the permissions of this command, and operational resources are within the scope that the user can operate on. The management of user roles also depends on this access control mechanism.

6.2.5.2 FMT_SMF.1 Specification of Management Functions

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

1. **Management of user accounts, authentication data and role association**
2. **Management of security banner, authentication failure policy**
3. **Management of customized user role and its authorities**
4. **Management of cypher suites**
5. **Management of the security audit records, audit configuration**
6. **Management of the session policy**
7. **Management of the time, NTP configuration**

6.2.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. **Administrator (as defined in the table below)**
2. **Operator (as defined in the table below)**
3. **Common User (as defined in the table below)**
4. **Custom Role(as defined in the table below)**

Table 6-3 User roles

Role	Authority
Common User	Users assigned with the Common User role has only the permission to modify his own password and view information, excluding OS information and operation logs.
Operator	Users assigned with the Operator role has all configuration and control rights, excluding user management, fault diagnosis, and security configuration.
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations.
Custom Role	The administrator can define up to 4 customized roles with customized permission.

Application Note: For roles Common user, Operator and Administrator, the roles are hierarchical, i.e. each role includes all authorities of the previous roles in addition to the authorities described for the role itself.

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable Timestamps

FPT_STM.1.1 The TSF shall be able to provide reliable timestamps.

Application Note: The reliable time stamps are based on the information of the real time clock (RTC) of the hardware. The RTC is not part of the TOE.

TOE can also connect to the NTP server and get reliable time stamps from the NTP server which is not part of the TOE.

6.2.7 TOE access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **a time interval of user inactivity which is default or can be configured.**

Application Note: When the session is idle for more than a certain period of time, the TSF terminates the current session. For Web GUI sessions, the time interval of user inactivity is configurable by the user with administrator privileges, a minimum of 5 minutes, a maximum of 480 minutes, and a default of 5 minutes. For Redfish sessions, the time interval of user inactivity is configurable by the user with administrator privileges, a minimum of 30 seconds, a maximum of 1440 minutes, and a default of 5 minutes. For SSH and CLI sessions, the time interval of user inactivity is a default of 15 minutes and not configurable.

6.2.7.2 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application Note: Access banner is enforced by the Web GUI only.

6.2.7.3 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

1. **Authentication failure**
2. **User is locked**
3. **Login rules limitation based on IP address, MAC address and time segment**

6.2.8 Trusted Path/Channel (FTP)

6.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **authentication**.

Application Note: The TOE Use TLS to establish a secure channel to communicate with the LDAP server. The TLS protocol shall be used that complies with RFCs 5246 [RFC 5246] and 4346 [RFC 4346]. For Key Exchange the ECDHE, DHE, RSA algorithm shall be used which is in agreement with [RFC 5246] and [RFC 4346]. For authentication the RSA algorithm shall be used which is in agreement with [RFC 8017].For encryption the AES-128/256 algorithm (GCM) shall be used which is in agreement with [RFC 5288]. For Data Integrity, the HMAC-SHA2 algorithm shall be used which is in agreement with [RFC 6234].

6.2.8.2 FTP_TRP.1 Trusted path

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 ***initial user authentication***.

Application Note:

a) To establish a trusted path, the TLS protocol shall be used that complies with [RFC 5246] and [RFC 4346]. For Key Exchange the ECDHE, DHE, RSA algorithm shall be used which is in agreement with [RFC 5246] and [RFC 4346]. For authentication the RSA algorithm shall be used which is in agreement with [RFC 8017].For encryption the AES-128/256 algorithm (GCM mode) shall be used which is in agreement with [RFC 5288]. For Data Integrity, the HMAC-SHA2-256 or HMAC-SHA2-384 algorithm shall be used which is in agreement with [RFC 6234].

b) To establish a trusted path, the SSH protocol shall be used that complies with [RFC 4251], [RFC 4252], [RFC 4253] and [RFC 4254]. For encryption the AES-128/192/256 algorithm (CTR mode) shall be used which is in agreement with [RFC 4253], AES-128/256 algorithm

(GCM mode) shall be used which is in agreement with [RFC 3268]. For Data Integrity, the HMAC-SHA2-256 or HMAC-SHA2-512 algorithm shall be used which is in agreement with [RFC 4253]. For Key Exchange the diffie-hellman-group1-sha1, diffie-hellman-group1-sha256 algorithm shall be used (AES encryption) which is in agreement with [RFC 4253]. For client user authentication the TOE shall support password authentication according to chap. 9.4.5 [RFC 4251] and chap. 8 [RFC 4252], respectively. Server authentication is performed using RSA according to chap. 6.6 of [RFC 4253], ssh-rsa. In addition, SFTP (i.e. FTP based on SSH protocol) is supported for secure file transfer.

6.3 Security Functional Requirements Rationale

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 6-4 Mapping SFRs to objectives

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit O.Authorization
FAU_STG.1	O.Audit O.Authorization
FAU_STG.3	O.Audit
FCS_CKM.1/DH FCS_CKM.1/RSA	O.Communication
FCS_CKM.4/DH FCS_CKM.4/RSA	O.Communication
FCS_COP.1/AES FCS_COP.1/RSA FCS_COP.1/HMAC-SHA2 FCS_COP.1/SHA256 FCS_COP.1/SHA384	O.Communication
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_UAU.2	O.Authentication

FIA_UAU.5	O.Authentication
FIA_UAU.7	O.Authentication
FIA_UID.2	O.Authentication O.Authorization
FMT_MOF.1	O.Authorization O.SecurityManagement
FMT_SMF.1	O.SecurityManagement
FMT_SMR.1	O.Authorization O.SecurityManagement
FPT_STM.1	O.Authentication O.Audit
FTA_SSL.3	O.Authentication O.Communication
FTA_TAB.1	O.Authentication
FTA_TSE.1	O.Authentication O.Communication
FTP_TRP.1	O.Authentication O.Communication
FTP_ITC.1	O.Communication

6.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Table 6-5 SFR sufficiency analysis

Security objective	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN.1. Audit records include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable. Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.2. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the audit trail exceeds the size of the storage device The TSF shall roll back the oldest records as required by FAU_STG.3.

Security objective	Rationale
O.Communication	Communication security is implemented by the establishment of a trusted channel for remote users in FTP_ITC.1 and FTP_TRP.1. FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA2, FCS_COP.1/SHA256 and FCS_COP.1/SHA384 are providing the cryptographic functions required for TLS and SSH channels. Password-based user authentication requires password hashing provided by FCS_CKM.1/RSA, and FCS_CKM.1/DH addresses key generation of AES/RSA keys. FCS_CKM.4/RSA addresses key destruction of RSA keys. Note that keys of AES algorithms as a result of the DH key agreement are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination according to FCS_CKM.4/DH. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.
O.Authentication	User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. Remote user authentication by LDAP as well as authentication via local users implemented by FIA_UAU.5. The authentication information protection is implemented in FIA_UAU.7.The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1. Time validity during authentication is implemented in FPT_STM.1. Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Display security banner before session established is implemented in FTA_TAB.1. Rejection of connections is addressed by FTA_TSE.1. User authentication via RMTs requires the use of a trusted path according to FTP_TRP.1.
O.Authorization	Permission control of audit records is implemented in FAU_SAR.2 and FAU_STG.1. User identification is addressed in FIA_UID.2. User IDs and user levels are bound to management sessions and available for access control decisions. User-related attributes are spelled out in FIA_ATD.1. Security Management is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1 and FMT_MOF.1.

Security objective	Rationale
O.SecurityManagement	The requirements on management of security functions behavior, security attributes, and static attribute initialization are provided in FMT_MOF.1 and FMT_SMF.1. The management functionality for the security functions of the TOE is defined in FMT_SMF.1 and the security user roles are defined in FMT_SMR.1.

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 6-6 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	TLS/SSH: FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	TLS/SSH: FCS_CKM.1/RSA FCS_CKM.4/RSA

Security Functional Requirement	Dependency	Resolution
FCS_COP.1/HMAC-SHA2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH FCS_CKM.4/DH
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1 and FCS_CKM.4
FCS_COP.1/SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1 and FCS_CKM.4
FCS_CKM.1/DH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/AES FCS_COP.1/HMAC-SHA2 FCS_CKM.4/DH
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA FCS_CKM.4/RSA
FCS_CKM.4/DH	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/DH
FCS_CKM.4/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No Dependencies	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	No Dependencies	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	No Dependencies	None
FTA_SSL.3	No Dependencies	None
FTA_TAB.1	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None

Security Functional Requirement	**Dependency**	**Resolution**
FTP_ITC.1	No Dependencies	None

6.3.4 Justification for unsupported dependencies

FCS_COP.1/SHA256, FCS_COP.1/SHA384 do not support dependencies of FCS_CKM.1 and FCS_CKM.4, because SHA256 and SHA384 are hash only algorithms, do not need keys for operation.

Other dependencies are supported.

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 with augmentation ALC_FLR.1, as specified in [CC] Part 3.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 2 with augmentation ALC_FLR.1 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL2) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

7 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 7-1 Mapping of Security Functionality to Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in Case of Possible Audit Data Loss
	FPT_STM.1	Reliable time stamps
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User Attribute Definition

	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Functionality Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
	FTA_TSE.1	TOE session establishment
Trusted Path/Channel	FTP_TRP.1 FTP_ITC.1	Trusted path Inter-TSF trusted channel

7.1 Security Audit

- The TOE provides an audit trail consisting of operation logs and security logs: support recording non-query operations in the operation logs, security-relevant operations in the security logs, the TOE generation of audit logs for the following events:

  i. User activity

     1. login, logout
     2. add, delete, modify users
     3. user password change
     4. user level change
     5. user lock and unlock

  ii. System management

     1. perform security management functions which are defined in FMT_SMF.1 Specification of Management
     2. Power on, power off, and restart the service system

- Operation logs and Security logs record the following information: the operation interface (if applicable), access IP address (if applicable), date and time, the outcome, and subject identity (if applicable), for all audit events the corresponding timestamp will be recorded together with the event.
- Users with security configuration rights can query and dump operation logs and security logs, can know that whoever accesses and logins the system and any operation on the system according to the content of the security log and the operation log.
- The iBMC log is saved in the flash file system of the iBMC in real time, the logs will not be lost when the system is powered off or restarted, does not allow manual changes.
- The operation logs and security logs keep records in time sequence. When the size of the log file reaches the specified size, the log file is automatically backed up.
- Operation logs and security logs support syslog. You can configure a syslog server to restore logs to a remote syslog server.

  (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3, FPT_STM.1)

7.2 Cryptographic functions

Cryptographic functions are required by security features as dependencies. These encryption algorithms protect the confidentiality and integrity of key data transmission and storage and prevent information disclosure. The following cryptographic algorithms are supported:

1) The TOE supports symmetric encryption and decryption using the AES algorithm. The TOE support the following algorithms.

   GCM mode, and cryptographic key sizes **256bits** that meet the following: **[FIPS 197], [NIST SP 800-38D]**

   GCM mode, and cryptographic key sizes **128bits** that meet the following: **[FIPS 197], [NIST SP 800-38D]**

   CTR mode, and cryptographic key sizes **128bits** that meet the following: **[FIPS 197], [NIST SP 800-38A]**

   CTR mode, and cryptographic key sizes **192bits** that meet the following: **[FIPS 197], [NIST SP 800-38A]**

   CTR mode, and cryptographic key sizes **256bits** that meet the following: **[FIPS 197], [NIST SP 800-38A]**

   AES-128/192/256 in CTR mode is used for encryption and decryption within SSH communication.

   AES-128/256 in GCM mode is used for encryption and decryption within SSH/TLS communication.

2) The TOE supports asymmetric authentication using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 with a key length of 2048/4096 bits for SSH communication.
3) The TOE supports keyed-hash message authentication using the HMAC-SHA256 and HMAC-SHA512 algorithm according to [FIPS 180-4]. This mechanism is used for the SSH communication. For all cipher suites defined in [RFC 5246] and [RFC 3268] it is used especially for data integrity protection. (For the remaining cipher suites defined in [RFC 5288] the mechanism is used according to [RFC 5288].)

4) SHA256 and SHA384 are used in TLS communication as hashing function.
5) The TOE supports generation and distribution of cryptographic keys according to diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048 bits according to [NIST SP 800-56A], [RFC 4253], [RFC 3526], [PKCS#3] for SSH/TLS.
6) The TOE supports destruction of temporary session keys used for secure communication channels based on TLS or SSH which are stored in volatile memory by erasing the corresponding area in memory reserved for the corresponding session. So the session keys are destroyed by the post-processing routines of the underlying trusted channel which are executed whenever a session is terminated for any reason.
7) The TOE supports the destruction of RSA keys through overwriting with 0, the destruction mechanism has to be triggered manually.
8) The TOE supports the SSH protocol according to [RFC 4251], [RFC 4252], [RFC 4253], [RFC 4254] and the following cipher suites according to [RFC 4253]:
   - Diffie-hellman-group14-sha1/diffie-hellman-group-exchange-sha1/diffie-hellman-group-exchange-sha256 as key exchange algorithm of SSH.
   - RSA (2048/4096 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (client) to the server.
   - HMAC-SHA2-256/HMAC_SHA2_512 data integrity generation and verification algorithm.
9) The TOE supports the HTTPS (TLS1.1/TLS1.2) protocol according to [RFC 4346] and [RFC 5246]. and the following cipher suites according to [RFC 8492]:
   - ECDHE, DHE, RSA as key exchange algorithm of HTTPS.
   - RSA (2048 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (server) to the client.

(FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA2, FCS_CKM.1/DH, FCS_CKM.1/RSA, FCS_CKM.4/DH, FCS_CKM.4/RSA, FCS_COP.1/SHA256, FCS_COP.1/SHA384)

7.3 Identification and Authentication

The TOE can identify users based on unique IDs and enforce their authentication before granting them access to any TSF management interfaces. Detailed functions include:

- Support for user individual attributes including the user ID, user level, and password to ensure that each user is unique in the system. TOE record user name, password, and user level for each local user. User privilege determine which TOE functions can be used， user privilege include user management, basic management, remote control, VMM, security management, power control, diagnostics, query and own password & SSH configuration.
- The TOE support authentication via local username and passwords. This function is achieved by comparing user information input with pre-defined user information stored in the flash. Users must successfully identify and authenticate before they are allowed to use TOE functions. The TOE enforces a password complexity :

  Contains 8 to 20 characters.

  Contains at least one space or the following special characters: `~!@#$%^& () -_=+\|[ ];: '", <.>/"*

  Contains at least two of the following combinations: lowercase letters a-z, uppercase letters A-Z, and digits 0-9

  Cannot be the same as a user name or the user name in reverse order.

- Support authentication via the remote LDAP authentication server. The TOE hands identification and authentication information provided by the user during login to the LDAP server and enforces the LDAP server's pass/fail decision.
- The password entered by the user is not displayed in plaintext during authentication. The password is displayed as asterisks (*).
- Support logout when no operation is performed on the user session within a specified interval. If an account that has logged in does not exchange information with the TOE within the specified interval, it will be automatically logged out. The account needs to be authenticated again for a new login.
- Support maximum attempts for authentication failures. By default, after five consecutive login attempts using one account fail, the account is locked. A log is recorded after the account is locked. The default value of lock period is 5 minutes, the user account will be automatically unlocked after 5 minutes by default.
- The TOE controls access by the group-based authorization framework with predefined role groups for management. Four hierarchical access groups are offered and can be assigned to individual user accounts.
- Only authenticated users can execute commands of the TOE. Only one user level can be assigned to a user account. So the user level of a user is unambiguous at any time. All authenticated users of the TOE are administrative users of some kind belonging to one of the user levels defined below. There are no authenticated non-administrative users.
- Accounts are managed in groups and each group represents a specific authority assigned to the accounts in the group. **Error! Reference source not found.** lists the groups and their definition. For example, the accounts of the "administrator" group are authorized to perform all security management and advanced diagnosis operations. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations.

Table 7-2 Groups of accounts

Group	Authority
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations.
Operator	Users assigned with the Operator role has all configuration and control rights, excluding user management, fault diagnosis, and security configuration.
Common User	Users assigned with the Common User role has only the permission to modify his own password and view information, excluding OS information and operation logs.
Custom Role	The system administrator defines the permission of custom users as required. The iBMC supports a maximum of four custom users. System permissions consist of common settings, remote control, remote media, security configuration, power control, diagnosis, query permissions, and configuration. Administrators can set any combination of them as a custom role's permission.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2)

7.4 Security Management

The TOE offers management functionality for its security functions.

The security functions include:

- Management of user accounts, authentication data and role association
- Management of security banner, authentication failure policy
- Management of customized user role and its authorities
- Management of cypher suites
- Management of the security audit records, audit configuration
- Management of the session policy
- Management of the time, NTP configuration.

There are four hierarchical user levels: Administrator, operator, common user and custom user as described in 7.3 Identification and Authentication

- A user level is assigned to each account.
- Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations.
- In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user level attribute beyond their own user level.
- Only the administrator has the permission to configure all user, including password change and permission modification. Users of other roles can only configure themselves.

(FMT_MOF.1, FMT_SMF.1, FMT_SMR.1)

7.5 TOE Access

The session timeout period can be configured on the iBMC. If you do not perform any operation for a long time, the session will be automatically disconnected. You can also configure warning information on the iBMC login page to prompt all login users. If a user fails to log in to the system for multiple times, the user is locked. The number of login failures and the locking duration are configurable.

The session can be terminated in either of the following ways:

1. Termination upon timeout: If a web, or SSH session is inactive until the timeout period expires, the session is automatically disconnected.
2. Manual termination: A user initiates a request to terminate a session. The system administrator can terminate sessions initiated by other users.

The TOE supports configuration of default access banner. Before user authentication, warning information is displayed on the page. The warning information can be configured by users. The TOE supports the anti-brute force cracking mechanism, Accounts can be locked based on consecutive login failures.

The iBMC software supports scenario-based login restriction, and access control policy based on time range, IP address, and MAC address. Only the users complying with the configured login time, IP address segment, or MAC address segment are allowed to access the system through the management channel. In this way, the access control of the server management interface is controlled within the minimum range.

(FTA_SSL.3, FTA_TAB.1, FTA_TSE.1)

7.6 Trusted Path/Channel

The TOE provides communication security by implementing trusted channels using the TLS communication protocol. The TOE acts as a TLS server and allows other trusted IT products to initiate communication. The TLS certificates for server authentication are managed and issued by users. The TOE supports TLS certificate loading and activation. Client authentication is performed password-based on the application layer. The TOE has been loaded with a preset TLS certificate before delivery.

The following TLS ciphers are supported by the TOE:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5288
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288

The TOE provides communication security by establishing a trusted channel for secure file transfer based on the SSH (SFTP) protocol. The TOE acts as a SFTP client which initiates communication with other trusted IT products. The SSH/SFTP-based communication is based on the following algorithms and ciphers, for details of the cipher, please refer to chapter 7.8:

- Authentication can be performed either public key-based or password-based as described in RFC 4252.
- Key exchange is performed using Diffie-hellman-group14-sha1/diffie-hellman-group-exchange-sha1/diffie-hellman-group-exchange-sha256 algorithms.
- The public key algorithm of the SSH transport implementation is ssh-rsa.
- For data encryption AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM and AES256-GCM are supported.
- For data integrity protection HMAC-SHA2-512 and HMAC-SHA2-256 are supported.

During LDAP authentication, the TOE Use TLS to establish a secure channel to communicate with the LDAP server.

The TOE supports session time-out after a configurable time of user inactivity. After the session has expired, the equipment user account will be automatically logged out.

The TOE supports denying session establishment based on authentication failure (i.e. device authentication failure for TLS and user authentication as well as device authentication failure for SSH).

(FTP_ITC.1, FTP_TRP.1)

A Abbreviations, Terminology and References

A.1 Abbreviations

CC	Common Criteria
PP	Protection Profile
LDAP	Lightweight Directory Access Protocol
RSA	Rivest Shamir Adleman
SDH	Synchronous Digital Hierarchy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

A.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator: An administrator in the content is the user of the TOE who may have been assigned specific administrative privileges within the TOE.

User: A user is a human or a product/application using the TOE.

A.3 References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017

[FIPS 180-4] FIPS PUB 180-4 – Secure Hash Standard (SHS)， August 2015

[FIPS 186-4] FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013

[FIPS 197] FIPS PUB 197 – Advanced Encryption Standard (AES), November 26, 2001

[FIPS 198-1] FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC), July 2008

[NIST SP 800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001

[NIST SP 800-38D] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[NIST SP 800-56A] NIST Special Publication 800-56A Rev.3 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[NIST SP 800-56B] NIST Special Publication 800-56B Rev. 2 – Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, March 2019

[PKCS#1 V2.1] PKCS #1 v2.1: RSA Cryptography Standard, June 2002

[PKCS#3] PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993

[RFC 2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC 3174] RFC 3174 - US Secure Hash Algorithm 1 (SHA1), September 2001

[RFC 3268] RFC 3268 - Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002

[RFC 3526] RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003

[RFC 4250] RFC 4250 - The Secure Shell (SSH) Protocol Assigned Numbers, January 2006

[RFC 4251] RFC 4251 - The Secure Shell (SSH) Protocol Architecture, January 2006

[RFC 4252] RFC 4252 - The Secure Shell (SSH) Authentication Protocol, January 2006

[RFC 4253] RFC 4253 - The Secure Shell (SSH) Transport Layer Protocol, January 2006

[RFC 4254] RFC 4254 - The Secure Shell (SSH) Connection Protocol, January 2006

[RFC 4346] RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[RFC 4634] RFC 4634 - US Secure Hash Algorithms (SHA and HMAC-SHA), July 2006

[RFC 5246] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

[RFC 5288] RFC 5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008

[RFC 6234] RFC 6234 – US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), May 2011

[RFC 8017] RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016

[RFC 8492] RFC 8492 - Secure Password Ciphersuites for Transport Layer Security (TLS), February 2019