D'Amo Agent v4.0

Security Target

Version 1.3

The Security Target related to the certified TOE.

This Security Target is written in Korean and translated from Korean into English.

Penta SECURITY

Revision History

Version	Revision Date	Reason for Revision
1.0	2020.01.28	- First issue
1.1	2021.03.02	- Changing component content
1.2	2021.06.18	- Modification requests reflected
1.3	2021.10.01	- Modification requests reflected

Table of Contents

1 SECURITY TARGET INTRODUCTION

This document is Penta Security Systems' D'Amo Agent v4.0 Security Target that complies with the EAL1+ level of the Common Criteria for information protection systems.

1.1 SECURITY TARGET REFERENCES

This ST is identified as follows.

Table 1-1 Security target references

Title	D'Amo Agent v4.0 ST
Version	v1.3
Author	Penta Security Systems Inc. Quality Management Division, Quality Team 2
Release	1st October 2021
Evaluation standard	Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning Notice No. 2013-51, 2013.8.8.)
CC version	CC V3.1 r5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1 added)
Protection profile compliance	Korean National Protection Profile for Database Encryption v1.1
Keyword	Databases, Encryption

1.2 TOE REFERENCES

The TOE that complies with this ST is identified as follows.

Table 1-2 TOE REFERENCES

TOE Identification	D'Amo Agent v4.0
TOE detailed version	D'Amo Agent v4.0.5 - Agent: D'Amo BA-SCP v4.0.5, D'Amo DA v4.0.5 - Key management server: D'Amo KMS v4.0.5 - Key management server console: D'Amo KMS console v4.0.5 User manual - D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo DA) - D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo BA-SCP) - D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo KMS)
TOE Developer	Penta Security Systems Inc., D'Amo development department DA Team, DX Team

1.3 TOE OVERVIEW

1.3.1 TOE OVERVIEW

TOE is a DB encryption system that protects internal assets from attackers by encrypting user data stored in the DB to be protected. The main security functions provided by the TOE include encryption/decryption of data stored in the DB, encryption key management, and auditing.

1.3.2TOE type and scope

The TOE is provided in the form of software and provides encryption/decryption functions for user data.
The types of TOE defined in this ST are database encryption products of 'Plug-in' and 'API', and the TOE is an agent (hereinafter referred to as 'SA') and a key management server (hereinafter referred to as 'KMS').) and a key management server Console (hereinafter referred to as 'KMS Console').

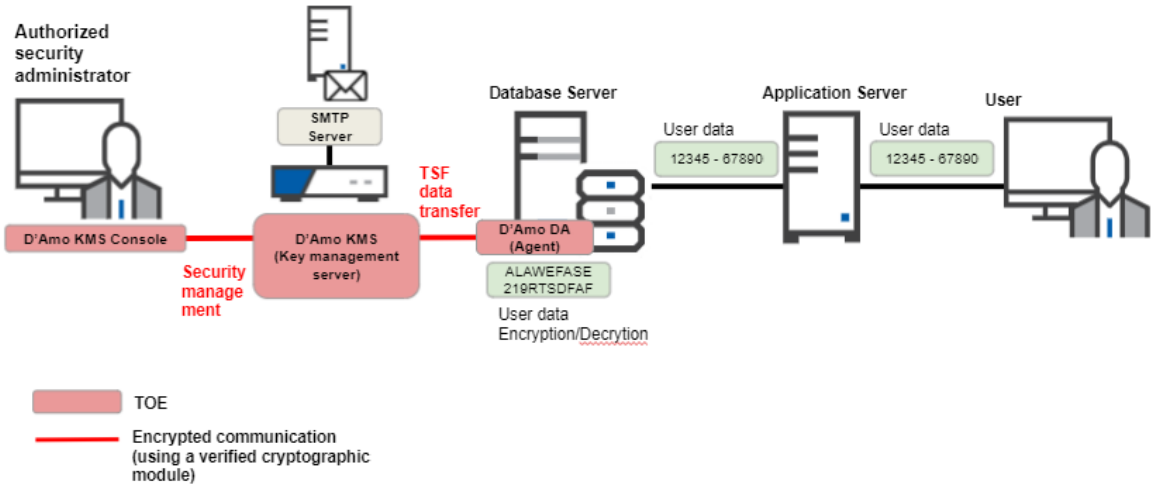
1.3.3TOE Purpose and Major Security Characteristics

The TOE is used to encrypt user data according to the policy set by the authorized administrator to prevent unauthorized exposure of the information to be protected. The TOE has a security audit function that records and manages audit data for major audit Table events, encryption key management for user and TSF data encryption, cryptographic operation, etc. password support function, user data protection function that encrypts user data and protects residual information, identification and authentication functions such as authentication of authorized administrator identity, authentication failure handling, mutual authentication between TOE components, security function and role definition, environment Security management function for setting, protection of TSF data transmitted between TOE components, protection of TSF data stored in storage controlled by TSF, TSF protection functions such as TSF self-test, TOE access for managing access session of authorized administrator function is provided. The data encryption key (DEK, Data Encryption Key) used to encrypt and decrypt user data is encrypted and protected with the key encryption key (KEK, Key Encryption Key).

1.3.4TOE operating environment

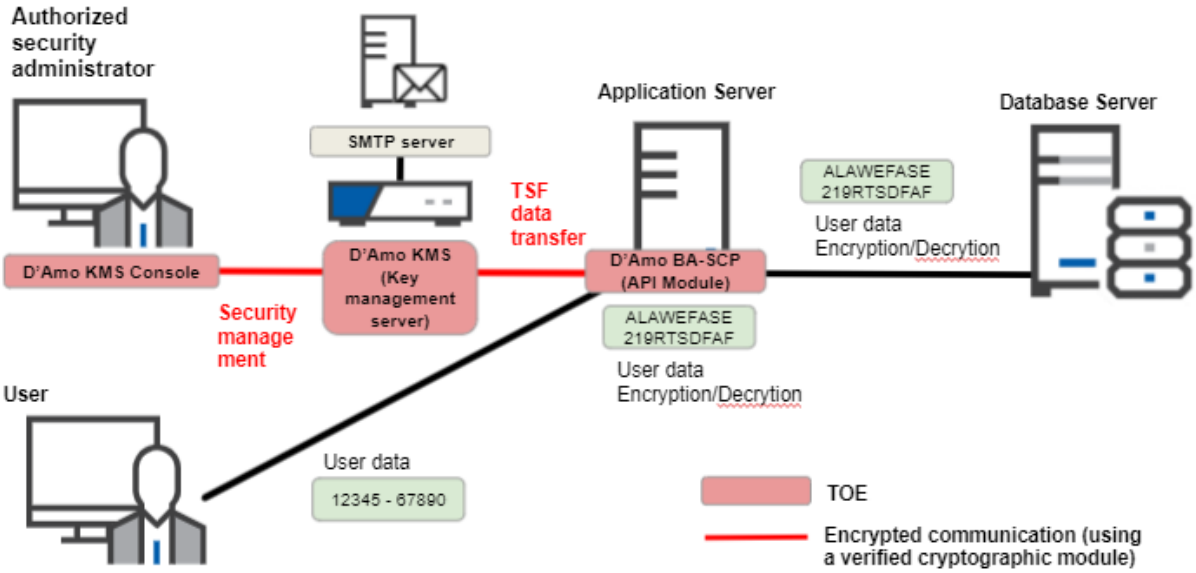
The TOE operating environment can be divided into 'Plug-in method' and 'API method'.
[Figure 1-1] shows the operating environment of 'Plug-in'. First, D'Amo DA (Plug-in module) is installed in the database server where the DB to be protected exists, and according to the policy of the authorized security administrator, user data received from the application server is encrypted before being stored in the DB. Then, decryption of encrypted user data transmitted from Database Server to Application Server is performed. KMS and KMS Consoles are installed physically separately from each other.

Figure 1-1 TOE operating environment: Plug-in method (agent, management server separate type)



[Figure 1-2] shows the operating environment of 'API method'.
Applications installed in the application server and providing application services are developed using the API provided by the API module to use the TOE cryptographic function. D'Amo BA-SCP (API module) is installed in the Application Server and performs encryption/decryption of user data according to the authorized administrator's policy. The user data entered by the application service user is encrypted by the D'Amo BA-SCP (API module) installed in the application server and transmitted to the database server. The encrypted user data transmitted from the database server is decrypted by the D'Amo BA-SCP (API module) installed in the application server and transmitted to the application service user.

Figure 1-2 TOE operating environment: API method (agent, management server separate type)



Transmission of TSF data between TOE components performs encrypted communication using verified cryptographic modules. In addition, even when accessing the key management server with the KMS Console that provides the management function of the authorized administrator, encrypted communication is performed using the verified encryption module.

An external IT entity required to operate the TOE includes an SMTP server for notifying authorized administrators when predicting audit data loss.

1.3.5Non-TOE required by TOE

1.3.5.1SA HW/SW/FW

The minimum requirements for the SA (D'Amo BA-SCP) operating environment in the TOE are as follows.

Table 1-3 SA (D'Amo BA-SCP) HW/SW/FW

		Minimum requirements	Remarks
H/W	CPU	Intel i3-9100 3.60 GHz or higher	
	RAM	16 GB or higher	
	HDD	50 GB or higher of space required for TOE installation	
	NIC	1 x 10/100/1000 Mbps or higher	
S/W	OS	Ubuntu 18.04 (Linux kernel 4.15) 64 bit	SA supported OS

Table 1-4 SA (D'Amo DA) HW/SW/FW

		Minimum requirements	Remarks
H/W	CPU	Intel Pentium CPU G4600 3.60 GHz or higher * PowerPC_POWER3 450 MHz or higher **	* Windows Server, Ubuntu environments only ** AIX environments only
	RAM	8 GB or higher	
	HDD	50 GB or higher of space required for TOE installation	
	NIC	1 x 10/100/1000 Mbps or higher	
S/W	OS	Windows Server 2012 R2 Standard 64bit Ubuntu 18.04 (Linux kernel 4.15) 64bit AIX 5.3 64bit	* Tibero and Cubrid can be installed on Windows Server and Ubuntu ** AIX can only be installed Tibero
	DBMS	Tibero 6 CUBRID 10.1	

1.3.5.2D'Amo KMS HW/SW/FW

The minimum requirements for the D'Amo KMS operating environment among the TOE are as follows.

Table 1-5 D'Amo KMS HW/SW/FW

		Minimum requirements	Remarks
H/W	CPU	Intel Xeon Quad Core E3-1275v6 3.80GHz or higher	
	RAM	24 GB or higher	
	HDD	100 GB or higher of space required for TOE installation	
	NIC	1 x 10/100/1000 Mbps or higher	
S/W	OS	Ubuntu 18.04 (Linux kernel 4.15) 64 bit	KMS supported OS
	DBMS	MariaDB 10.2.39	

1.3.5.3D'Amo KMS Console HW/SW/FW

The minimum requirements for the KMS Console operating environment among the TOE are as

follows.

Table 1-6 D'Amo KMS Console HW/SW/FW

		Minimum requirements	Remarks
H/W	CPU	Intel Core i7-7700 3.60 GHz or higher	
	RAM	16 GB or higher	
	HDD	20 GB or higher of space required for TOE installation	
	NIC	1 x 10/100/1000 Mbps or higher	
S/W	OS	Windows 10 Pro K 32bit	D'Amo KMS Console supported OS

1.3.5.4etc

Table 1-7 External IT entity

external IT entity	Description
SMTP Server	TOE interworks with SMTP server when sending alert mail

1.4 TOE DESCRIPTION

This section describes the physical and logical scope of the TOE.

1.4.1Physical scope of the TOE

The physical scope of the TOE is as follows <Table 1-9>. The TOE is in the form of software, and the preparation procedure and user operation manual are loaded and distributed on the CD in the form of an electronic document (PDF). The TOE is divided into API method and plug-in method according to the operating environment. The API method consists of the D'Amo BA-SCP (API module) agent, KMS, and KMS Console. The plug-in method consists of D'Amo DA (plug-in module) agent, KMS, and KMS Console.

Table 1-8 Physical scope

Category	Type	Components	Form of delivery
TOE components	S/W	● Agents: ■ D'Amo BA-SCP v4.0.5 (Install_D'Amo_BA-SCP_v4.0.5.zip), ■ D'Amo DA v4.0.5 (Install_D'Amo_DA_v4.0.5.zip) ● Key Management Server: ■ D'Amo KMS v4.0.5 (Install_D'Amo_KMS_v4.0.5.kip) ● Key Management Server Console: ■ D'Amo KMS Console v4.0.5 (Install_D'Amo_KMS_Console_v4.0.5.exe)	CD
Manual	electronic document (PDF)	Document name ● D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo BA-SCP) ● D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo	CD

		DA) ● D'Amo Agent v4.0 Preparation procedure and user operation manual v1.3(D'Amo KMS) File name ● D'Amo_Agent_v4.0_Preparation procedure and user operation manual_v1.3(D'Amo BA-SCP).pdf ● D'Amo_Agent_v4.0_Preparation procedure and user operation manual_v1.3(D'Amo DA).pdf ● D'Amo_Agent_v4.0_Preparation procedure and user operation manual_v1.3(D'Amo KMS).pdf)	

The verified cryptographic modules included in the TOE are as follows.

Table 1-9 Verified encryption module

Category	Contents
Cryptographic module name	CIS-CC v3.3
Verification number	CM-145-2023.11
developer	Penta Security Systems Inc.
verification date	2018-11-07

1.4.2Logical scope of the TOE

As shown in <Figure 1-3> and <Figure 1-4>, the TOE provides security functions (last name) such as [Security audit, password support, user data protection, identification and authentication, security management, TSF protection, TOE access] as shown in <Figure 1-3> and <Figure 1-4>. to provide.

Figure 1-3 Logical scope of the TOE: API method

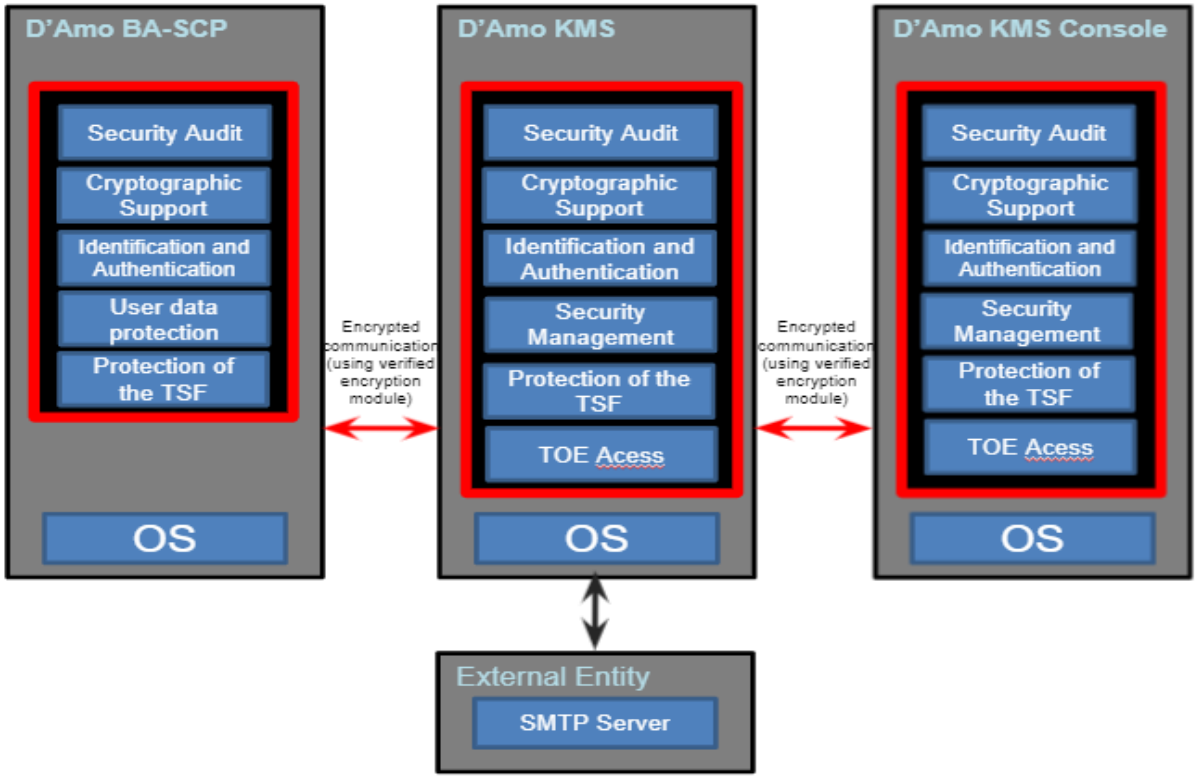
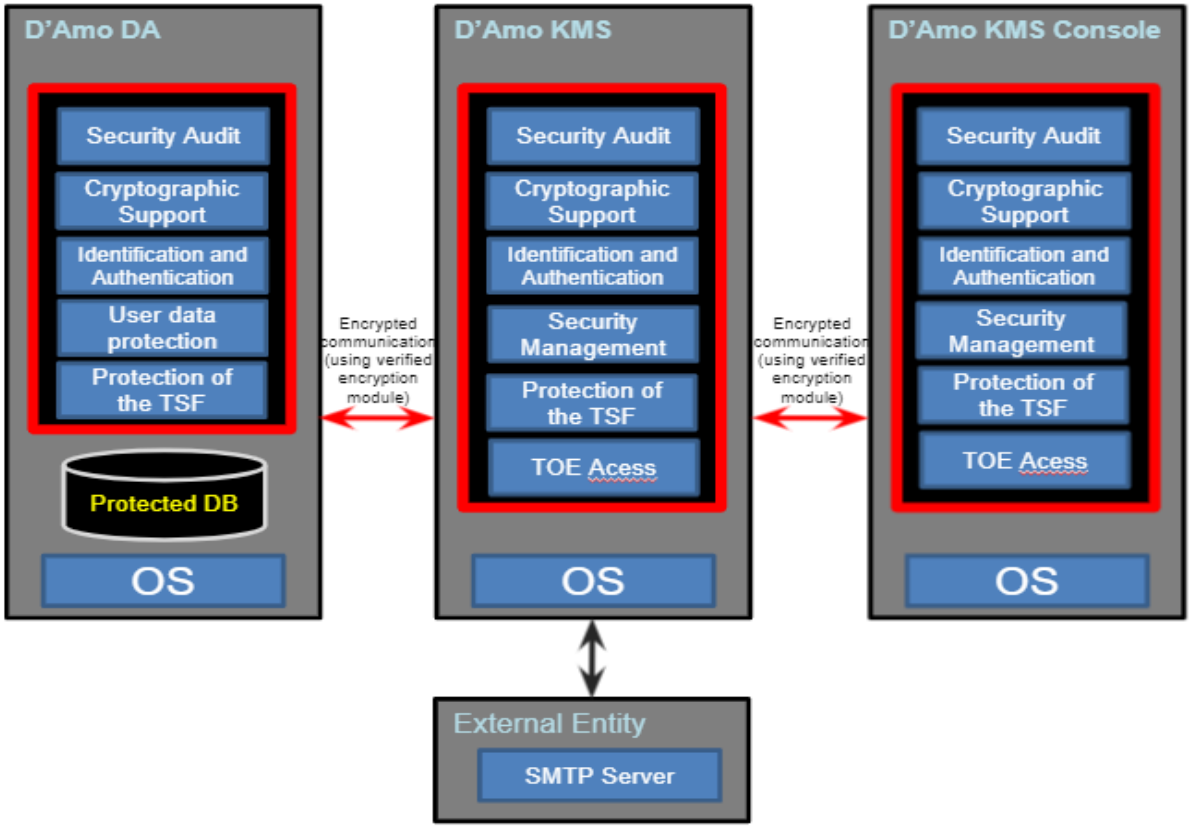


Figure 1-4 Logical scope of TOE: Plug-in method



1.4.2.1 SA logical scope

SA is an agent that actually performs encryption/decryption with the encryption/decryption policy set in the KMS Console.
Through the established encryption channel (self-implemented security protocol) between the SA and the subsystem, application of setting information and transmission/reception of requested information are performed safely.
The security functions provided through SA are as follows.

Security audit

SA creates audit data of security-related events to trace responsibility for security-related actions. SA delivers audit data to KMS.

Cryptographic Support

SA is generated using the random number generator of CIS-CC v3.3, which is a key verification encryption module required for mutual authentication with KMS.
SA performs encryption key distribution and encryption key operation during mutual authentication with KMS, and communicates with KMS after mutual authentication is completed. The encryption key used for encryption communication is destroyed in the memory area after completion of use.
In addition, encryption operation is performed when user data is encrypted/decrypted with the user data encryption key received from KMS, and the corresponding encryption key is destroyed immediately after encryption/decryption.

Identification and Authentication

SA performs mutual authentication before performing cryptographic communication between KMS.

User Data Protection

SA provides the ability to encrypt/decrypt user data and supports column-based encryption of DB. When user data encryption is executed, the remaining work Table is not left separately. When encrypting user data, the same ciphertext is not generated for the same plaintext.

Protection of the TSF

When SA transmits/receives setting information and request information to KMS, it securely encrypts data exchanged using CIS-CC v3.3 before transmitting/receiving.
SA secures and encrypts important data such as data encryption key policy using CIS-CC v3.3.
SA performs integrity checks on SA library files periodically during startup and during operation to ensure its own correct operation, and performs self-tests on key processes.

1.4.2.2KMS logical scope

As a key management system, KMS can manage all encryption keys from creation to destruction.
Through the established encryption channel (self-implemented security protocol) between SA and KMS subsystems, it safely performs setting information applications and requests information transmission/reception.
The security functions provided through KMS are as follows.
.

Security Audit

KMS creates and records audit records of security-related events to trace responsibility for security-related actions.
The KMS provides the KMS local security manager with an interface for the log inquiry function.
KMS provides the following actions for potential security violations.
When the audit trail exceeds the specified threshold or the audit trail becomes saturated, an authorized administrator is notified by e-mail. If the self-test failure of the verified cryptographic module occurs, the service is disabled. If the integrity verification of the verified cryptographic module fails at startup, the service is disabled, and if a failure occurs in the periodic verification, the authorized administrator is notified by e-mail. If integrity verification fails in other executable files, it is notified by e-mail designated by the authorized administrator. A warning message is provided when authentication failure of the KMS local security manager occurs.

Cryptographic Support

KMS generates keys required for mutual authentication with SA and KMS Consoles, a key for

encrypting user data, and a key for encrypting an encryption key using the random number generator of CIS-CC v3.3, a verified encryption module.
In case of mutual authentication with SA and KMS Consoles, KMS distributes encryption keys and calculates encryption keys, and after mutual authentication is completed, encryption communicates with SA and KMS Consoles. The encryption key used for encryption communication is destroyed in the memory area after completion of use.

Identification and Authentication

KMS performs mutual authentication before performing cryptographic communication between SA and KMS Consoles.
KMS enforces password acceptance rules (at least 9 characters in 4 combinations of uppercase English letters, lowercase English letters, numbers, and special characters). Also, it prevents exposure of input values when entering passwords (changes input characters to fake characters ('*')).

Security Management

KMS administrators are divided into KMS local security manager, KMS security manager, and KMS assistant security manager.

- KMS Local Security Manager: Control KMS internal settings via CLI.
- KMS Security Manager: Created by the KMS local security manager and all functions of the KMS console are available.
- KMS Secondary Security Manager: Created by the KMS security manager and only the inquiry function of the KMS console can be used.

Protection of the TSF

When KMS transmits/receives configuration information and request information to the SA and KMS console, it uses CIS-CC v3.3 to securely encrypt the data exchanged and then transmit/receive.
KMS securely encrypts and stores data encryption keys using CIS-CC v3.3.
In order to ensure its own correct operation, KMS periodically performs integrity checks at startup and during operation and performs self-tests on key processes.

TOE Access

If the inactivity time of the KMS local security manager exceeds a certain amount of time, KMS terminates the logged-in administrator's session to prevent access by unauthorized administrators. KMS can set the access allowed IP address of the KMS Console. Only one person can access each of KMS CLI and Console at the same time. KMS permits only the management access session attempted to access from the terminal designated by the allowed IP address. If the administrator attempts to log in from another terminal while already successfully logged in, the existing connection is maintained and new connections are not allowed.

1.4.2.3KMS Console Logical Scope

The KMS Console provides a GUI-type security management function that can operate KMS to the authorized administrator and applies and requests setting information through the encryption channel (self-implemented security protocol) established between the KMS Console and the KMS subsystem. Safely transmit and receive information.
The security functions provided through the KMS Console are as follows.

Security Audit

The KMS Console creates audit data for KMS security manager login and KMS security manager setting change.
The KMS Console provides the KMS security manager with an interface for the log inquiry function and provides the KMS security manager with the ability to selectively review audit information according to the audit data type, search criteria item, and logical relationship.
The KMS Console provides a function to set an e-mail alarm related to the overflow of the audit trail storage threshold or saturation of the audit trail among potential security violations of KMS. In

addition, a warning message is provided in case of authentication failure and violation after integrity verification.

Cryptographic Support

The KMS Console generates a key required for mutual authentication with KMS, a key for encrypting user data and setting values, and a key for encrypting an encryption key using the random number generator of CIS-CC v3.3, a verified encryption module.
In case of mutual authentication with KMS, the KMS Console distributes the encryption key and calculates the encryption key and communicates with KMS after completion of mutual authentication. The encryption key used for encryption communication is destroyed in the memory area after completion of use.

Identification and Authentication

The KMS Console performs mutual authentication before performing cryptographic communication with KMS.
The KMS Console provides the KMS security manager with an interface for certificate-based identification and authentication and performs the function of requesting identification and authentication of the security manager. If identification and authentication fail, authentication failure response function (reject identification and authentication request for 10 minutes if the maximum allowed number of authentication failures (5) is exceeded) and detailed information related to the cause of authentication failure is not provided
The KMS Console enforces password acceptance rules (at least 9 characters in 4 combinations of uppercase English letters, lowercase English letters, numbers, and special characters). Also, it prevents exposure of input values when entering passwords (changes input characters to fake characters ('*')).
The KMS Console uses time stamp to prevent reuse of authentication data used for administrator authentication.

Security Management

The KMS security manager of the KMS Console provides a security management function that can set and manage security functions and important data.
The security manager of the KMS Console manages the encryption key setting to be used when encrypting user data, the log backup setting for KMS, and the environment setting data.

Protection of the TSF

When the KMS Console transmits/receives setting information and request information to/from KMS, it uses CIS-CC v3.3 to securely encrypt the data exchanged and then transmit/receive. In order to ensure its own correct operation, KMS Console periodically performs integrity checks on executable files during startup and during operation and performs self-tests on key processes. TSF data is encrypted and stored with the verified encryption module CIS-CC v3.3 and protected from unauthorized exposure and modification. The protected TSF data is a session key used for mutual authentication, an administrator key pair.

TOE Access

The KMS Console prevents unauthorized administrator access by terminating the logged-in KMS security manager's or KMS assistant security manager's session when the security administrator's inactivity time exceeds a certain amount of time.

1.5 Writing rules

In this Security Target, some abbreviations and English are used to convey clear meanings. The notation, form, and preparation rules used follow the Common Criteria.

The CC permits Iteration, Assignment, *Selection*, Refinement operations that can be performed in the security functional requirements. Each operation is used in this ST.

Iteration

It is used when one component is repeated several times by applying various

operations. The result of the iteration operation is indicated by the iteration number in parentheses, that is, (iteration No.) after the component identifier.

Assignment
Used to assign a specific value to an unspecified parameter (e.g., password length). The result of the assignment operation is displayed in square brackets, that is, [assignment_ value].

Selection
It is used to select one or more of the options provided in the CC when describing requirements. The result of the selection operation is displayed *underlined and assignment value*

Refinement
It is used to further restrict the requirement by adding details to the requirement. The result of the refinement operation is displayed in **bold**

1.6 Terms and definitions

Among the terms used in this Security Target, the same terms used in the CC apply mutatis mutandis.

Attack potential
Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources, and motivation

Element
Minimum unit of indivisible security requirement (requirement)

Identity
A unique representation that identifies an authorized user. It may be the user's real name, an abbreviation, or a pseudonym.

Iteration
Use of the same component to express two or more distinct requirements

Object
Passive entity in the TOE containing or receiving information and on which subjects perform operations

Operation (on a component of the CC)
Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement, and selection

Operation (on a subject))
Specific type of action performed by a subject on an object

PP, Protection Profile)
Implementation-independent statement of security needs for a TOE type

Role
Predefined set of rules on permissible interactions between a user and the TOE

ST, Security Target

Implementation-dependent security requirements for a specific TOE

Selection
Specification of one or more items from a list in a component

User
See "External Entity"

External Entity
An entity (human or IT) that interacts with (or can interact with) from outside the TOE

Threat Agent
An unauthorized external entity that creates threats such as illegal access, modification, or deletion of assets

Authorized Administrator
Authorized users who safely operate and manage the TOE

- KMS Console
  - KMS Local Security Manager
  - KMS Security Manager
  - KMS Assistant Security Manager

Authorized User
Users who can execute functions according to SFR (Security Functional Requirements)

Authentication Data
Information used to prove your identity

Assets
The entity to which the owner of the TOE places a value

Refinement
To specify by adding details to a component

Organizational Security Policies
A set of security rules, procedures, practices, and guidelines that are currently or will be imposed on the operating environment by an actual or hypothetical organization.

Dependency
As a relationship between components, if a requirement based on a dependent component is included in a PP, ST, or package, the requirement based on the component (on that component) is also included in the PP, ST, or package. relationship to be included in

Subject
An active entity in the TOE that performs operations on objects

Augmentation
Adding one or more requirements to a package

Component
A collection of elements, the smallest unit of choice that can be used to form the basis of a requirement.

Class
A collection of CC families with the same security objective.

Target of Evaluation (TOE)
A set of software, firmware and/or hardware accompanied by possible documentation

Evaluation Assurance Level (EAL)
Assurance package consisting of three parts assurance requirements with predefined assurance levels in the CC

Family
A collection of components that have a similar purpose but differ in emphasis or rigor

Assignment
specifying the identified parameters within a component or requirement (of the Common Criteria)

TOE Security Functionality (TSF)
A set consisting of all hardware, software, and firmware of the TOE contributing to the correct execution of SFRs (Security Functional Requirements)

TSF Data
Data generated for the TOE by the TOE that may affect the operation of the TOE

Packet
A bundle of data used in data transmission on the Internet network

Network Time Protocol (NTP)
NTP is a protocol used to synchronize clock times to computers connected to a network. NTP was first developed by David Mills of the University of Delaware in the United States but has now become an Internet standard. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to less than 1/1000 of a second.

SA (Security Agent)
A library to provide data encryption/decryption capabilities to users

KMS (Key Management System)
As a key management server, it creates and manages KEKs and DEKs.

Agent key pair
These are public and private keys generated by KMS. It is used for mutual authentication with SA in KMS and encryption of TSF data.

KMS site key pair
These are public and private keys generated by KMS. It is used for mutual authentication with SA and KMS Consoles in KMS, and for encryption of TSF data.

KMS Console Key Pair
These are public and private keys generated by KMS. It is used for mutual authentication with KMS in KMS Console and for encryption of TSF data.

Data Encryption Key (DEK)
Encryption key (symmetric key) used to encrypt database column data

Key Encryption Key (KEK)
The DB key corresponds to the encryption key used to encrypt the data encryption key.

Session key
A symmetric key used for cryptographic communication between TOEs and performs encryption/decryption with the corresponding key when sending and receiving TSF data.

Security policy file
Save the security policy stored in the database to the OS file. Security policy refers to information necessary for encryption and product operation.

Product main security parameters
column key, security policy file

KMS Security Manager
Security administrator who can set and operate TOE security management functions through D'Amo KMS Console

KMS Assistant Security Manager
A secondary security manager who can inquire the TOE security management settings through the D'Amo KMS Console. The authority to set or operate TOE functions is limited.

KMS Local Security Manager
The only top-level security administrator who can set and operate TOE security management functions through D'Amo KMS

1.7 Structure of the Security Target

This Security Target is composed as follows.

<1. Security Target Introduction> describes the ST reference, TOE reference, TOE overview, TOE description, writing rules, terminology, and the security target structure.
<2. Conformance Claims> describes the rationale for the Common Criteria Conformity Declaration, PP Conformity Declaration, Package Conformity Declaration, and Conformity Declaration.
<3. Security Problem Definition> describes assets, threats, organizational security policies, and assumptions.
<4. Security Objectives> describes the TOE security objectives, the security objectives for the operating environment, and the rationale for the security objectives.
<5. EXTENDED COMPONENTS DEFINITION> describes TOE extended components.
<6. Security Requirements> describes the security functional requirements and assurance requirements, and the rationale for the security requirements.
<7. TOE summary specification> describes the rationale for the TOE summary specification and the TOE summary specification.

2 Conformance Claims

The conformance declaration describes how this ST complies with the Common Criteria (CC), PP and package.

2.1 CC CONFORMANCE CLAIM

This Security Target complies with the following information protection system Common Criteria Version 3.1 Revision 5

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

B. Conformance claim
   a. 2nd extension of Common Criteria for Information Security System: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
   b. Compliance with 3 parts of the Common Evaluation Criteria for Information Security Systems
   c. Add Package: Add EAL1 (ATE_FUN.1)

2.2 PP conformance clam

This security target complies with the Korean National Protection Profile for Database Encryption v1.1

2.3 Package conformance claim

This Protection Profile claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4 Rationale for Declaration of Conformity

The basis of this Security Target's declaration of conformance to the Korean National Database Encryption Protection Profile v1.1 is as follows.

Security functional class	Security functional component		Whether to declare a PP	Whether the ST is declared
Security Audit (FAU)	FAU_ARP.1	Security alarms	O	O
	FAU_GEN.1	Audit data generation	O	O
	FAU_SAA.1	Potential violation analysis	O	O
	FAU_SAR.1	Audit review	O	O
	FAU_SAR.3	SelecTable audit review	O	O
	FAU_STG.3	Action in case of possible audit data loss	O	O
	FAU_STG.4	Prevention of audit data loss	O	O
Cryptographic support (FCS)	FCS_CKM.1	Cryptographic key generation	O	O
	FCS_CKM.2	Cryptographic key distribution	O	O
	FCS_CKM.4	Cryptographic key destruction	O	O
	FCS_COP.1	Cryptographic operation	O	O
	FCS_RBG1 (Extended)	Random bit generation	O	O
User data protection (FDP)	FDP_UDE.1(Extended)	User data encryption	O	O
	FDP_RIP.1	Subset residual information protection	O	O

Identification and authentication (FIA)	FIA_AFL.1	Authentication failure handling	O	O
	FIA_IMA.1	TOE Internal mutual authentication	O	O
	FIA_SOS.1	Verification of secrets	O	O
	FIA_UAU.1	authentication	O	O
	FIA_UAU.4	Single-use authentication mechanisms	O	O
	FIA_UAU.7	Protected authentication feedback	O	O
	FIA_UID.1	Timing of identification	O	O
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour	O	O
	FMT_MTD.1	Management of TSF data	O	O
	FMT_PWD.1	Management of ID and password	O	O
	FMT_SMF.1	Specification of management functions	O	O
	FMT_SMR.1	Security roles	O	O
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection	O	O
	FPT_PST.1	Basic protection of stored TSF data	O	O
	FPT_TST.1	TSF testing	O	O
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	O	O
	FTA_SSL.5	Management of TSF-initiated sessions	O	O
	FTA_TSE.1	TOE session establishment	O	O

2.5 PP conformance statement

This Protection Profile requires "strict PP conformance" of any ST or PP, which claims conformance to this PP.

3 Security object

3.1 Security objectives for the operational environment

The following are security objectives that must be dealt with by technical and procedural means supported by the operating environment so that the TOE can accurately provide security functions.

OE. PHYSICAL_CONTROL

The place where the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

OE. TRUSTED_ADMIN

The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidance.

OE. SECURE_DEVELOPMENT

The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

OE. LOG_BACKUP

The authorized administrator of the TOE shall periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

OE. OS enhancement

The TOE must ensure the reliability and safety of the operating system by removing all unnecessary services and means on the operating system and reinforcing vulnerabilities in the operating system.

OE. Timestamp

The TOE must accurately record security-related events using the reliable timestamp provided by the TOE operating environment.

OE. Audit trail protection

It should be protected from unauthorized deletion or modification of audit records in which audit trails are stored, such as DBMS that interacts with the TOE.

4 Extended components definition

4.1 Cryptographic Support (FCS, Cryptographic support)

4.1.1 Random bit generation

Family Behaviour
This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Component leveling

FCS_RBG.1 random bit generation, requires TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Management: FCS_RBG.1
There are no management activities foreseen.

Audit: FCS_RBG.1
There are no audit table events foreseen.

4.1.1.1 FCS_RBG.1.1 Random bit generation

Hierarchical to No other components.
Dependencies No dependencies.

FCS_RBG.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following [assignment: list of standards].

4.2 Identification and authentication (FIA, Identification & authentication)

4.2.1 TOE Internal mutual authentication

Family behaviour
This family defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component leveling

FIA_IMA.1 TOE Internal mutual authentication requires that the TSF provides mutual authentication function between TOE components in the process of user identification and authentication.

Management: FIA_IMA.1
There are no management activities foreseen.

Audit: FIA_IMA.1
The following actions are recommended to record if FAU_GEN Security audit data generation family is included in the PP/ST:
a) Minimal: Success and failure of mutual authentication
b) Minimal: Modification of authentication protocol

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication between [assignment: different parts of TOE] using the [assignment: authentication protocol] that meets the following [assignment: list of standards].

4.3 User data protection (FDP, User Data protection)

4.3.1 User data encryption

Family Behaviour
This family provides requirements to ensure confidentiality of user data.

Component leveling

FDP_UDE.1 User data encryption requires confidentiality of user data.

Management: FDP_UDE.1 The following actions could be considered for the management functions in FMT:
a) Management of user data encryption/decryption rules

Audit: FDP_UDE.1 The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: Success and failure of user data encryption/decryption

4.3.1.1 FDP_UDE.1 User data encryption

Hierarchical to	No other components.
Dependencies	FCS_COP.1 Cryptographic operation

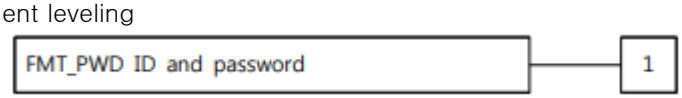
FDP_UDE.1.1	TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: the list of encryption/decryption methods] specified

4.4 Security Management (FMT, Security Management)

4.4.1 ID and password

Family Behaviour
This family defines the capability that is required to control ID and password management used in the TOE and set or modify ID and/or password by authorized users.

Component leveling



FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:
a) Management of ID and password configuration rules.

Audit: FMT_PWD.1
The following actions are recommended to record if FAU_GEN Security audit data generation is included
in the PP/ST:
a) Minimal: All changes of the password.

4.4.1.1 FMT_PWD.1 Management of ID and password

Hierarchical to	No other components.
Dependencies	FMT_SMT.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_PWD.1.1
The TSF shall restrict the ability to manage the password of [assignment: list of functions] to [assignment: the authorized identified roles].
1. [assignment: password combination rules and/or length]
2. [assignment: other management such as management of special characters unusable for password, etc.]

FMT_PWD.1.2
The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles].
1. [assignment: ID combination rules and/or length]
2. [assignment: other management such as management of special characters unusable for ID, etc.]

FMT_PWD.1.3
The TSF shall provide the capability for [selection, choose one of: setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time].

4.5 Protection of the TSF (FPT, Protection of the TSF)

4.5.1. Protection of stored TSF data

Family Behaviour
This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component leveling

FPT_PST.1 Basic protection of stored TSF data, requires the protection of TSF data stored in containers controlled by the TSF.

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1
There are no audit Table events foreseen.

4.5.1.1 FPT_PST.1 Basic protection of stored TSF data

Hierarchical to No other components.
Dependencies No dependencies.

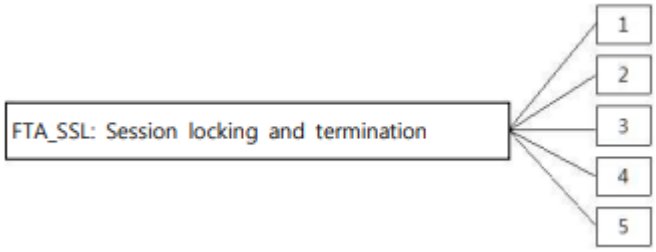
FPT_PST.1.1 The TSF shall protect [assignment: TSF data] stored in containers controlled by the TSF from the unauthorized [selection: disclosure, modification].

4.6 TOE Access (FTA, TOE Access)

4.6.1 Session locking and termination

Family Behaviour
This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Component leveling



In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.
※ The relevant description for four components contained in CC Part 2 is omitted.
FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.
FTA_SSL: Session locking and termination

Management: FTA_SSL.5
The following actions could be considered for the management functions in FMT:
a) Specification for the time interval of user inactivity that is occurred the session locking and termination for each user
b) Specification for the time interval of default user inactivity that is occurred the session locking and termination

Audit: FTA_SSL.5
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: Locking or termination of interactive session

4.6.1.1 FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to No other components.
Dependencies [FIA_UAU.1 authentication or none]

FTA_SSL.5.1 The TSF shall [selection:
• lock the session and re-authenticate the user before unlocking the session,
• terminate] an interactive session after a [assignment: time interval of user inactivity].

5. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this PP.

5.1 Security functional requirements

The security functional requirements of this ST are composed by selecting the relevant functional components from the CC Part 2 and Chapter 4 extended component definitions. The following <Table 5-1> summarizes the security functional requirements components used in this ST.

Table 5-1 Security functional requirements

Security functional class	Security functional component	
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1(1)	Audit review (KMS Security Manager)
	FAU_SAR.1(2)	Audit review (KMS Assistant Security Manager)
	FAU_SAR.1(3)	Audit review (KMS local security manager)
	FAU_SAR.3	SelecTable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic support	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2(1)	Cryptographic key distribution (User data encryption)
	FCS_CKM.2(2)	Cryptographic key distribution (Mutual authentication and cryptographic communication function between TOE components)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
User data protection	FDP_UDE.1(Extended)	User data encryption
	FDP_RIP.1	Subset residual information protection
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(1) (Extended)	TOE Internal mutual authentication (SA – KMS communication section mutual authentication)
	FIA_IMA.1(2) (Extended)	TOE Internal mutual authentication (KMS – KMS Console communication mutual authentication)
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1(1)	authentication (KMS Security Manager)
	FIA_UAU.1(2)	authentication (KMS Assistant Security Manager)
	FIA_UAU.2	User authentication before every action (KMS local security manager)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1(1)	Timing of identification (KMS Security

		Manager)
	FIA_UID.1(2)	Timing of identification (KMS Assistant Security Manager)
	FIA_UID.2	User identification before every action (KMS local security manager)
Security Management	FMT_MOF.1	Management of security functions behaviour (KMS Security Manager)
	FMT_MTD.1(1)	Management of TSF data (KMS Security Manager)
	FMT_MTD.1(2)	Management of TSF data (KMS Assistant Security Manager)
	FMT_MTD.1(3)	Management of TSF data (KMS local security manager)
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing
TOE Access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5 (Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1 Security Audit (FAU)

FAU_ARP.1 Security alarms

Hierarchical to	No other components.
Dependencies	FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [the fellowing list of actions] upon detection of a potential security violation

Table 5-2 Security alarms action list

구분	Security functional component	potential security violation.	response action
SA	FPT_TST.1	Failed self-test of verified cryptographic module	disable service
		Integrity verification failure of verified cryptographic module	- initial start-up: disable service - periodically during normal operation: Notified by e-mail designated by the authorized administrator
		Other integrity verification failures	- initial start-up: warning message output - periodically during normal operation: Notified by e-mail

			designated by the authorized administrator
KMS	FAU_STG.3	Events in which the audit trail exceeds a specified threshold	Notified by e-mail designated by the authorized administrator
	FAU_STG.4	Events with saturated audit trails	Notified by e-mail designated by the authorized administrator
	FPT_TST.1	Failed self-test of verified cryptographic module	disable service
		Integrity verification failure of verified cryptographic module	- initial start-up: Disable service - periodically during normal operation: Disable service and Notified by e-mail designated by the authorized administrator
		Other integrity verification failures	Notified by e-mail designated by the authorized administrator
	FIA_UAU.2	KMS local security manager authentication failure audit event	Account lock after 5 authentication failures
KMS Console	FPT_TST.1	Failed self-test of verified cryptographic module	disable service
		Integrity verification failure of verified cryptographic module	- initial start-up: Disable service - periodically during normal operation: Disable service and warning message output
		Other integrity verification failures	warning message output
	FIA_UAU.1	KMS Security Manager, KMS Assistant Security Manager authentication failure audit event	Account lock after 5 authentication failures

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 audit Table events for the *not specified* level of audit; and
c) [Refer to the "auditable events" in [Table 5-3] Audit events, *no other components*].

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 [Refer to the contents of "additional audit record" in [Table 5-3] Audit events, *no other components*].

Table 5-3 Audit event

Security functional component	Audit event	Additional audit record
FAU_ARP.1	Actions taken due to potential security violations	-
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	-
FAU_STG.3	Actions taken due to exceeding of a threshold	-
FAU_STG.4	Actions taken due to the audit storage failure	-
FCS_CKM.1(1)	Success and failure of the activity	-
FCS_CKM.1(2)	Success and failure of the activity	-
FCS_CKM.2(1)	Success and failure of the activity (Applies only to key distribution related to user data encryption/decryption)	-
FCS_CKM.2(2)	Success and failure of the activity (Applies only to key distribution related to user data encryption/decryption)	-
FCS_CKM.4	Success and failure of the activity (Applies only to key destruction related to user data encryption/decryption)	-
FCS_COP.1(1)	Success and failure of cryptographic operations, types of cryptographic operations	-
FCS_COP.1(2)	Success and failure of cryptographic operations, types of cryptographic operations	-
FDP_UDE.1	Success and failure of user data encryption/decryption	-
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal stat	-
FIA_IMA.1(1)	Success and failure of mutual authentication Modify of authentication protocol	-
FIA_IMA.1(2)	Success and failure of mutual authentication Modify of authentication protocol	-
FIA_UAU.1(1)	All use of the authentication mechanism	-
FIA_UAU.1(2)	All use of the authentication mechanism	-
FIA_UAU.4	Attempts to reuse authentication data	-
FIA_UID.1(1)	All use of the user identification mechanism, including the user identity provided	-
FIA_UID.1(2)	All use of the user identification mechanism, including the user identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1(1)	All modifications to the values of TSF data	Modified values of TSF data
FMT_MTD.1(2)	All modifications to the values of TSF data	Modified values of TSF data
FMT_MTD.1(3)	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1	All changes of the password	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Modifications to the user group of rules divided	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity

		violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	-
FTA_SSL.5	Locking or termination of interactive session	-
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	-

FAU_SAA.1 Potential violation analysis

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [

▪ Authentication failure audit event among auditable events of FIA_UAU.1

▪ Integrity violation audit event and selftest failure event of validated cryptographic module among auditable events of FPT_TST.1

[An event in which the audit trail of FAU_STG.3 exceeds the specified threshold, an event in which the audit trail of FAU_STG.4 is saturated, and an authentication failure audit event among the auditable events of FIA_UAU.2]

] known to indicate a potential security violation

b) [none]

FAU_SAR.1(1) Audit review (KMS Security Manager)

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAR.1.1 TSF shall provide [**KMS Security Manager**] with the capability to read [**Audit trail of KMS that can be viewed using KMS Console**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit record in a manner suitable for the **KMS Security Manager** to interpret the information.

FAU_SAR.1(2) Audit review (KMS Assistant Security Manager)

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAR.1.1 TSF shall provide [**KMS Assistant Security Manager**] with the capability to read [**Audit trail of KMS that can be viewed using KMS Console**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit record in a manner suitable for the **KMS Assistant Security Manager** to interpret the information.

FAU_SAR.1(3) Audit review (KMS local security manager)

Hierarchical to	No other components.
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**KMS local security manager**] with the capability to read [**Audit trail of KMS that can be viewed using KMS CLI**] from the audit record.

FAU_SAR.1.2 The TSF shall provide the audit record in a manner suitable for the **KMS local security manager** to interpret the information.

FAU_SAR.3 Select Table 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 [the following selection and/or ordering method] of audit data based on [the criteria having the following logical relationship].

< KMS >

a) Criteria with a logical relationship – Required (AND)

- Search period: Last few hours, set log search period
- Log Type: Service Log, System Log, Administrator Log
- Log Level: Select from Full, Warning, Error, Success, Debug
- Number of Views: Set the number of recent 500, 1000, 1500, 2000, 3000, 5000, log inquiry

b) Criteria with Logical Relationship – Choices (AND)

- Include keywords: Enter keywords to include in the log content.
- Negative keywords: Enter keywords to exclude from log content
- Excluding service self-diagnostic logs
- No selection Yes

c) method of selection and/or ordering

- Audit data search period specified by KMS Security Manager or KMS Assistant Security Manager (last 1, 6, 12, 24 hours and user-defined) AND type AND level AND number of cases
- Each item can be sorted in ascending/descending order (initial value: sort descending by time)

[Caution] For the audit trail, event type, date of occurrence (event date and time), subject, information (event type, event result), remarks (other information), etc. are provided.

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to	No other components.
Dependencies	FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notification to the authorized administrator, [response action in Table 5-4]] if the audit trail exceeds [capacity limit of audit trail inspection conditions in Table 5-4]

Table 5-4 Capacity limits and response actions for audit trail inspection conditions

Object	Capacity limit	Response action
KMS	90%	Send email notifications

FAU_STG.4 Prevention of audit data loss

Hierarchical to	FAU_STG.3	Action in case of possible audit data loss
Dependencies	FAU_STG.1	Protected audit trail storage

FAU_STG.4.1 The TSF shall *ignore the audited event* and [response action in Table 5-5] if the audit trail is full.

Table 5-5 Actions to take when predicting audit loss

Object	Capacity limit	Response action
KMS	100%	Send email notifications

5.1.2 Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic key generation (User data encryption)

Hierarchical to	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Encryption algorithm name in Table 5-6] and specified cryptographic key sizes [Encryption key length in Table 5-6] that meet the following: [Standard list in Table 5-6]

Table 5-6 Encryption algorithm to generate encryption key used for user data encryption, key length

	Standard	cryptographic algorithm	encryption key length	purpose of use
#1	TTAK.KO-12.0190	Hash_DRBG	128, 256, 384, 512	Key used for user data encryption

FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)

Hierarchical to	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Cryptographic algorithm name in Table 5-7] and specified cryptographic key sizes [Encryption key length in Table 5-7] that meet the following: [Standard of Table 5-7].

Table 5-7 A cryptographic algorithm that generates an encryption key used for encryption of TSF data, key length

	Standard	Cryptographic algorithm	Encryption key length	Purpose of use
#1	TTAK.KO-12.0190	Hash_DRBG	256	Key used to encrypt TSF data
#2	KS X ISO/IEC 18033-2	RSAES	2048	Session key encryption
#3	PKCS#5	PBKDF2	256	Private key encryption
#4	KS X ISO/IEC 9797-2	HMAC_SHA	256	KMS system log integrity verification

FCS_CKM.2(1) Cryptographic key distribution (User data encryption)

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_CKM.2.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [Table 5-8 Cryptographic key distribution method (User data encryption)] that meets the following: [None].

Table 5-8 Cryptographic key distribution method (User data encryption) – Between KMS and SA

Object	Distribution to	Distribution method
Between KMS and SA	Key used for user data encryption in FCS_CKM.1(1)	Communication encryption using mutual authentication using verified encryption module CIS-CC v3.3

FCS_CKM.2(2) Cryptographic key distribution (Mutual authentication and cryptographic communication function between TOE components)

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_CKM.2.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [Table 5-9 Cryptographic key distribution sequence (Mutual authentication and cryptographic communication function between TOE components)] that meets the following: [None].

Table 5-9 Cryptographic key distribution (Mutual authentication and cryptographic communication function between TOE components) – between SA/KMS Console and KMS

Object	Distribution to	Distribution method
Between SA/KMS Console and KMS	Session key	Communication encryption using mutual authentication using verified encryption module CIS-CC v3.3

FCS_CKM.4 Cryptographic key destruction

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.4.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [Overwrite all plaintext encryption keys and security-critical parameters in the device related to encryption keys with '0x00, 0x55, 0xAA' (DEK of SA, KMS), '0x00' (other than KMS)] that meets the following: [None].

FCS_COP.1(1) Cryptographic operation (User data encryption)

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 [Table 5-10 Cryptographic operation list] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in Table 5-10] and cryptographic key sizes [Encryption key length in Table 5-10] that meet the following: [Standard of Table 5-10].

Table 5-10 Cryptographic operation list of encryption keys used for user data encryption

	Standard	cryptographic algorithm	encryption key length	Cryptographic operation 목록
#1	KS X 1213-1, KS X 1213-2	ARIA	128, 256	User data encryption/decryption operation
#2	TTAS.KO-12.0004/R1, TTAS.KO-12.0025	SEED	128	User data encryption/decryption operation
#3	KS X ISO/IEC 9797-2	HMAC_SHA	256, 384, 512	User data encryption operation
#4	KS X ISO/IEC 10118-3	SHA 256/384/512	-	User data encryption operation

FCS_COP.1(2) Cryptographic operation (TSF data encryption)

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 [Table 5-11 Cryptographic operation list] in accordance with a specified cryptographic algorithm [Cryptographic algorithm in Table 5-11] and cryptographic key sizes [Encryption key length in Table 5-11] that meet the following: [Standard of Table 5-11].

Table 5-11 Cryptographic operation list of cryptographic keys used for TSF data encryption

	Standard	cryptographic algorithm	encryption key length	Cryptographic operation 목록
#1	KS X 1213-1, KS X 1213-2	ARIA	256	1) TSF data from KMS 2) Used when encrypting packets with session key
#2	KS X ISO/IEC 18033-2	RSAES	2048	1) Used for mutual authentication between SA (BA, DA) and KMS 2) Used for mutual authentication

				between KMS Console and KMS
#3	ISO/IEC 14888-2,RFC 3447	RSA-PSS	2048	1) Digital signature for cryptographic key distribution 2) Integrity check target list digital signature
#4	KS X ISO/IEC 10118-3	SHA256	-	First generation of hash value to be used for integrity check
#5	KS X ISO/IEC 9797-2	HMAC_SHA	256	KMS system log integrity verification

FCS_RBG.1 Random bit generation (Extended)

Hierarchical to	No other components.
Dependencies	No dependencies

FCS_RBG.1.1 The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [Standard of Table 5-12].

Table 5-12 List of random bit generation

Standard	cryptographic algorithm
ISO/IEC 18031-3 (2005)	Hash_DRBG

5.1.3User data protection (FDP)

FDP_UDE.1 User data encryption (Extended)

Hierarchical to	No other components.
Dependencies	FCS_COP.1 cryptographic operation

FDP_UDE.1.1 The TSF shall provide a function that can encrypt/decrypt the user data to the TOE user according to the specified [encryption/decryption method by column, [none]].

FDP_RIP.1 Subset residual information protection

Hierarchical to	No other components.
Dependencies	No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to, deallocation of the resource from* the following objects: [user data].

5.1.4Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to	No other components.
Dependencies	FIA_UAU.1 authentication

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [administrator authentication attempts]..

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [response action (Account Lockout) that does not process the Identification and authentication request for 10 minutes].

FIA_IMA.1(1) TOE Internal mutual authentication (SA – KMS communication section mutual authentication)

Hierarchical to	No other components.
Dependencies	No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication using [self-implemented authentication protocol] in accordance with [None] between [SA and KMS].

FIA_IMA.1(2) TOE Internal mutual authentication (KMS – KMS Console communication section mutual authentication)

Hierarchical to	No other components.
Dependencies	No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication using [self-implemented authentication protocol] in accordance with [None] between [KMS and KMS Console].

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 secret meet [Table 5-13 Password per TOE].

Table 5-13 Password Combination Rules for Each TOE

	TOE	Description
#1	KMS	a) Allowable characters - Capital letters of the alphabet (A ~ Z, 26 types) - Lowercase letters of the alphabet (a ~ z, 26 types) - Numbers (0 ~ 9, 10 types) - Special characters: *~!@#$% ()-=+;|₩.,/? Available b) Combination rules - At least one uppercase letter, lowercase letter, number, and special character must be included. - The same character cannot be used more than 3 times in a row - Alphabet and numbers cannot be used in ascending or descending order more than 3 times in a row c) Minimum length: 9 characters (9 bytes) d) Maximum length: 15 characters (15 bytes)
#2	KMS Console	a) Allowable characters - Capital letters of the alphabet (A ~ Z, 26 types) - Lowercase letters of the alphabet (a ~ z, 26 types) - Numbers (0 ~ 9, 10 types) - Special characters: >& | ; Only special characters other than b) Combination rules - At least one uppercase letter, lowercase letter, number, and special character must be included.

		– The same character cannot be used more than 3 times in a row – Alphabet and numbers cannot be used in ascending or descending order more than 3 times in a row c) Minimum length: 9 characters (9 bytes) d) Maximum length: 15 characters (15 bytes)

FIA_UAU.1(1) Timing of authentication (KMS Security Manager)

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

FIA_UAU.1.1 The TSF shall allow [the following list] on behalf of the **KMS Security Manager** to be performed before the **KMS Security Manager** is authenticated.
a) Enter IP of KMS to connect]

FIA_UAU.1.2 The TSF shall require each **KMS Security Manager** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **KMS Security Manager**.

FIA_UAU.1(2) Timing of authentication (KMS Assistant Security Manager)

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

FIA_UAU.1.1 The TSF shall allow [the following list] on behalf of the **KMS Assistant Security Manager** to be performed before the **KMS Assistant Security Manager** is authenticated.
a) Enter IP of KMS to connect

FIA_UAU.1.2 The TSF shall require each **KMS Assistant Security Manager** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **KMS Assistant Security Manager**.

FIA_UAU.2 User authentication before any action (KMS local security manager)

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

FIA_UAU.2.1 The TSF shall require each **KMS local security manager** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **KMS local security manager**

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to	No other components.
Dependencies	No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the following list].
a) The authentication mechanism used to authenticate the KMS security manager and auxiliary security manager
b) The authentication mechanism used to authenticate the local security manager of KMS

FIA_UAU.7 Protected authentication feedback

Hierarchical to	No other components.
Dependencies	FIA_UAU.1 authentication

FIA_UAU.7.1 The TSF shall provide only [the following feedback list] to the user while the authentication is in progress.
a) When entering secret information (password), the input character is changed to a fake character (eg, '•' character) and output
b) 'authentication failure message' without details on the reason for failure (ID and/or password errors must not be distinguished)

FIA_UID.1(1) Timing of identification (KMS Security Manager)

Hierarchical to	No other components.
Dependencies	No dependencies

FIA_UID.1.1 The TSF shall allow [the following list of defined actions] on behalf of the **KMS Security Manager** to be performed before the **KMS Security Manager** is identified.
a) Enter IP of KMS to connect

FIA_UID.1.2 The TSF shall successfully identify each **KMS Security Manager** before allowing any other TSF-mediated actions on behalf of the **KMS Security Manager** other than those specified in FIA_UID.1.1.

FIA_UID.1(2) Timing of identification (KMS Assistant Security Manager)

Hierarchical to	No other components.
Dependencies	No dependencies

FIA_UID.1.1 The TSF shall allow [the following list of defined actions] on behalf of the **KMS Assistant Security Manager** to be performed before the **KMS Assistant Security Manager** is identified.
a) Enter IP of KMS to connect

FIA_UID.1.2 The TSF shall successfully identify each **KMS Assistant Security Manager** before allowing any other TSF-mediated actions on behalf of the **KMS Assistant Security Manager** other than those specified in FIA_UID.1.1.

FIA_UID.2 User identification before every action (KMS local security manager)

Hierarchical to	FIA_UID.1 Timing of identification
Dependencies	No dependencies

FIA_UID.2.1 The TSF shall require each **KMS local security manager** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **KMS local security manager**.

5.1.5Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of management functions

	FMT_SMR.1	Security roles

FMT_MOF.1.1 The TSF shall restrict the ability *to conduct management actions of* the functions [List of security functions below] to [KMS Security Manager].
a) Initiation of the response *action to be taken* when the capacity of the log storage reaches the set threshold
b) Start and stop response *actions to be taken* in case of authentication failure]

FMT_MTD.1(1) Management of TSF data (KMS Security Manager)

Hierarchical to	No other components.	
Dependencies	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [the following list of TSF data] to [KMS Security Manager].
a) *Change* KMS Security Manager password
b) *Query and change* KMS audit trail storage capacity threshold notification settings
c) KMS log *query*
d) *Query and change* KMS Console access allowed IP settings
e) *Query* the maximum allowable value of KMS Security Manager inactivity period
f) *Change, query, and delete* encryption policies and services

FMT_MTD.1(2) Management of TSF data (KMS Assistant Security Manager)

Hierarchical to	No other components.	
Dependencies	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [the following list of TSF data] to [KMS Assistant Security Manager].
a) KMS audit trail *Query* for storage capacity threshold notification setting
b) *Query* for KMS log
c) KMS Console access allowed IP setting *query*
d) *Query* the maximum allowable value of KMS Security Manager inactivity period
e) Encryption policy and service *query*

FMT_MTD.1(3) Management of TSF data (KMS local security manager)

Hierarchical to	No other components.	
Dependencies	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [the following list of TSF data] to [KMS local security manager].
a) Query and delete KMS Console access allowed IP settings
b) Change KMS local security manager password

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to	No other components.	
Dependencies	FMT_SMF.1	Specification of management functions

FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [None] to [None].
1. [none]
2. [none]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [None] to [None].
1. [none]
2. [none]

FMT_PWD.1.3 The TSF shall provide the capability *setting password when installing*.

FMT_SMF.1 Specification of management functions

Hierarchical to	No other components.
Dependencies	No dependencies

FMT_SMF.1.1 The TSF shall be capable to performing the following management functions: [
a) Management list of security functions specified in FMT_MOF.1
b) List of Management of TSF data specified in FMT_MTD.1]

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 [Security roles of authorized administrator for each TOE in Table 5-14].

Table 5-14 Security roles of authorized administrators for each TOE

No.	TOE	Security roles	Description
#1	KMS	KMS local security manager	As an administrator with the right to change the internal settings of the product through CLI, he has the right to create KMS Security Manager. It is the only top-level administrator created after installation and cannot be added or deleted.
#2	KMS Console	KMS Security Manager	'KMS local security manager' is an administrator added through CLI command. 'KMS Security Manager' can use all functions of the Console.
#3		KMS Assistant Security Manager	'KMS Security Manager' is an administrator added through the Console. The KMS Assistant Security Manager has the right to inquire

			encryption keys and logs. Operations other than inquiry through the Console are restricted.

FMT_SMR.1.2 The TSF shall be able to associate users and their roles **defined in FMT_SMR.1.1**.

5.1.6Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to	No other components.
Dependencies	No dependencies

FPT_ITT.1.1 The TSF shall protect the TSF data from *disclosure, modification* by **verifying encryption and message integrity** when the TSF data is transmitted among TOE's separated parts.

FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to	No other components.
Dependencies	No dependencies

FPT_PST.1.1 The TSF shall protect [the following list of TSF data] stored in the containers controlled by the TSF from the unauthorized *disclosure, modification*.
a) KMS> data encryption key (encryption key to be used for user data encryption)
b) KMS> DB account access information

FPT_TST.1 TSF testing

Hierarchical to	No other components.
Dependencies	No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *[the following list of TSF]*
a) SA executable
b) KMS executable
c) KMS console executable
d) process

FPT_TST.1.2 The TSF shall provide **authorized administrator** with the capability to verify the integrity of [*the following list of TSF data*].
a) SA's service log
b) KMS service log, system log, administrator log
c) KMS> DB account access information)

FPT_TST.1.3 The TSF shall provide **authorized administrator** with the capability to verify the integrity of [*the following list of TSFs*].
a) SA library
b) CIS-CC v3.3 library
c) KMS executable file
d) KMS Console executable file

[Caution] The authorized administrator specified in this SFR means the security administrator specified in FMT_SMR.1.1.

5.1.7TOE Access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to	FTA_MCS.1	Basic limitation on multiple concurrent sessions
Dependencies	FIA_UID.1	Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions [belonging to the same **administrator** according to the rules for the list of management functions defined in FMT_SMF1.1]
a) limit the maximum number of concurrent sessions to 1 for management access by the same administrator who has the right to perform FMT_MOF.1.1 "Management actions" and FMT_MTD.1.1 "Management."
b) limit the maximum number of concurrent sessions to { number of sessions by TOE-specific query authorization managers in Table 5-15 } for management access by the same administrator who doesn't have the right to perform FMT_MOF.1.1 "Management actions" but has the right to perform a query in FMT_MTD.1.1 "Management" only

Table 5-15 Number of sessions by TOE-specific query authorization managers

	Object	Number of sessions of the query execution authority manager
#1	KMS Console	2
#2	KMS	1

c) [MAXIMUM NUMBER OF CONCURRENT SESSIONS PER TOE rule in Table 5-16]

Table 5-16 MAXIMUM NUMBER OF CONCURRENT SESSIONS PER TOE

	Object	MAXIMUM NUMBER OF CONCURRENT SESSIONS PER TOE
#1	KMS Console	KMS Security Manager: 1 KMS Assistant Security Manager: 2
#2	KMS	KMS local security manager: 1

FTA_MCS.2.2 The TSF should enforce the limit of [1] session per **administrator** by default.

FTA_SSL.5 Management of TSF-initiated sessions (Extended)

Hierarchical to	No other components.
Dependencies	FIA_UAU.1 authentication or none

FTA_SSL.5.1 The TSF shall *terminate* the administrator's interactive session after a [Inactivity time for each TOE in Table 5-17].

Table 5-17 Inactivity time for each TOE

	Object	Inactivity time
#1	KMS CLI	KMS Local Security Manager: The initial value is 5 minutes. Time cannot be adjusted
#2	KMS Console	KMS Security Manager: The initial value is 10 minutes. Time cannot be adjusted KMS Assistant Security Manager: 10 minutes. Time cannot be adjusted

FTA_TSE.1 TOE session establishment

Hierarchical to	No other components.
Dependencies	No dependencies

FTA_TSE.1.1 The TSF shall be able to refuse the management access session of the

administrator, based on [Access IP, *None*].

5.2 Security assurance requirements

5.2.1 Security Target evaluation

ASE_INT.1 introduction

Dependencies: No dependencies

Developer action element

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE
ASE_INT.1.2C The ST reference shall uniquely identify the ST.
ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.
ASE_INT.1.4C The TOE overview shall summaries the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.
ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action element

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action Elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies No dependencies.

Developer action element

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies No dependencies

Developer action element

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action Elements
ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies :ASE_ECD.1 Extended components definition

Developer action element

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.
ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.1.6C The description of security requirements should be internally consistent.

Evaluator action Elements
ASE_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies : ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action element

ASE_TSS.1.1D The developer shall provide a TOE summary specification

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements
ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with

the TOE overview and the TOE description.

5.2.2Development

ADV_FSP.1 Basic functional specification

Dependencies No dependencies

Developer action element

ADV_FSP.1.1D The developer shall provide a functional specification.
ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action element

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational

environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies No dependencies

Developer action element

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4Life-cycle support

ALC_CMC.1 TOE Lavelling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action element

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Content and presentation

ALC_CMC.1.1E The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies No dependencies

Developer action element

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for

content and presentation of evidence.

5.2.5Tests

ATE_FUN.1 Functional testing

Dependencies ATE_COV.1 Evidence of coverage
Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements
ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent testing – conformance

Dependencies ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action element
ATE_IND.1.1D The developer shall provide the TOE for testing

Content and presentation elements

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements
ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

5.2.6Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action element

AVA_VAN.1.1D The developer shall provide the TOE for testing

Content and presentation elements

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirements rationale

5.3.1 Dependency rationale of security functional requirements

User operation The following <Table 5-19> shows the dependencies of functional components.
FAU_GEN.1 has Dependencies on FPT_STM.1, but the TOE accurately records security-related events using the trusted timestamp provided by the TOE operating environment, so instead of FPT_STM.1, the security objective for the operating environment is OE. Trusted Dependencies of FAU_GEN.1 are satisfied by timestamp.
FAU_STG.3 and FAU_STG.4 have dependencies on FAU_STG.1, but only authorized administrators can access the place where the TOE is installed and operated. .3, Dependencies of FAU_STG.4 are satisfied.
In FCS_COP.1(1) and FCS_COP.1(2), the hash algorithm is an algorithm characteristic, and generation and destruction of encryption keys are not applied.
FIA_AFL.1, FIA_UAU.7, FTA_SSL.5 have Dependencies on FIA_UAU.1, but for KMS local security manager, FIA_UAU.2 successfully authenticates the manager before allowing any other TSF-mediated actions on behalf of the user. Therefore, the dependencies of FIA_AFL.1 , FIA_UAU.7 , and FTA_SSL.5 are satisfied.
FIA_UAU.2, FMT_SMR.1, FTA_MCS.2 have Dependencies on FIA_UID.1, but for the KMS local security manager, FIA_UID.2 identifies the user before all actions, so Dependencies are satisfied manual

Table 5-19 Rationale for the dependency of the security functional requirements

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE. Time stamp
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1(1)	FAU_GEN.1	2
5	FAU_SAR.1(2)	FAU_GEN.1	2
6	FAU_SAR.1(3)	FAU_GEN.1	2
7	FAU_SAR.3	FAU_SAR.1	4, 5, 6
8	FAU_STG.3	FAU_STG.1	OE. Audit trail protection
9	FAU_STG.4	FAU_STG.1	OE. Audit trail protection
10	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	12, 15
		FCS_CKM.4	14
11	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	13, 16
		FCS_CKM.4	14
12	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10
		FCS_CKM.4	14
13	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	11
		FCS_CKM.4	14

14	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10, 11
15	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10
		FCS_CKM.4	14
16	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	11
		FCS_CKM.4	14
17	FCS_RBG.1	–	–
18	FDP_UDE.1	FCS_COP.1	15
19	FDP_RIP.1	–	–
20	FIA_AFL.1	FIA_UAU.1	24, 25, 26
21	FIA_IMA.1(1)	–	–
22	FIA_IMA.1(2)	–	–
23	FIA_SOS.1	–	–
24	FIA_UAU.1(1)	FIA_UID.1	29
25	FIA_UAU.1(2)	FIA_UID.1	30
26	FIA_UAU.2	FIA_UID.1	31
27	FIA_UAU.4	–	–
28	FIA_UAU.7	FIA_UAU.1	24, 25, 26
29	FIA_UID.1(1)	–	–
30	FIA_UID.1(2)	–	–
31	FIA_UID.2	–	–
32	FMT_MOF.1	FMT_SMF.1	37
		FMT_SMR.1	38
33	FMT_MTD.1(1)	FMT_SMF.1	37
		FMT_SMR.1	38
34	FMT_MTD.1(2)	FMT_SMF.1	37
		FMT_SMR.1	38
35	FMT_MTD.1(3)	FMT_SMF.1	37
		FMT_SMR.1	38
36	FMT_PWD.1	FMT_SMF.1	37
		FMT_SMR.1	38
37	FMT_SMF.1	–	–
38	FMT_SMR.1	FIA_UID.1	29, 30, 31
39	FPT_ITT.1	–	–
40	FPT_PST.1	–	–
41	FPT_TST.1	–	–
42	FTA_MCS.2	FIA_UID.1	29, 30, 31
43	FTA_SSL.5	FIA_UAU.1	24, 25, 26

44	FTA_TSE.1	–	–

5.3.2 Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.
The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. But, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

6. TOE security function

6.1.1 Security Audit (TSS_AU)

TSS_AU.1 Audit data generation

Related SFR: FAU_GEN.1 Audit data generation

TSS_AU.1.1 The TOE creates audit data for the audit Table event list for follow-up when a potential security violation event occurs. At this time, the TOE includes the event date and time, event type, identity of the object that caused the event (if possible), work history and results (success/failure), etc. in the audit record. The list of audit Table events of the TOE is as follows. For more information on this, refer to <Table 6-1 Audit event> below. FAU_GEN.1

Table 6-1 Audit event

functional component	Audit event	Additional audit record
FAU_ARP.1	Actions taken due to potential security violations	-
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	-
FAU_STG.3	Actions taken due to exceeding of a threshold	-
FAU_STG.4	Actions taken due to the audit storage failure	-
FCS_CKM.1(1)	Success and failure of the activity	-
FCS_CKM.2	Success and failure of the activity (only applying to distribution of key related to user data encryption/decryption)	-
FCS_CKM.4	Success and failure of the activity (Only applying to destruction of key related to user data encryption/decryption)	-
FCS_COP.1(1)	Success and failure of cryptographic operations, types of cryptographic operations	-
FDP_UDE.1	Success and failure of user data encryption/decryption	-
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken, and the subsequent, if appropriate, restoration to the normal stat	-
FIA_IMA.1	Success and failure of mutual authentication Modify of authentication protocol	-
FIA_UAU.1	All use of the authentication mechanism	-
FIA_UAU.4	Attempts to reuse authentication data	-
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	-
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	-
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1	All changes of the password	-
FMT_SMF.1	Use of the management functions	-
FMT_SMR.1	Modifications to the user group of rules divided	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	access IP
FTA_SSL.5	Locking or termination of interactive session	-

FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	–

TSS_AU.1.2 For reference, the TOE obtains and uses the time information from the trusted OS of the TOE operating environment to generate accurate time information on the occurrence date and time information of major events when generating audit data.

TSS_AU.2 Response to security violations

Related SFR: FAU_ARP.1 Security alarms
FAU_SAA.1 Potential violation analysis

TSS_AU.2.1 TSF detects potential violations in 'potential security violation.' in <Table 6-2 Security alarms action list> below and performs 'response actions' for the violation. FAU_SAA.1, FAU_ARP.1

Table 6-2 Security alarms action list

Category	Security functional component	potential security violation.	response action
SA	FPT_TST.1	Failed self-test of verified cryptographic module	disable service
		Integrity verification failure of verified cryptographic module	- initial start-up: disable service - periodically during normal operation: Notified by e-mail designated by the authorized administrator
		Other integrity verification failures	- initial start-up: warning message output - periodically during normal operation: Notified by e-mail designated by the authorized administrator
KMS	FAU_STG.3	Events in which the audit trail exceeds a specified threshold	Notified by e-mail designated by the authorized administrator
	FAU_STG.4	Events with saturated audit trails	Notified by e-mail designated by the authorized administrator
	FPT_TST.1	Failed self-test of verified cryptographic module	disable service
		Integrity verification failure of verified cryptographic module	- initial start-up: Disable service - periodically during normal operation: Disable service and notified by e-mail designated by the authorized administrator
		Other integrity verification failures	Notified by e-mail designated by the authorized administrator
	FIA_UAU.2	KMS local security manager authentication failure audit event	Account lock after 5 authentication failures
KMS Cons	FPT_TST.1	Failed self-test of verified cryptographic module	disable service

ole		Integrity verification failure of verified cryptographic module	- initial start-up: disable service - periodically during normal operation: Disable service and warning message output
		Other integrity verification failures	warning message output
	FIA_UAU.1	KMS Security Manager, KMS Assistant Security Manager authentication failure audit event	Account lock after 5 authentication failures

TSS_AU.3 Audit review

Related SFR: FAU_SAR.1(1) Audit review (DCC Security Manager)
FAU_SAR.1(2) Audit review (KMS Security Manager)
FAU_SAR.1(3) Audit review (KMS Assistant Security Manager)
FAU_SAR.3 Selectable audit review

TSS_AU.3.1 The TOE provides the KMS local security manager with the ability to read KMS audit data that can be inquired using the KMS CLI. The TOE provides KMS security managers and KMS assistant security managers with the ability to read KMS audit data that can be viewed using KMS Console. FAU_SAR.1(1), FAU_SAR.1(2), FAU_SAR.1(3)

TSS_AU.3.2 When an authorized administrator reviews audit data, the KMS Console provides a function to selectively review audit data type, search criteria item, and logical relationship (AND) between search criteria items. For audit review criteria, selection/sequencing method, and sequencing criteria, refer to the specifications in FAU_SAR.3.1 of ST. FAU_SAR.3

TSS_AU.4 Audit trail loss response

Relevant SFR: FAU_STG.3 Actions to take when predicting loss of audit data
FAU_STG.4 Prevention of loss of audit data (SA, KMS, KMS Console)

TSS_AU.4.2 When KMS of TOE exceeds 90%, it notifies the authorized administrator by e-mail so that they can take action.FAU_STG.3

TSS_AU.4.3 In the TOE, KMS prevents loss of audit data by ignoring audited events when audit trails reach saturation.FAU_STG.4

Table 6-3 Capacity limits and response actions for audit trail inspection conditions

Object	Capacity limit	response action
KMS, KMS Console	90%	Send email notifications

Table 6-4 Actions to take when predicting audit loss

Object	Capacity limit	response action
KMS	100%	Send email notifications

6.1.2Cryptographic Support (TSS_CS)

TSS_CS.1 Cryptographic key management and Cryptographic operation

Related SFR:

FCS_CKM.1(1) Cryptographic key generation (User data encryption)

FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)

FCS_CKM.2(1) Cryptographic key distribution (User data encryption)
FCS_CKM.2(2) Cryptographic key distribution (Mutual authentication and cryptographic communication function between TOE components)
FCS_CKM.4 Cryptographic key destruction
FCS_COP.1(1) Cryptographic operation (User data encryption)
FCS_COP.1(2) Cryptographic operation (TSF data encryption)
FCS_RBG.1(Extended) Random bit generation

TSS_CS.1.1 The TOE generates a key for encryption of user data and a key for encryption of TSF data using the verified encryption module CIS-CC v3.3.

Table 6-5 Verified encryption module

구분	내용
Cryptographic module name	CIS-CC v3.3
Verification number	CM-145-2023.11
Developer	Penta Security Systems Inc.
verification date	2018-11-07

The cryptographic algorithm and encryption key length used for cryptographic key generation are shown in the table below.

Table 6-6 A cryptographic algorithm that generates an encryption key used for user data encryption, key length

	Standard	cryptographic algorithm	encryption key length	purpose of use
#1	TTAK.KO-12.0190	Hash_DRBG	128, 256, 384, 512	Key used for user data encryption

Table 6-7 A cryptographic algorithm that generates an encryption key used for encryption of TSF data, key length

	Standard	cryptographic algorithm	encryption key length	purpose of use
#1	TTAK.KO-12.0190	Hash_DRBG	256	Key used to encrypt TSF data
#2	KS X ISO/IEC 18033-2	RSAES	2048	session key encryption
#3	PKCS#5	PBKDF2	256	private key encryption
#4	KS X ISO/IEC 9797-2	HMAC_SHA	256	KMS system log integrity verification

In case of cryptographic key generation, it is generated using the following random number generator provided by the verified cryptographic module CIS-CC v3.3.

Table 6-8 List of random bit generation

Standard	cryptographic algorithm
ISO/IEC 18031-3 (2005)	Hash_DRBG

The table below describes the cryptographic algorithm, encryption key length, and purpose of use required for cryptographic operation of the TOE.FCS_CKM.1(1), FCS.CKM.1(2), FCS_RBG.1, FCS_COP.1(1) , FCS_COP.1(2)

Table 6-9 Cryptographic operation list of encryption keys used for user data encryption

	Standard	cryptographic algorithm	encryption key length	mode	purpose of use
#1	TTAK.KO-12.0190	Hash_DRBG	128, 256, 384, 512	CBC, CFB	Key used for user data encryption
#2	TTAS.KO-12.0004/R1, TTAS.KO-12.0025	SEED	128	CBC, CFB	Key used for user data encryption
#3	KS X ISO/IEC 9797-2	HMAC_SHA	256, 384, 512	-	Key used for user data encryption
#4	KS X ISO/IEC 10118-3	SHA 256/384/512	-	-	Key used for user data encryption

Table 6-10 Cryptographic operation list of cryptographic keys used for TSF data encryption

	Standard	Cryptographic algorithm	Encryption key length	Purpose of use
#1	KS X 1213-1, KS X 1213-2	ARIA	256	1) Used for encryption when storing symmetric key (DEK) in KMS 2) When sending data from SA (BA, DA) or KMS console to KMS, it is used to encrypt transmission data (PKD). 3) Used for encryption when storing DB access account information in KMS 4) Used for encryption when storing random numbers used as KEKs for DB access account information in KMS 5) When sending data from KMS to SA (BA, DA) or KMS Console, used for encryption of transmission data (PKD) 6) Used for encryption when loading the password (pin value) of the security manager private key in the KMS console into memory
#2	KS X ISO/IEC 18033-2	RSAES	2048	1) When sending data from SA (BA, DA) or KMS console to KMS, it is used for public key encryption of the session key. 2) Used for encryption when storing the random number generated at the time of generating the site key pair used as the KEK of the symmetric key in KMS in the DB 3) When sending data from KMS to SA (BA, DA) or KMS Console, it is used for public key encryption of the session key. 4) Used for private key encryption when storing the site/agent/security manager

				key pair in KMS
#3	ISO/IEC 14888-2,RFC 3447	RSA-PSS	2048	1) Digital signature when distributing encryption key 2) Integrity check target list digital signature
#4	KS X ISO/IEC 10118-3	SHA256	-	First generation of hash value to be used for integrity check
#5	KS X ISO/IEC 9797-2	HMAC_SHA	256	KMS system log integrity verification

TSS_CS.1.2 When encrypting user data, the TOE distributes the encryption key by the Distribution method specified in the table below. FCS_CKM.2(1)

Table 6-11 Cryptographic key distribution (User data encryption) – Between KMS and SA

Object	Seq.	Distribution method
Between KMS and SA	1	KMS generates session key using CIS-CC v3.3 random number generator.
	2	Encrypts the encryption key (DEK) for user data encryption with the session key generated in step 1 using symmetric key encryption
	3	The session key is encrypted using public key encryption with the agent public key issued to communicate with the SA.
	4	Digitally sign the encryption value generated in steps 2 and 3 with the KMS site private key
	5	The values 2, 3, and 4 are transmitted to the SA.
	6	Encrypt the data in the database with the encryption service received in step 5

TSS_CS.1.3 The TOE distributes the cryptographic key by the Distribution method specified in the table below during mutual authentication and cryptographic communication between TOE components. FCS_CKM.2(2)

Table 6-12 Cryptographic key distribution sequence (Mutual authentication and cryptographic communication function between TOE components) – between SA/KMS Console and KMS

Seq.	Distribution method
1	KMS> Delivers agent public key pair and KMS site public key to SA/KMS Console.
2	KMS> Digitally sign the TSF data encryption key (DEK) to be transmitted with the KMS site private key.
3	KMS> Session key is generated using the random number generator of CIS-CC v3.3.
4	KMS> Encrypt the data encryption key (DEK) to be transmitted and the signature value of No. 2 using the symmetric key encryption with the session key created in Step 3.
5	The session key is encrypted using public key encryption with the agent public key

	issued to communicate with KMS> SA/KMS Console.
6	KMS> Transmits No. 4, No. 5 to SA/KMS Console.
7	SA/KMS console > Decrypt the data received in step 6 with the agent private key to obtain the session key
8	SA/KMS Console > Decrypt the contents of No. 4 received in No. 6 with the session key obtained in Step 7.
9	SA/KMS Console > Verify the signature value obtained in step 8 using the KMS site public key
10	KMS and SA/KMS console Session key is always generated as in No. 2, and mutual authentication is always performed.

TSS_CS.1.4 In the TOE, KMS destroys the encryption key by changing all plaintext encryption keys and security parameters in the device related to the encryption key to '0x00, 0x55, 0xAA', and SA in the TOE to '0x00'. In addition, the DEK loaded into the memory of the TOE operating environment DBMS is managed as a DBMS global variable and is automatically destroyed when the session ends.FCS_CKM.4

As shown in the TOE <Table 6-13 Cryptographic key destruction list>, the encryption key is destroyed by the destruction method corresponding to the specified destruction time for each encryption key. FCS_CKM.4

Table 6-13 Cryptographic key destruction list

TOE	Cryptographic key	Time of destruction	Method of destruction
SA	key for user data encryption	Immediately after encryption/decryption	0x00 overwrite
	Session Key	Immediately after mutual authentication	Overwrite 0xAA, 0x55, 0x00
	Key for TSF Data Encryption	Immediately after mutual authentication	0x00 overwrite
	KEK of key for encryption of TSF data	Immediately after mutual authentication	0x00 overwrite
	agent private key	Immediately after mutual authentication	0x00 overwrite
KMS	site private key	Immediately after mutual authentication	Overwrite 0xAA, 0x55, 0x00
	security manager private key	Immediately after mutual authentication	Overwrite 0xAA, 0x55, 0x00
	Session Key	Immediately after mutual authentication	Overwrite 0xAA, 0x55, 0x00
	key for user data encryption	Immediately after encryption/decryption	Overwrite 0xAA, 0x55, 0x00
	KEK of key for user data encryption	Immediately after encryption/decryption	Overwrite 0xAA, 0x55,

			0x00
	Key for TSF Data Encryption	Immediately after encryption/decryption	0x00 overwrite
	KEK of key for encryption of TSF data	Immediately after encryption/decryption	0x00 overwrite
	Key for Log Integrity Verification	Immediately after creating the log integrity value	0x00 overwrite
KMS Console	Security manager private key	Immediately after mutual authentication	0x00 overwrite
	Session key	Immediately after mutual authentication	Overwrite 0xAA, 0x55, 0x00
	Key for TSF Data Encryption	Immediately after mutual authentication	0x00 overwrite
	KEK of key for encryption of TSF data	Immediately after mutual authentication	0x00 overwrite

6.1.3User data protection (TSS_DP)

TSS_DP.1 **User data protection**

Related SFR: FDP_UDE.1 User data encryption

FDP_RIP.1 Subset residual information protection

TSS_DP.1.1 The TOE provides encryption and decryption functions for the plaintext input by the user, and the same ciphertext is not generated for the same plaintext during user data encryption. FDP_UDE.1

TSS_DP.1.2 When the TOE encrypts the plaintext entered by the user, the remaining data is not left behind and the information is no longer available. FDP_RIP.1

6.1.4Identification and authentication (TSS_IA)

The TOE provides the following functions to safely identify and authenticate the security manager.

TSS_IA.1 **Identification and authentication**

Related SFR: FIA_UID.1 Timing of identification

FIA_UAU.1 authentication

FIA_AFL.1 Authentication failure handling

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.7 Protected authentication feedback

TSS_IA.1.1 The TOE locks the account when the number of authentication failure attempts reaches or exceeds the maximum allowed number of failures (eg, 5). Locked accounts will be rejected for a specified period of time (eg 10 minutes) for identification and authentication requests.FIA_AFL.1

TSS_IA.1.2 The TOE performs mutual authentication for each separated TOE component. The order of mutual authentication between each TOE is shown in Figures [6-1] and [6-2] below, and security protocol v3.0 is used.
A) The mechanism of the request protocol is as follows.
The SA or KMS console signs the requested data with the agent private key or the

security manager private key. The session key is encrypted with the KMS site public key. The request message and signature value are encrypted with the session key and delivered to the KMS. KMS decrypts the encrypted session key with the KMS site private key to obtain the session key, decrypts the encrypted request message with the session key to obtain the request message, and verifies the signature value with the agent public key or the security manager public key.

B) The mechanism of response protocol is as follows.

The response message is signed using the KMS private key. The session key is encrypted with the D'Amo public key or the security manager public key. The response message and signature value are encrypted with the session key and delivered to the SA or KMS Console. The SA or KMS Console decrypts the encrypted session key with the agent private key or the security manager private key to obtain the session key, decrypts the encrypted response message with the session key to obtain the response message, and verifies the signature value with the KMS site public key. FIA_IMA.1(1), FIA_IMA.1(2)

Figure 6-1 Mutual authentication and request protocol between TOE components

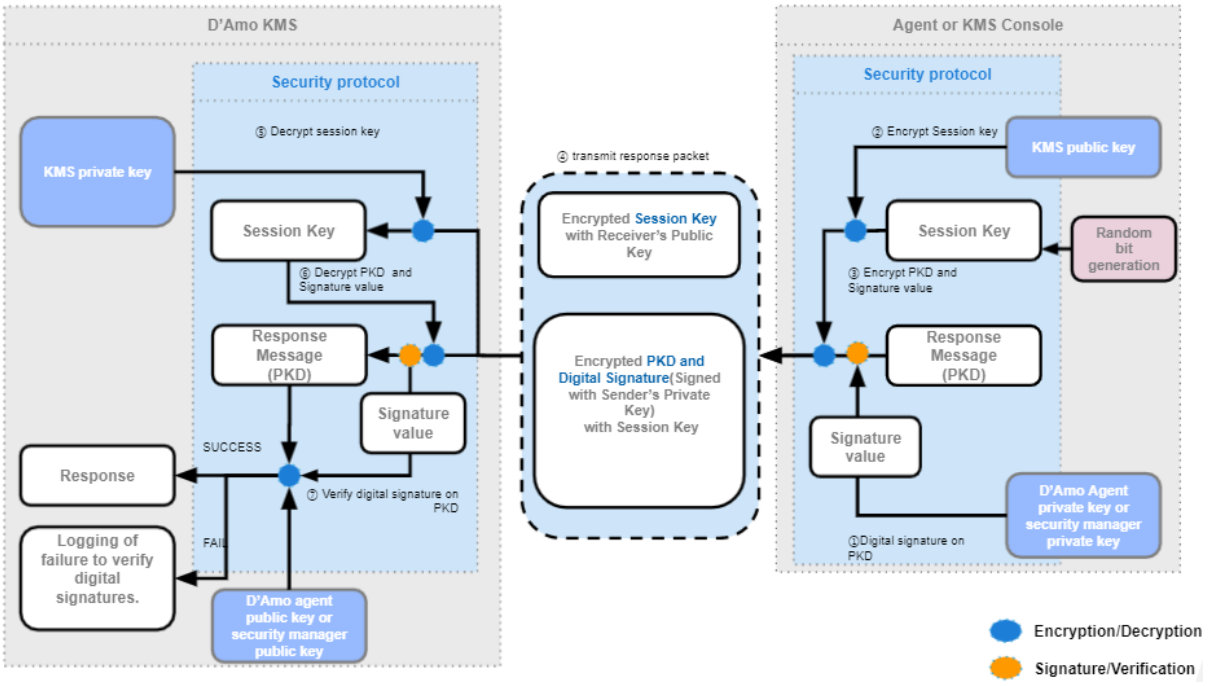
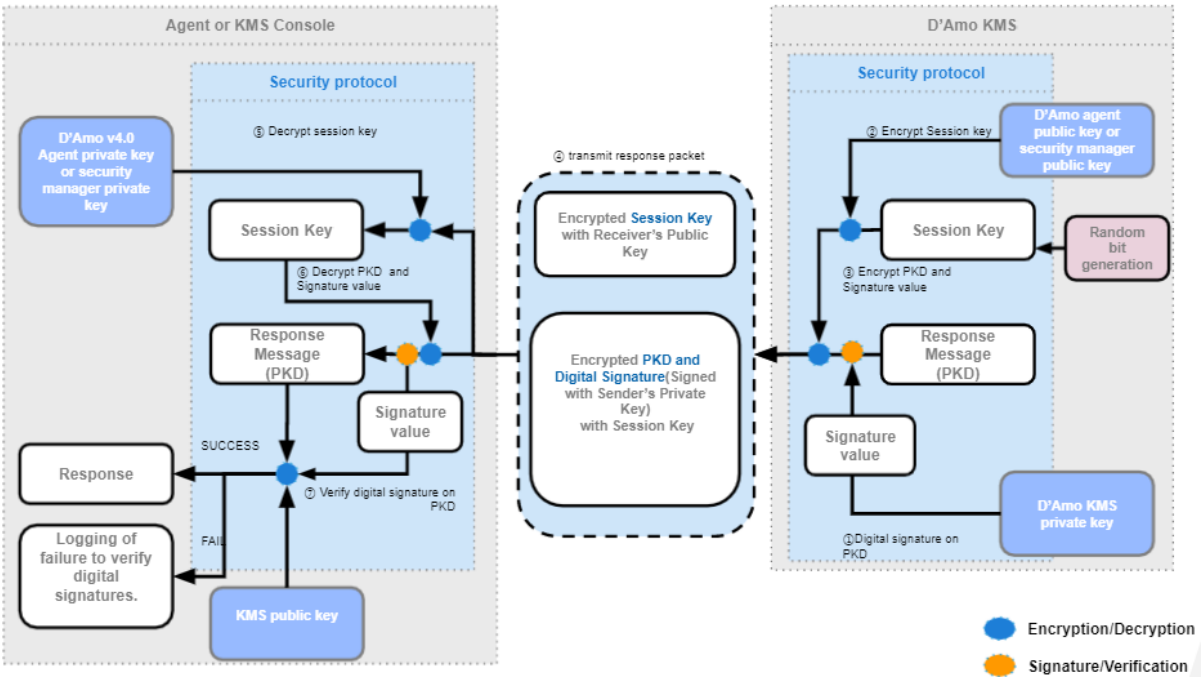


Figure 6-2 Mutual authentication and response protocol between TOE components



TSS_IA.1.3 One default account is provided for KMS local security manager, and additional creation is not possible. It provides identification and authentication functions along with passwords.FIA_UAU.2, FIA_UID.2

TSS_IA.1.4 When the KMS security manager authenticates in the KMS Console, the KMS Console provides a certification-based identification and authentication function, and the KMS console provides the security management function only when identification and authentication are successfully completed.FIA_UAU.1(1), FIA_UID.1(1)

TSS_IA.1.5 When the KMS assistant security manager authenticates in the KMS Console, the KMS Console provides a certification-based identification and authentication function, and the KMS console provides the inquiry function only when identification and authentication are successfully completed.FIA_UAU.1(2), FIA_UID.1(2)

TSS_IA.1.6 When secret information is input while identification and authentication is in progress, KMS CLI and KMS Console changes the character to a fake character. (eg, '*' character) and outputs it. The TOE does not provide detailed information on the reason for failure if authentication fails.(eg, login failed). FIA_UAU.7

TSS_IA.1.7 The KMS Console uses time stamp to prevent reuse of authentication data used for administrator authentication.FIA_UAU.4

TSS_IA.2 Define User (Administrator) Attributes

Related SFR: FIA_SOS.1 Verification of secrets

FMT_PWD.1(Extended) Management of ID and password

TSS_IA.2.1 When registering a password (password), the TOE verifies that the acceptance criteria in <Table 5-14 Password for each TOE> are satisfied. If the password requested for registration does not meet the acceptance criteria, the administrator is forced to re-enter the password.FIA_SOS.1, FMT_PWD.1(Extended)
The password combination rules are shown in the table below.

Table 6-14 Password Combination Rules for Each TOE

	TOE	Description
#1	KMS	a) Allowable characters

		– Capital letters of the alphabet (A ~ Z, 26 types) – Lowercase letters of the alphabet (a ~ z, 26 types) – Numbers (0 ~ 9, 10 types) – Special characters: *~!@#$% ()–=+;|₩.,/? Available b) Combination rules – At least one uppercase letter, lowercase letter, number, and special character must be included. – The same character cannot be used more than 3 times in a row – Alphabet and numbers cannot be used in ascending or descending order more than 3 times in a row c) Minimum length: 9 characters (9 bytes) d) Maximum length: 15 characters (15 bytes)
#2	KMS Console	a) Allowable characters – Capital letters of the alphabet (A ~ Z, 26 types) – Lowercase letters of the alphabet (a ~ z, 26 types) – Numbers (0 ~ 9, 10 types) – Special characters: >&	; Only special characters other than b) Combination rules – At least one uppercase letter, lowercase letter, number, and special character must be included. – The same character cannot be used more than 3 times in a row – Alphabet and numbers cannot be used in ascending or descending order more than 3 times in a row c) Minimum length: 9 characters (9 bytes) d) Maximum length: 15 characters (15 bytes)

TSS_IA.2.2 The TOE forces the authorized user to enter the initial password when first connecting to KMS and to change the password when logging in for the first time.

6.1.5Security Management (TSS_MT)

The TOE provides functions that allow the authorized administrator to set and manage security functions, security policies, and important data.

TSS_MT.1 Management of security functions behaviour

Related SFR FMT_MOF.1 Management of security functions behaviour

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_PWD.1 Management of ID and password

TSS_MT.1.1 The TOE provides functions that allow the authorized administrator to manage security functions such as response actions when a security violation event occurs. The security function management list and capabilities provided to the authorized administrator are as follows. The password set at the time of initial installation must be changed. FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FMT_PWD.1

- **KMS Security Manager**

- ✔ Initiate actions for response actions to be taken when the capacity of the log storage reaches the threshold
- ✔ Start and stop response actions to be taken in case of authentication failure

- **KMS Assistant Security Manager**
  - ✔ None
- **KMS local security manager**
  - ✔ None

TSS_MT.2 Management of TSF data

Related SFR: FMT_MTD.1 Management of TSF data

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

TSS_MT.2.1 In the TOE, an authorized administrator can perform the following management functions for the TSF data through the Console. FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1

- KMS Security Manager
  - ✔ Changes to the KMS Security Manager password
  - ✔ KMS audit trail Query and change storage capacity threshold notification settings
  - ✔ Query for KMS logs
  - ✔ Query and change KMS Console access allowed IP settings
  - ✔ KMS Security Manager Query the maximum allowable period of inactivity
  - ✔ Change, query, and delete encryption policies and services
- KMS Assistant Security Manager
  - ✔ KMS audit trail Query for storage capacity threshold notification setting
  - ✔ Query for KMS logs
  - ✔ KMS Console access allowed IP setting query
  - ✔ KMS Security Manager Query the maximum allowable period of inactivity
  - ✔ Encryption policy and service query
- KMS local security manager
  - ✔ Query and delete KMS Console access allowed IP settings
  - ✔ Change KMS local security manager password

6.1.6TSF protection (TSS_PT)

TSS_PT.1 Integrity Verification

Related SFR FPT_TST.1 TSF testing

TSS_PT.1.1 The TOE provides the integrity verification function to ensure the integrity of the mechanism constituting the security function and the safety of the security management. The TOE performs periodic integrity checks during initial start-up and operation to ensure the correct operation of the TOE. Integrity verification targets are main executable files and security policy/environment configuration files. FPT_TST.1

- SA library (cycle: 1 hours)
- KMS (cycle: 1 hour)
- KMS Console executable file (cycle: 5 minutes)

- SA's service log
- KMS service log, system log, administrator log
- KMS> DB account access information

TSS_PT.2 Self test

Related SFR: FPT_TST.1 TSF testing

TSS_PT.2.1 To ensure its own correct operation, the TOE periodically conducts self-tests on major processes during initial start-up and operation, and performs self-tests of verified cryptographic modules. FPT_TST.1

- SA encryption/decryption process (cycle: 1 hour)
- KMS key generation process (cycle: 5 minutes)
- KMS connection process of KMS Console (cycle: 5 minutes)

TSS_PT.3 Stored TSF data protection

Related SFR: FPT_PST.1(Extended) Basic protection of stored TSF data

TSS_PT.3.1 The TOE protects important TSF data from unauthorized exposure and modification by encrypting it with the verified cryptographic module CIS-CC v3.3 and storing it. FPT_PST.1

- Critical TSF data
  - ✔ SA> session key used for mutual authentication
  - ✔ KMS> Symmetric key used for user data encryption
  - ✔ KMS> DB account access information
  - ✔ KMS> session key used for mutual authentication
  - ✔ KMS> Site, Agent, Security Manager key pair
  - ✔ KMS> Local security manager password
  - ✔ KMS Console> session key used for mutual authentication
- Algorithm used to encrypt the administrator password
  - ✔ KMS local security manager password: SHA256-based hash value storage
  - ✔ Security Manager Key Pair: RSA 2048 OAEP
- Encryption algorithm when saving TOE settings
  - ✔ KMS> DB account access information: ARIA256
- KEK protection measures
  - ✔ The KEK of user data is encrypted with the site public key so that only the KMS that owns the site private key can decrypt it.
  - ✔ KMS> The KEK of DB account access information is self-encoded with a random number generated by a random number generator and loaded into memory for use.
- Encryption algorithm of encryption key and key security parameters loaded into memory
  - ✔ Random number used as KEK of symmetric key: ARIA256
  - ✔ Password (pin value) of the site private key used as the KEK of the site private key: RSA 2048 OAEP
  - ✔ Password of site private key used as KEK of agent private key (pin value): RSA 2048 OAEP
  - ✔ Password (pin value) of the site private key used as the KEK of the security manager private key: RSA 2048 OAEP

Table 6-15 TSF data list

TOE	TSF data or user data	Algorithm used when encry	DEK	Algorithm used for encry	KEK	Algorithm used for encryption with the key to	key to encrypt the KEK

			pting with DEK		ption with KEK		encrypt the KEK	
BA	User data encryption	plain text	(depending on user created values)	Symmetric key (key received from KMS) – Time of destruction: immediately after use – Zeroing method: 0x00	ARIA 256	Randomly generated value (KEK) at the time of site key pair generation – Storage location: KMS DB > VALUE column, KMS_SPECIAL_KEY table, condition ID = 'KEK', key_TYPE=107 ; – Destruction time: It is encrypted and loaded into memory and destroyed when the KMS daemon ends. – Zeroing method: 0xAA, 0x55, 0x00	–	–
	TSF data encryption	transmission data (PKD)	ARIA 256	session key – Memory destruction time: Immediately after data transfer – Zeroing method: Overwrite 0xAA, 0x55, 0x00	RSA 2048 OAEP	1) When requesting from SA→KMS, session key encryption: Site public key – Timing of destruction: destroy immediately after use – Zeroing method: 0xAA, 0x55, 0x00 overwrite	–	–
DA	User data encryption	Plain text	(Depends on the value created by the user)	Symmetric key (key received from KMS) – Time of destruction: immedia	ARIA 256	Random number generated value (KEK) at the time of site key pair generation – Storage location: KMS DB > VALUE column, KMS_SPECIAL_KEY table,	–	–

				tely after use – Zeroing method: 0x00		condition ID = 'KEK', key_TYPE=107 ; – Destruction time: It is encrypted and loaded into memory and destroyed when the KMS daemon ends. – Zeroing method: 0xAA, 0x55, 0x00		
	TSF data encryption	transmission data (PKD)	ARIA 256	session key – Memory destruction time: Immediately after data transfer – Zeroing method: Overwrite 0xAA, 0x55, 0x00	RSA 2048 OAEP	1) When requesting from SA→KMS, session key encryption: Site public key – Timing of destruction: destroy immediately after use – Zeroing method: 0xAA, 0x55, 0x00 overwrite	–	–
KMS	User data encryption	Plain text	(Depending on the value created by the user)	Symmetric key (data encryption key, DEK) – Storage location: KMS DB > KMS_SECRET_KEY table > VALUE column – Memory destruction time: immediately after use – Zeroing	ARIA 256	Random number generated value (KEK) at the time of site key pair generation – Storage location: KMS DB > VALUE column, KMS_SPECIAL_KEY table, condition ID = 'KEK', key_TYPE=107 ; – Destruction time: It is encrypted and loaded into memory and destroyed when the KMS daemon ends. – Zero Method: 0xAA, 0x55, 0x00 Overwrite	RSA 2048 OAEP	Site Key Pair – Destruction time: public key when KMS module is closed/private key immediately after decryption

				method: 0x00				
	TSF data encryption	transmission data (PKD)	ARIA 256	session key – Memory destruction time: Immediately after data transfer – Zeroing method: Overwrite 0xAA, 0x55, 0x00	RSA 2048 OAEP	1) When responding to KMS→SA, session key encryption: Agent public key 2) When responding to KMS→KMS Console, session key encryption: Security manager public key – Destruction time: Immediately after mutual authentication – Zeroing method: 0x00 overwrite	–	–
		DB access account information – Saved in: /opt/penta/km/conf/kmsdb.conf	ARIA 256	random number – Destruction time: When the log receiver daemon is terminated	ARIA 256	The value derived from the password entered by the user when starting from the CLI – Time of destruction: immediately after use – Zeroing method: 0x00 overwrite	–	–
		site key pair – Storage location: KMS_SPECIAL_KEY table, condition TYPE in (1, 2) TYPE=1: Site public key TYPE=2: Site private key – Private key is PKCS#8	RSA 2048 OAEP	Password of the site's private key (pin value)	–	–	–	–

		format and password –based encryption (seedCBC WithSHA256) by PKCS#5 – Destruction time: public key when KMS module is closed/private key immediately after decryption – Zeroing method: public key is not zeroed / private key is overwritten by 0x00						
		Agent key pair – Storage location: KMS_AGENT_CRYPTOKI_KEY table – Private key is PKCS#8 format and password –based encryption by PKCS#5 method (seedCBC WithSHA256)	RSA 2048 OAEP	Agent private key password (pin value)	–	–	–	–
		security manager key pair – Storage location:	RSA 2048 OAEP	Password of security manager private	–	–	–	–

		KMS_CONSOLE_MANAGER_KEY table – Private key is PKCS#8 format and password –based encryption (seedCBCWithSHA256) by PKCS#5		key (pin value)				
KMS Console	TSF data encryption	Transmission data (PKD)	ARIA 256	session key – Destruction time: Immediately after data transmission – Zeroing method: 0xAA, 0x55, 0x00 overwrite	RSA 2048 OAEP	1) KMS Console→ When requesting KMS, session key encryption: Site public key – Destruction time: Immediately after decrypting key pair location information in the registry, immediately after signing KMS transmission data – Zeroing method: 0x00 overwrite	–	–
		security manager key pair – Storage location: PC with Consoles installed (customized) – Private key is PKCS#8 format and password –based encryption (seedCBCWithSHA2	RSA 2048 OAEP	Security manager private key password (pin value) ARIA256	ARIA 256	Password of security manager private key (pin value) – Memory destruction time: Release memory immediately after signing KMS transmission data	–	–

		56) by PKCS#5						

TSS_PT.4 **Protection of transmitted data**

Related SFR: FPT_ITT.1 Basic internal TSF data transfer protection

TSS_PT.4.1 The TOE encrypts the data transmitted by the KMS after the authorized administrator requests the KMS through the KMS Console or SA with a session key created using the random number generated by the random number generator of CIS-CC v3.3, the verified cryptographic module, and changes it. or to protect from exposure. FTP_ITT.1,

6.1.7TOE Access (TSS_TA)

TSS_TA.1 **Limit number of sessions and end sessions**

Related SFR: FTA_TSE.1 TOE session setup

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

FTA_SSL.5 Management of TSF-initiated sessions

TSS_TA.1.1 KMS limits the number of concurrent access sessions to one KMS local security manager, one KMS security manager, and two KMS assistance security managers. The TOE enforces the identification and authentication procedures even when the connection is through a terminal with an allowed IP address. If the administrator attempts to log in from another terminal while already successfully logged in, the existing connection is maintained and new connections are not allowed. FTA_TSE.1, FTA_MCS.2

TSS_TA.1.2 KMS, KMS Console terminates the session if the inactivity time is exceeded after successful login. FTA_SSL.5

- KMS CLI: KMS Local Security Manager: The initial value is 5 minutes. Time cannot be adjusted.
- KMS Console:

a. KMS Security Manager: 10 minutes. Time cannot be adjusted.
b. KMS Assistant Security Manager: 10 minutes. Time cannot be adjusted.