D'Amo v4.0

Security Target Lite

Version 1.1

Penta SECURITY

Revision History

Version	Revision Date	Reason for Revision
1.0	2019.05.15	- Sanitized version of the ST version 1.10
1.1	2019.06.11	- Terms and definitions> Add Term - TOE Specification summary> Security management(TSS_MT) supplement content

Table of Contents

Figures

Tables

1 ST Introduction

This Document is D'Amo v4.0 Security Target of Penta Security System Inc. which conforms to EAL 1+ level of Common Criteria.

1.1 ST Reference

Table 1-1..... ST Reference

Title	D'Amo v4.0 Security Target
Version	v1.0
Author	Penta Security System Inc.
Publication Date	2019-05-14
Common Criteria version	CC V3.1 r5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)
Keywords	Database, Encryption

1.2 TOE Reference

Table 1-2..... TOE Reference

TOE Title	D'Amo v4.0
TOE Version	D'Amo v4.0.10 - Agent: D'Amo DP-ORA v4.0.4, D'Amo DP-MSQ v4.0.4 - Management Server: D'Amo DCA v4.0.6 - Management Console: D'Amo DCC Console v4.0.10 - Key Management Server: D'Amo KMS v4.0.10 - Key Management Server Management Console: D'Amo KMS Console v4.0.10 User Guide - D'Amo v4.0 Preparative Procedures, Operational Guide v1.8(DCC Console) - D'Amo v4.0 Preparative Procedures, Operational Guide v1.8(DP-MSQ) - D'Amo v4.0 Preparative Procedures, Operational Guide v1.8(DP-ORA) - D'Amo v4.0 Preparative Procedures, Operational Guide v1.8(KMS)

Developer	Penta Security System Inc.

1.3 TOE overview

1.3.1 TOE summary

TOE is a DB encryption system that protects internal assets from attackers by encrypting user data stored in the protected DB. The main security functions provided by the TOE are encryption and decryption of data stored in the DB, cryptographic key management, access control, and audit.

1.3.2 TOE type and scope

TOE is provided as software and provides encryption/decryption of user data by column. The type of TOE defined in this Security Target is a 'plug-in' type database encryption product. TOE is composed of an agent (hereinafter 'SA'), management server (hereinafter 'DCA'), management console (hereinafter 'DCC console'), key management server (hereinafter 'KMS'), and key management server management console (hereinafter 'KMS console').

1.3.3 TOE usage and major security features

TOE is used to encrypt user data according to the policy set by the authorized administrator to prevent unauthorized exposure of information to be protected. TOE provides security audit function that records and manages audit data about major auditable events to enable authorized administrator to operate TOE securely within organization's operating environment, cryptographic key management for user and TSF data encryption, cryptographic support function such as cryptographic operations, user data protection function that encrypts user data and protects residual information, authorized administrator identity verification, authentication failure handling, identification and authentication functions such as mutual authentication between TOE components, security functions and role definitions, security management function for setting environment, protection of TSF data transmitted between TOE components, protection of TSF data stored in repository controlled by the TSF, TSF protection function such as TSF self-test, and TOE access function for authorized administrator's access session management. The data encryption key (DEK) used to encrypt / decrypt user data is encrypted and protected with a key encryption key (KEK).

1.3.4 TOE operational environment

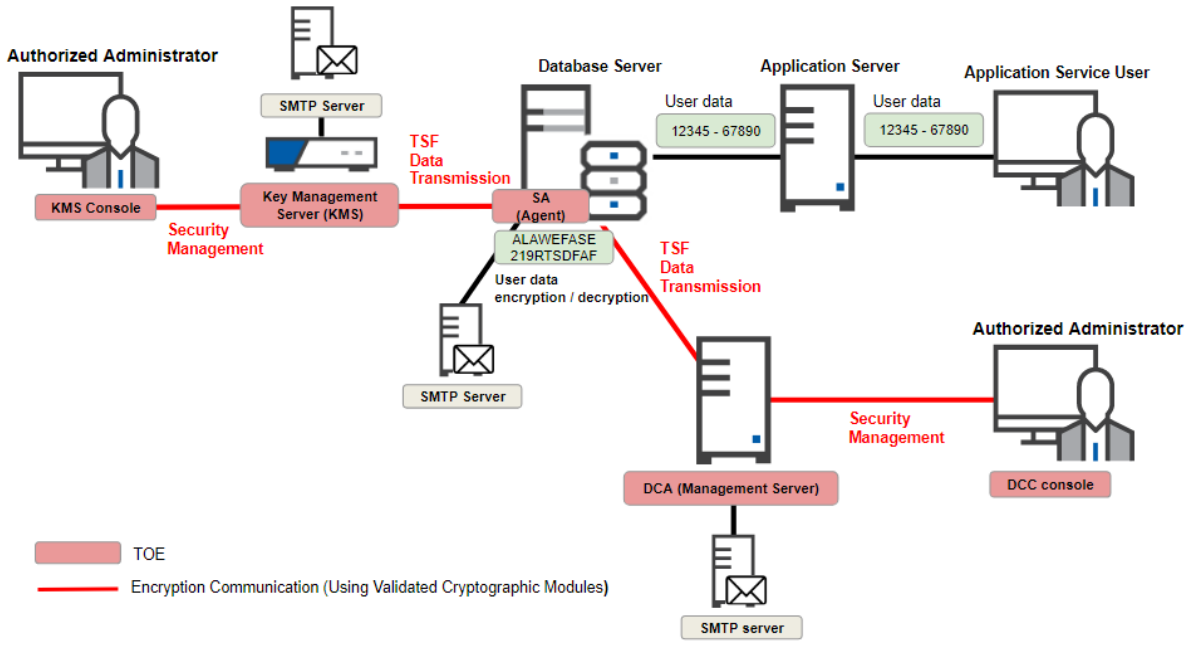
The operating environment of the TOE is 'Plug-in method'. SA is installed in the database server where the protected database exists and encrypts the user data received from the application server according to the policy of the authorized security administrator before storing it in the DB. Also, it decrypts the encrypted user data transmitted from the Database Server to the Application Server.

The operating environment of the TOE is divided into 'Agent and management server separated type' and 'Agent and management server integrated type' according to the installation location of management server and agent.

[Figure 1-1] represents the operating environment of 'agent and management server separated type'. This is installed together with SA in the protected DB, and DCA, DCC Console, and KMS are physically separated and

installed.

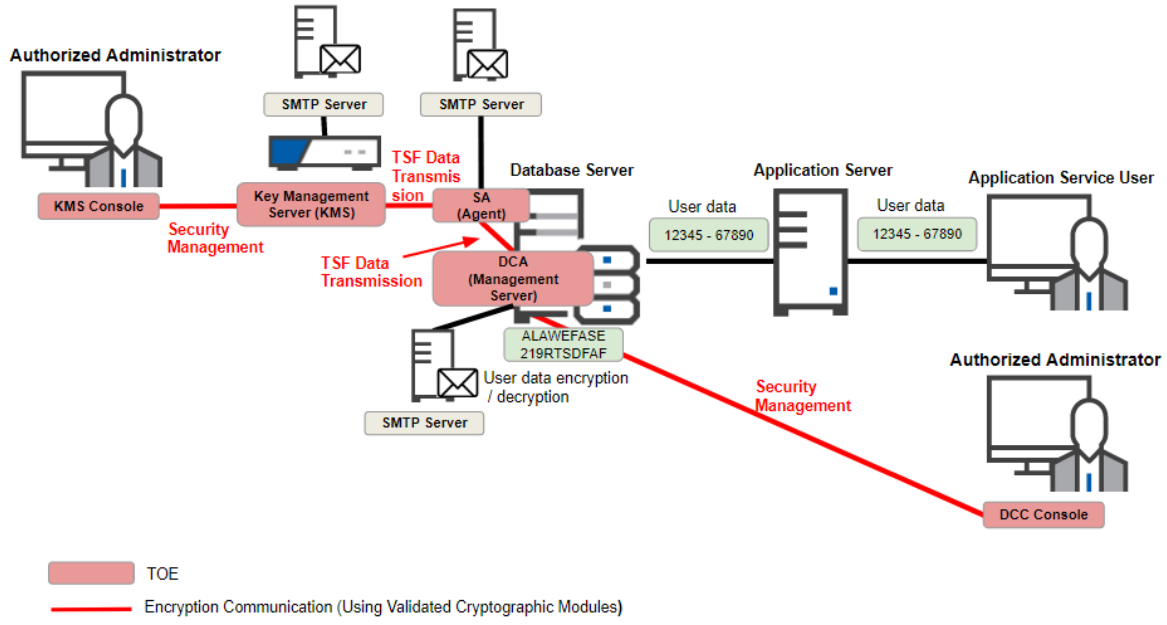
Figure 1-1..... TOE operational environment: Agent and management server separated type



[Figure 1-2] represents the operating environment of 'agent and management server integrated type'. This is installed SA and DCA together in the protected DB, and the DCC Console and KMS are physically separated and installed.

Even when the TOE operates in an 'agent and management server integrated type', TSF data transmission between TOE components performs encryption communication using the validated cryptographic modules. Also, the KMS Console and the DCC Console that provide the authorized administrator's management function perform the encryption communication using the validated cryptographic modules even when accessing the key management server and the management server. There is external IT entities needed to operate the TOE which is a mail server for notification of authorized administrators when predicting audit data loss.

Figure 1-2..... TOE operational environment: Agent and management server integrated type



1.3.5 Non-TOE required by the TOE

1.3.5.1 DCC Console HW/SW/FW

Table 1-3..... DCC Console HW/SW/FW

Type		Minimum requirements	Remarks
H/W	CPU	Intel Core i5 1.60 GHz or higher	
	RAM	4 GB or higher	
	HDD	20 GB or higher (space for TOE installation)	
	NIC	10/100/1000 Mbps x 1EA or higher	
S/W	OS	Windows 7 Pro 32bit Windows Server 2008 R2 Enterprise 32bit Windows 10 Pro K 32bit	Supported operating systems of DCC Console
	3rd Party S/W	.NET Framework 4.6.1	Third-party software required to run DCC Console

1.3.5.2 DCA HW/SW/FW

Table 1-4..... DCA HW/SW/FW

Type		Minimum requirements	Remarks
H/W	CPU	Intel Pentium CPU G4600 3.60 GHz or higher PowerPC_POWER3 450 MHz or higher	
	RAM	8 GB or higher	
	HDD	20 GB or higher (space for TOE installation)	
	NIC	10/100/1000 Mbps x 1EA or higher	
S/W	OS	Windows Server 2012 Standard 64bit Windows Server 2008 R2 Enterprise 64bit Windows 10 Pro K 64bit CentOS release 6.10 (Linux kernel 2.6, 64bit) AIX 5.3 64bit	Supported operating systems of DCA

1.3.5.3 SA HW/SW/FW

Table 1-5..... SA HW/SW/FW

Type		Minimum requirements	Remarks
H/W	CPU	Intel Pentium CPU G4600 3.60 GHz or higher PowerPC_POWER3 450 MHz or higher	
	RAM	8 GB or higher	
	HDD	60 GB or higher (space for TOE installation)	
	NIC	10/100/1000 Mbps x 1EA or higher	
S/W	OS	Windows Server 2012 Standard 64bit	Supported operating systems of SA

Type		Minimum requirements	Remarks
		Windows Server 2008 R2 Enterprise 64bit Windows 10 Pro K 64bit CentOS release 6.10 (Linux kernel 2.6, 64bit) AIX 5.3 64bit	
	3rd Party S/W	Oracle 10g Enterprise Oracle 11g Enterprise Oracle 12c Enterprise SQL Server 2008 R2 Enterprise SQL Server 2012 Enterprise SQL Server 2014 Enterprise	DBMS where SA is installed

1.3.5.4 KMS HW/SW/FW

Table 1-6..... KMS HW/SW/FW

Type	Minimum requirements	Remarks
CPU	Intel Pentium CPU G4600 3.60 GHz or higher	
RAM	8 GB or higher	
HDD	200 GB or higher (space for TOE installation)	
NIC	10/100/1000 Mbps x 1EA or higher	
OS	Debian Linux OS 8.5 (Kernel 3.16)	Supported operating systems of KMS
3rd Party S/W	MariaDB 10.0.25	Third-party software required to run KMS

1.3.5.1 KMS Console HW/SW/FW

Table 1-7..... KMS Console HW/SW/FW

Type		Minimum requirements	Remarks
H/W	CPU	Intel Core i5 1.60 GHz or higher	

Type		Minimum requirements	Remarks
	RAM	4 GB or higher	
	HDD	20 GB or higher (space for TOE installation)	
	NIC	10/100/1000 Mbps x 1EA or higher	
S/W	OS	Windows 10 Pro K 32bit	Supported operating systems of KMS Console
	3rd Party S/W	.NET Framework 4.5	Third-party software required to run KMS Console

1.3.5.2 Other

Table 1-8..... External IT entities

External IT entities	Description
SMTP server	TOE interoperates with SMTP server when sending alarm mail

1.4 TOE description

1.4.1 Physical scope of the TOE

TOE is in the form of software, and the Preparative Procedures and the Operational Guide are loaded on the CD in the form of electronic document (PDF).

Table 1-9..... Physical scope

Type	Format	File name	Delivery Method
TOE components	S/W	• DP-ORA v4.0.4 (Install_DAmo_DP-ORA_v4.0.4.zip) • DP-MSQ v4.0.4 (Install_DAmo_DP-MSQ_v4.0.4.exe) • DCA v4.0.6 (Packages are included with SA) • DCC Console v4.0.10 (Install_DAmo_DCC_Console_v4.0.10.msi) • KMS v4.0.10	CD

		(KMS-4.0.10.kip) • KMS Console v4.0.10 (Install D'Amo KMS Console 4.0.10.exe)	
Manual	Electronic document (PDF)	• D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DCC Console).pdf • D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DP-MSQ).pdf • D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DP-ORA).pdf • D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(KMS).pdf	Electronic document PDF file

The third party list distributed with the TOE is as follows and is not included in the TOE scope.

Table 1-10 ..... 3rd Party list

Type	Usage
.NET Framework 4.6.1	Programs needed to run DCC Console
.NET Framework 4.5	Programs needed to run KMS Console
MariaDB v10.0.25	DBMS used to store DEK, KEK, log, etc. of KMS

Validated cryptographic modules installed in the TOE are as follows.

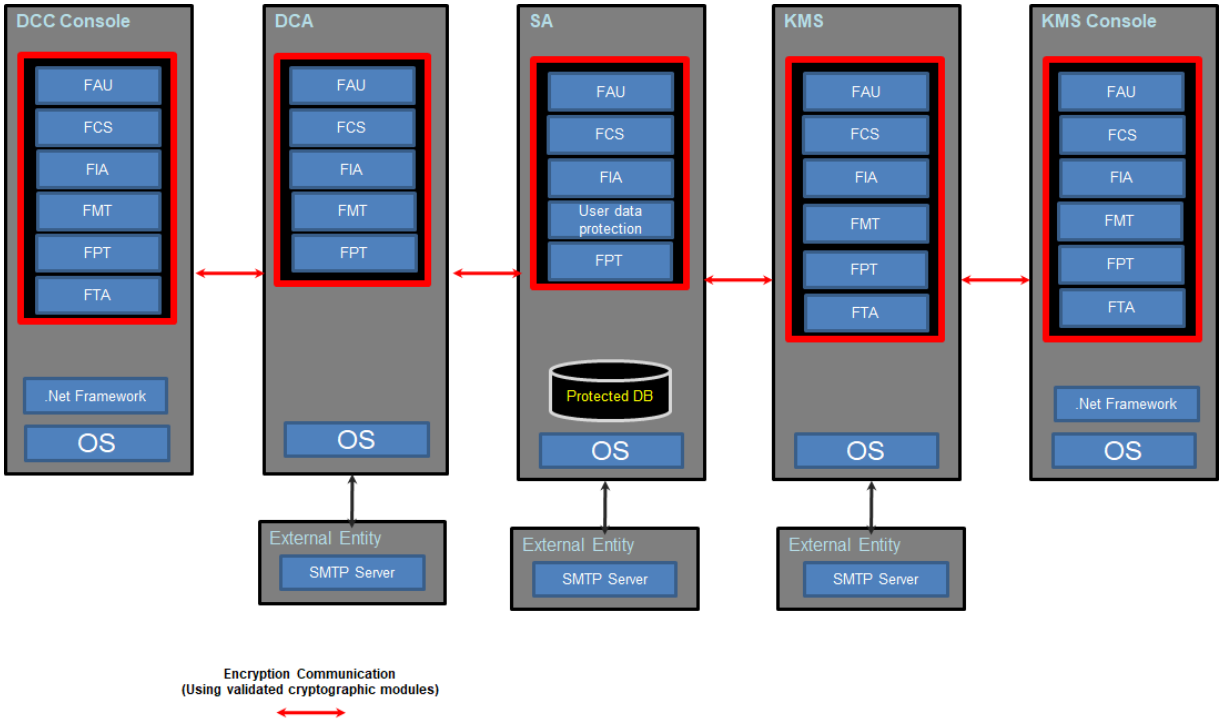
Table 1-11 ..... Validated cryptographic modules

Cryptographic module & version	Validation number	Validation date	Developer
CIS-CC v3.3	CM-145-2023.11	2018-11-07	Penta Security System Inc.

1.4.2 Logical scope of the TOE

TOE provides security functions such as security audit, cryptographic support, user data protection, identification and authentication, security management, TSF protection, and TOE Access as shown in <Figure 1-3>.

Figure 1-3..... Logical scope of the TOE



1.4.2.1 Logical scope of DCC Console

DCC console provides security management features for operating the TOE through a GUI, and the encryption channel (self-implemented security protocol) between DCC console and the DCA sub system ensures safe application of settings, and the transmission/reception of request data.

Security features provided through DCC console are as follows.

Security audit

DCC Console provides the ability to set email alarms related to exceeding the threshold of the audit trail storage or saturating the audit trail and provides a warning message when the audit trail size of the DCC Console exceeds the limit. It also provides warning messages in case of violation after authentication failure and integrity verification. DCC Console generate audit records for Security Manager logins, Security Manager configuration modifications, etc..

DCC Console provides an interface for the log inquiry to the Security Manager, and provides the Security Manager with the ability to selectively review all audit information according to the audit data type, search criteria, and logical relationship.

Cryptographic support

DCC Console generates [keys required for mutual authentication of DCC management tools, DCA, and SA], [key to encrypt setting value], [key for encrypting a cryptographic key] using a random number generator of a validated cryptographic module, CIS-CC v3.3.

DCC Console performs cryptographic key distribution and cryptographic key operations when mutual authentication with the DCA. And it performs encrypted communication after completing mutual authentication with the DCA. The encryption key using in the encryption communication is destroyed in the memory area after the use is completed.

Identification and authentication

DCC Console performs mutual authentication before performing cryptographic communication with the DCA.
DCC Console provides the Security Manager with an interface for certificate-based identification and authentication, and performs the identification and authentication request of the Security Manager.
DCC Console provides a security management UI to the Security Manager and performs ID and password-based identification and authentication to verify the authorized administrator or identity. If the identification and authentication fails, the authentication failure countermeasure function(reject authentication and identification requests for 10 minutes if the maximum number of authentication failures exceeds (5 times)) is provided and detailed information related to the cause of the authentication failure is not provided. DCC Console enforces the rules(minimum of 9 characters combining 4 types of characters including uppercase letters, lowercase letters, numbers, and special characters) for accepting passwords. Also, it prevents input value exposure (converts input values to '*') when inputting password.

Security management

DCC console provides DCC console Security Manager with features for configuring and managing security functions, security properties management, TSF data management, etc..
DCC console provides security functions such as security administrator ID and password criteria management, countermeasures for when the capacity of the log storage reaches the set threshold, and security features for integration with KMS.
DCC console Security Manager manages passwords of security administrators, component information, alert settings for when DCC console, DCA, or SA log storage capacity exceeds threshold, and management of DCC console, DCA, and SA logs.

Protection of the TSF

DCC Console checks the integrity of the executable file at startup and periodically during operation to ensure its correct operation.
DCC Console securely encrypts and transmits data to and from each other using the CIS-CC v3.3, a validated cryptographic module, when sending and receiving configuration and request information to the DCA.
DCC Console securely encrypts and stores the settings related to the DCC Console using CIS-CC v3.3, a validated cryptographic module.

TOE Access

DCC Console prevents unauthorized administrator access by terminating the session of the Security Manager who is logged in when the inactivity time of the Security Manager exceeds a certain period of time.
DCC console only allows management sessions accessing from terminals specified as accessible IP addresses (up to 2). If duplicate login is attempted from a different terminal, the new connection will be blocked and only the first connection will be allowed access.

1.4.2.2 Logical scope of DCA

DCA is a management server for processing tasks between the DCC Console and the SA.
DCA securely transmits and receives configuration information and request information through the encryption channel (self-implemented security protocol) when communicating with the DCC Console and the SA.

The security functions provided through DCA are as follows.

Security audit

DCA generates audit records about DCA execution, mutual authentication success / failure, and results of integrity verification.

DCA will notify the DCC Security Manager by email if the audit trail size exceeds the limit (90MB). When the size of the audit trail is at maximum (100MB), it performs the corresponding action according to the predefined method (Additional logs are not recorded).

Cryptographic support

DCA generates key required for mutual authentication with DCC console and SA, security administrator password, and the encryption key for encrypting DCA's configuration files, etc., using the random number generator from the validated encryption module, CIS-CC v3.3.

DCC console performs cryptographic key distribution and cryptographic key operations during mutual authentication with DCC and SA. And it performs encrypted communication after mutual authentication with DCC console and SA is complete. The encryption key used in the encryption communication is destroyed in the memory area after the use is completed.

Identification and authentication

DCA performs mutual authentication before performing the cryptographic communication with DCC Console and SA.

Security management

DCA provides functions to manage security functions, security attributes management, and TSF data management.

DCA manages the actions to be taken when the capacity of the log storage reaches a set threshold.

DCA manages DCC Security Manager password, component information, DCC Console/DCA log storage capacity threshold alarm setting, DCC Console/DCA log.

Protection of the TSF

The DCA securely encrypts and transmits data to and from each other using the CIS-CC v3.3, a validated cryptographic module, when sending and receiving configuration and request information to the DCC Console and SA.

The DCA securely encrypts and stores [Security Manager account and permissions], [SA component information] using CIS-CC v3.3, a validated cryptographic module.

The DCA checks the integrity of the executable file at startup and periodically during operation to ensure its correct operation.

1.4.2.3 Logical scope of SA

SA is an agent that performs actual encryption and decryption using the encryption / decryption policy set by the DCC Console.

SA securely transmits / receives settings information and request information through the encrypted channel established between the SA and the DCA subsystem.

The security functions provided through SA are as follows.

Security audit

SA generates and records audit records of security-related events to track accountability of security-related incidents.

SA will notify the Security Manager by email if the audit trail size exceeds the limit(90% of the audit trail storage capacity and the user-defined setting threshold value). When the size of the audit trail is at maximum, it performs the corresponding action according to the predefined method(Additional logs are not logged).

Cryptographic support

SA generates key required for mutual authentication with DCA and KMS, and the key for encrypting the encryption key, using the random number generator from the validated encryption module, CIS-CC v3.3.

SA performs cryptographic key distribution and cryptographic key operations during mutual authentication with DCA and KMS. And it performs encrypted communication after mutual authentication with DCA and KMS is complete. The encryption key used in the encryption communication is destroyed in the memory area after the use is completed.

Identification and authentication

SA performs mutual authentication before performing the cryptographic communication with DCA and KMS.

User data protection

SA provides a function to encrypt / decrypt user data, and column-level encryption of ORACLE and MS SQL DB. When SA encrypts user data, it removes the remaining worktable without storing it.

Protection of the TSF

SA securely encrypts and transmits data to and from each other using the CIS-CC v3.3, a validated cryptographic module, when sending and receiving configuration and request information to the DCA and KMS.

SA securely encrypts and stores important data such as data encryption key, access control policy etc. using CIS-CC v3.3, a validated cryptographic module.

SA checks the integrity of the executable file at startup and periodically during operation to ensure its correct operation.

1.4.2.4 Logical scope of KMS

KMS is a key management system that can manage all encryption keys from creation to destruction.

KMS securely transmits / receives setting information and request information through the encrypted channel established between the SA and the KMS subsystem.

The security functions provided through KMS are as follows.

Security audit

KMS generates and records audit records of security-related events to track accountability of security-related incidents.

KMS provides an e-mail alarm function related to exceeding the threshold of audit trail storage or saturation of audit trail, and warning message in case of breach after verifying integrity.

Cryptographic support

KMS generates key required for mutual authentication with KMS, and the key for encrypting the encryption key, using the random number generator from the validated encryption module, CIS-CC v3.3.

KMS performs cryptographic key distribution and cryptographic key operations during mutual authentication with KMS and SA. And it performs encrypted communication after mutual authentication with KMS and SA is complete. The encryption key used in the encryption communication is destroyed in the memory area after the use is completed.

Identification and authentication

KMS performs mutual authentication before performing cryptographic communication with the SA and KMS Console.
KMS enforces password criteria (minimum of 9 characters combining 4 types of characters including uppercase letters, lowercase letters, numbers, and special characters). It also prevents exposure during password input (converts input values to '*').

Security management

The types of managers for KMS are as follows. KMS Local Security Manager that can change the internal settings of the product through the CLI, KMS Security Manager added by KMS Local Security Manager through the CLI command, and Assistant Security Manager with inquiry-only console access permissions added by KMS Security Manager. In addition, the KMS Security Manager can set the password when creating Assistant Security Manager.

Protection of the TSF

KMS securely encrypts and transmits data to and from each other using the CIS-CC v3.3, a validated cryptographic module, when sending and receiving configuration and request information to the SA subsystem.
KMS securely encrypts and stores the data encryption keys using CIS-CC v3.3, a validated cryptographic module.
KMS checks the integrity of the executable file when startup and periodically during operation to ensure its correct operation.

TOE Access

KMS prevents unauthorized administrator access by terminating the session of the Security Manager who is logged in when the inactivity time of the KMS Local Security Manager, KMS Security Manager, or KMS Assistant Security Manager exceeds a certain period of time.
KMS can set accessible IP address(up to 2) of KMS Console.

1.4.2.5 Logical scope of KMS Console

The KMS console provides a GUI for authorized administrator to operate the KMS for security management. And KMS securely transmits / receives setting information and request information through the encrypted channel established between the SA and the KMS subsystem.
The security functions provided through KMS Console are as follows.

Security audit

KMS console generates audit records for Security Manager logins, Security Manager configuration changes, etc..
KMS console provides an interface for Security Managers to perform log inquiries, and provides the Security Manager with the ability to selectively review all audit information according to the audit data type, search criteria, and relational logic.
KMS console provides an e-mail alarm function for when the audit trail threshold is exceeded or audit trail reaches maximum capacity, and warning messages in case of authentication failures or breaches occurring after integrity verification is complete.

Cryptographic support

KMS console generates key required for mutual authentication with KMS, and the key for encrypting the encryption key, using the random number generator from the validated encryption module, CIS-CC v3.3.
KMS console performs cryptographic key distribution and cryptographic key operations during mutual

authentication with KMS. And it performs encrypted communication after mutual authentication with KMS is complete. The encryption key used in the encryption communication is destroyed in the memory area after the use is completed.

Identification and authentication

KMS Console performs mutual authentication before performing cryptographic communication with the KMS. KMS Console provides the Security Manager with an interface for certificate-based identification and authentication, and performs the identification and authentication request of the Security Manager.

If the identification and authentication fails, the authentication failure countermeasure function((reject authentication and identification requests for 10 minutes if the number of authentication failures exceeds limit (5 times)) is provided and detailed information related to the cause of the authentication failure is not provided.

KMS Console enforces the rules(minimum of 9 characters combining 4 types of characters including uppercase letters, lowercase letters, numbers, and special characters) for accepting passwords. Also, it prevents input value exposure (converts input values to '*') when inputting password.

Security management

The Security Manager of KMS Console provides security management function to configure and manage security functions and important data.

The KMS console Security Manager manages data related to the configuration of encryption keys used in encrypting user data, configuration of access control for SA, log backup settings, and environment settings.

Protection of the TSF

KMS Console checks the integrity of the executable file at startup and periodically during operation to ensure its correct operation.

KMS Console securely encrypts and transmits data to and from each other using the CIS-CC v3.3, a validated cryptographic module, when sending and receiving configuration and request information to the KMS.

TOE Access

KMS console prevents unauthorized administrator access by terminating the session of the Security Manager who is logged in when the inactivity time of the Security Manager exceeds a certain period of time.

KMS console can set accessible IP addresses (up to 2) for monitoring managers. In addition, KMS console only allows management sessions accessing from terminals specified as accessible IP addresses.

1.5 Conventions

The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text**.

1.6 Terms and definitions

Most terms used in this ST are consist with the Common Criteria for Information Technology Security Evaluation. Additional terms used only in this ST are as follows.

Object

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

Attack potential

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

Iteration

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

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

User

Refer to "External entity"

Selection

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

Identity

Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE

Element

Indivisible statement of a security need

Role

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

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

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Threat Agent

Entity that can adversely act on assets

Authorized Administrator

Authorized user to securely operate and manage the TOE

- DCC Console
  - DCC Security Manager
- KMS Console
  - KMS Local Security Manager
  - KMS Security Manager,
  - KMS Assistant Security Manager

Authorized User

TOE user who may, in accordance with the SFRs, perform an operation

Authentication Data

Information used to verify the claimed identity of a user

Assets

Entities that the owner of the TOE presumably places value upon

Refinement

Addition of details to a component

Organizational Security Policies
Set of security rules, procedures, or guidelines for an organization wherein the set is currently given by actual or virtual organizations, or is going to be given

Dependency
Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Subject
Active entity in the TOE that performs operations on objects

Augmentation
Addition of one or more requirement(s) to a package

Component
Smallest selectable set of elements on which requirements may be based

Class
Set of CC families that share a common focus

Target of Evaluation (TOE)
Set of software, firmware and/or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Family
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Assignment
The specification of an identified parameter in a component (of the CC) or requirement

TOE Security Functionality (TSF)
Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data
Data for the operation of the TOE upon which the enforcement of the SFR relies

Packet

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

NTP(Network Time Protocol)

NTP is a protocol used to synchronize clock times to networked computers.

DCC Console (D'Amo Control Center console)

The entity of the DCC subsystem, GUI-type console that provides security management function to authorized administrator

DCA (D'Amo Control Agent)

The process of passing the commands entered in the DCC Console to the SA, which can be executed in Windows, Linux, and Unix environments.

SA (Security Agent)

The component that executes the command that is input from the DCC Console.

KMS (Key Management System)

As the key management server, it generates and manages KEK and DEK.

KeyWizard

A program that generates site key pairs, DB key pairs, DCA key pairs, and DCC Console key pairs required for product operation.

Site key pair

It is the public key and private key generated by KeyWizard. Site key pair is required when generating the DCC Console key pair, DCA key pair, and DB key pair. It is also used for mutual authentication with DCC Console, DCA, SA. And It is used for TSF data encryption.

DB key pair

It is the public key and private key generated by KeyWizard. It is used for mutual authentication with DCA in SA. And It is used for TSF data encryption.

DCA key pair

It is the public key and private key generated by KeyWizard. In DCA, It is used for mutual authentication with DCC Console, mutual authentication with SA. And It is used for TSF data encryption.

DCC Console key pair

It is the public key and private key generated by KeyWizard. It is used for mutual authentication with DCA in DCC Console. And It is used for TSF data encryption.

Agent key pair
It is the public key and private key generated by KMS. It is used for mutual authentication with SA in KMS. And It is used for TSF data encryption.

KMS Site key pair
It is the public key and private key generated by KMS. In KMS, It is used for mutual authentication with SA, mutual authentication with KMS Console. And It is used for TSF data encryption.

KMS Console key pair
It is the public key and private key generated by KMS. It is used for mutual authentication with KMS in KMS Console. And It is used for TSF data encryption.

Data Encryption Key (DEK)
The encryption key (symmetric key) used to encrypt the database column data.

Key Encryption Key (KEK)
This is the encryption key used to encrypt the data encryption key, which is the DB key.

Session Key
This is a symmetric key used for cryptographic communication between TOEs. When sending/receiving TSF data, encryption/decryption is performed with that key.

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

Core security parameters
Column key, Security policy file

DCC Security Manager
Security Manager who can set and operate security management function of TOE through DCC Console

KMS Security Manager
Security Manager who can configure and operate TOE security management function through D'Amo KMS Console

KMS Assistant Security Manager

An Assistant Security Manager that can inquire the configuration of security management of TOE through D'Amo KMS Console. The authority to set up or operate the functions of the TOE is limited.

KMS Local Security Manager

Security Manager who can configure and operate TOE security management function through D'Amo KMS.

2 Conformance claim

2.1 CC conformance claim

Table 2-1..... CC conformance claim

Item	Description
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 • Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April 2017) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April 2017) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April 2017)
CC Part2: Security Functional Components	Extended: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
CC Part3: Security Assurance Components	Conformant
Package	Augmented: EAL1 augmented (ATE_FUN.1)

2.2 PP conformance claim

This ST claim conformance the following PP.

- Korean National Protection Profile for Database Encryption V1.0

2.3 Package conformance claim

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

2.4 Conformance claim rationale

This Security Target declares "strict PP conformance" with the Korean National PP for Database Encryption v1.0, and the basis of the declaration is as follows.

Security functional class	Security functional component		Protection Profile Declaration	Security Target Declaration
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
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
FDP	FDP_UDE.1(Extended)	User data encryption	O	O
	FDP_RIP.1	Subset residual information protection	O	O
FIA	FIA_AFL.1	Authentication failure handling	O	O
	FIA_IMA.1(Extended)	TOE Internal mutual authentication	O	O
	FIA_SOS.1	Verification of secrets	O	O
	FIA_UAU.1	Timing of 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

FMT	FMT_MOF.1	Management of security functions behaviour	O	O
	FMT_MTD.1	Management of TSF data	O	O
	FMT_PWD.1(Extended)	Management of ID and password	O	O
	FMT_SMF.1	Specification of management functions	O	O
	FMT_SMR.1	Security roles	O	O
FPT	FPT_ITT.1	Basic internal TSF data transfer protection	O	O
	FPT_PST.1(Extended)	Basic protection of stored TSF data	O	O
	FPT_TST.1	TSF testing	O	O
FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions	O	O
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions	O	O
	FTA_TSE.1	TOE session establishment	O	O

3 Security objectives

3.1 Security objectives for the operational environment

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

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 guidances.

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 checks 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. OPERATION_SYSTEM_REINFORCEMENT

The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

OE. TIMESTAMP

The TOE accurately records incidents related to security by receiving reliable time stamps provided by the TOE operating environments.

OE. AUDIT_DATA_PROTECTION

Audit records with stored audit evidence, such as DBMS that interact with TOE, shall be protected from unauthorized deletion or modification.

4 Extended components definition

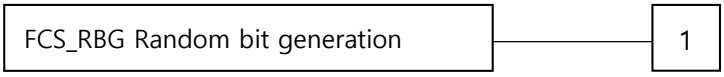
4.1 Cryptographic support

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 auditable 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 an cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

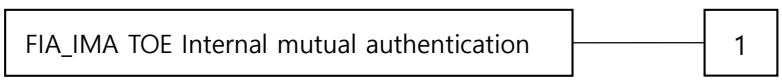
4.2 Identification & authentication

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 is included in the PP/ST:
a) Minimum: Success and failure of mutual authentication.
b) Minimum: Change of authentication protocol.

4.2.1.1 FIA_IMA.1 TOE Internal mutual authentication

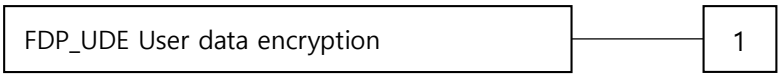
Hierarchical to: No other components.
Dependencies: No dependencies.
The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: *authentication protocol*] that meets the following [assignment: *list of standards*].

4.3 User Data protection

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) The following actions could be considered for the management functions in FMT:

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) Minimum: 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

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

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) Minimum: All changes of the password.

4.4.1.1 FMT_PWD.1 Management of ID and password

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 [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.*]

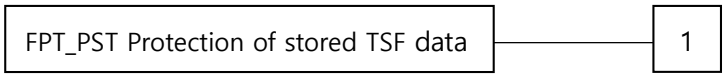
FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]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

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 auditable 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*].

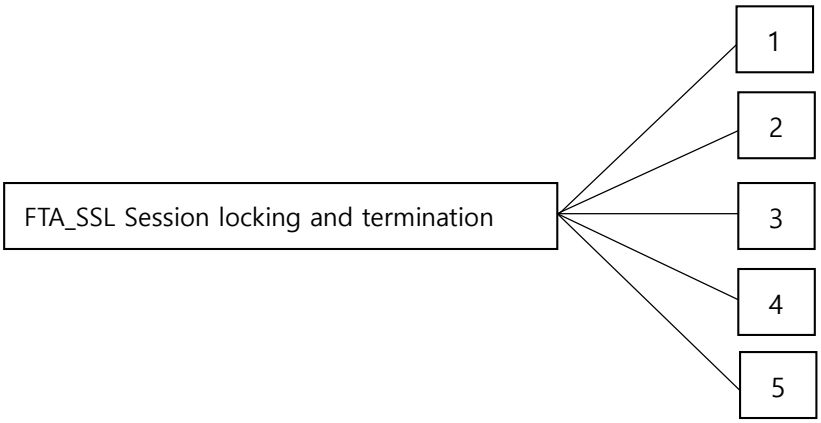
4.6 TOE Access

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.

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) Minimum: 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 No dependencies.

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

This chapter describes the security functional requirements and assurance requirements that the TOE should provide.

5.1 Security functional requirements

The security functional requirements of this Security Target are composed by selecting relevant functional components from CC Part 2 and Chapter 4 extended component definition. Table 5-1 summarizes the security functional requirements components used in this Security Target.

Table 5-1..... Security functional requirements

Security functional class	Security functional component		Optional SFR
FAU	FAU_ARP.1	Security alarms	
	FAU_GEN.1	Audit data generation	
	FAU_SAA.1	Potential violation analysis	
	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	
	FAU_STG.3	Action in case of possible audit data loss	
	FAU_STG.4	Prevention of audit data loss (DCC Console, DCA, SA, KMS, KMS Console)	
FCS	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 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)	

Security functional class	Security functional component		Optional SFR
	FCS_RBG.1(Extended)	Random bit generation (Extended)	
FDP	FDP_UDE.1(Extended)	User data encryption	
	FDP_RIP.1	Subset residual information protection	
FIA	FIA_AFL.1	Authentication failure handling	
	FIA_IMA.1(1)(Extended)	TOE Internal mutual authentication (mutual authentication of DCC-DCA communication section)	
	FIA_IMA.1(2)(Extended)	TOE Internal mutual authentication (mutual authentication of DCA-SA communication section)	
	FIA_IMA.1(3)(Extended)	TOE Internal mutual authentication (mutual authentication of SA-KMS communication section)	
	FIA_IMA.1(4)(Extended)	TOE Internal mutual authentication (mutual authentication of KMS-KMS Console communication section)	
	FIA_SOS.1	Verification of secrets	
	FIA_UAU.1(1)	Timing of authentication (DCC Security Manager)	
	FIA_UAU.1(2)	Timing of authentication (KMS Security Manager)	
	FIA_UAU.1(3)	Timing of authentication (KMS Assistant Security Manager)	
	FIA_UAU.2	User authentication before any 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 (DCC Security Manager)	
	FIA_UID.1(2)	Timing of identification (KMS Security Manager)	

Security functional class	Security functional component		Optional SFR
	FIA_UID.1(3)	Timing of identification (KMS Assistant Security Manager)	
	FIA_UID.2	User identification before any action (KMS Local Security Manager)	
FMT	FMT_MOF.1(1)	Management of security functions behaviour (DCC Security Manager)	
	FMT_MOF.1(2)	Management of security functions behaviour (KMS Security Manager)	
	FMT_MTD.1(1)	Management of TSF data (DCC Security Manager)	
	FMT_MTD.1(2)	Management of TSF data (KMS Security Manager)	
	FMT_MTD.1(3)	Management of TSF data (KMS Assistant Security Manager)	
	FMT_MTD.1(4)	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	
FPT	FPT_ITT.1	Basic internal TSF data transfer protection	
	FPT_PST.1(Extended)	Basic protection of stored TSF data	
	FPT_TST.1	TSF testing	
FTA	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 [actions on <Table 5-2 Actions for potential security violation>] upon detection of a potential security violation.

Table 5-2..... Actions for potential security violation

Type	Security functional component	Potential security violation	Countermeasure
DCC Console	FPT_TST.1	selftest failure event of validated cryptographic module	Service disabling
		integrity violation audit event of validated cryptographic module	- At start-up: Service disabling - Periodically: Show warning message
		Other integrity violation audit event	Show warning message
	FIA_AFL.1	[DCC Security Manager] authentication failure audit event	Show warning message
SA	FAU_STG.3	An event that the audit trail exceeds the specified threshold	Notify by email designated by authorized administrator
	FAU_STG.4	An event that the audit trail is full	Notify by email designated by authorized administrator
	FPT_TST.1	selftest failure event of validated cryptographic module	Service disabling
		integrity violation audit event of validated cryptographic module	- At start-up: Service disabling - Periodically: Notify by email designated by authorized administrator
		Other integrity violation audit event	- At start-up: Show warning message - Periodically: Notify by email designated by authorized administrator
DCA	FAU_STG.3	An event that the DCC console, DCA audit trail exceeds the specified threshold	Notify by email designated by authorized administrator
	FAU_STG.4	An event that the DCC console, DCA audit trail is full	Notify by email designated by authorized administrator
	FPT_TST.1	selftest failure event of validated cryptographic module	Service disabling

Type	Security functional component	Potential security violation	Countermeasure
		integrity violation audit event of validated cryptographic module	- At start-up: Service disabling - Periodically: Termination of violation process execution
		Other integrity violation audit event	Termination of violation process execution
KMS	FAU_STG.3	An event that the audit trail exceeds the specified threshold	Notify by email designated by authorized administrator
	FAU_STG.4	An event that the audit trail is full	Notify by email designated by authorized administrator
	FPT_TST.1	selftest failure event of validated cryptographic module	Service disabling
		integrity violation audit event of validated cryptographic module	- At start-up: Service disabling - Periodically: Notify by email designated by authorized administrator
		Other integrity violation audit event	Notify by email designated by authorized administrator
	FIA_AFL.1	[KMS Local Security Manager] authentication failure audit event	Notify by email designated by authorized administrator
KMS Console	FPT_TST.1	selftest failure event of validated cryptographic module	Service disabling
		integrity violation audit event of validated cryptographic module	- At start-up: Service disabling - Periodically: Show warning message
		Other integrity violation audit event	Show warning message
	FIA_AFL.1	[KMS Security Manager, KMS Assistant Security Manager] authentication failure audit event	Show warning message

FAU_GEN.1 Audit data generation

```
Hierarchical to:    No other components.
Dependencies:       FPT_STM.1    Reliable time stamps
```

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

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

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

c) [Refer to the "auditable events" in [Table 5-3] Audit events]

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]

Table 5-3..... Audit events

Security functional component	Auditable 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 the activity	-
FDP_UDE.1 (Extended)	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 state	-
FIA_IMA.1 (Extended)	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 (Extended)	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 (Extended)	Locking or termination of interactive 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 that the audit trail exceeds the specified threshold among auditable events of FAU_STG.3
- An event that the audit trail is saturated among auditable events of FAU_STG.4]]

known to indicate a potential security violation

b) [none]

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

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

FAU_SAR.1.1 The TSF shall provide [**DCC Security Manager**] with the capability to read [**all the audit data of DCC Console, DCA, SA**] from the audit records.

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

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

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

FAU_SAR.1.1 The TSF shall provide [**KMS Security Manager**] with the capability to read [**all the audit data of KMS, KMS Console**] from the audit records.

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

FAU_SAR.1(3) Audit review (KMS Assistant Security Manager)

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

FAU_SAR.1.1 The TSF shall provide [**KMS Assistant Security Manager**] with the capability to read [**all the audit data of KMS, KMS Console**] from the audit records.

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [*criteria with logical relations*] of audit data based on [*methods of selection and/or ordering*]. <SA>

a) criteria with logical relations – Required items (AND)
   - Types of audit data: Access log, Policy log
   - Search period: Start date, End date
   - ID: Log filter ID

b) criteria with logical relations – Required items (AND)
   - Log separator: Separator indicating characteristics of logs

- Owner: Name of owner of the table to be logged
- Table: Name of table to be logged
- Column: Name of column to be logged
- Policy: Name of policy to be logged
- IP: IP address of DCC console Security Manager
- DB account: Oracle account for generating policy logs
- SP_ALIAS: SP_ALIAS to be logged
- No selection available

c) Selection and/or sorting method

- The audit data type AND search period (start date, end date) AND ID (log filter ID) specified by the authorized administrator
- Each item can be sorted in ascending / descending order (Initial value: Sort by time in ascending order)

<DCC Console/DCA>

a) criteria with logical relations(AND)

- Search period: Start date, End date

b) Selection and/or sorting method

- Sort by search period in descending order
- Each item can be sorted in ascending / descending order (Initial value: Sort by time in ascending order)

<KMS>

a) criteria with logical relations(AND)

- Search period: Start date, End date
- Number of views
- Log level : Select between warning, error, success, and debug
- Keyword search

b) methods of selection and/or ordering

- The type of audit data specified by KMS Security Manager or KMS Assistant Security Manager AND Search period(Recently 1, 6, 12, 24 hours and custom) AND Type AND Level AND Count
- Each item can be sorted in ascending / descending order (Initial value: Sort by time in ascending order)

[Precautions] For audit data, event type, date of occurrence (event date), subject, information (event type, event result), remarks (other information) 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, [Corresponding action of Table 5-4] if the audit trail exceeds [Capacity limits of audit trail test conditions of Table 5-4].

Table 5-4..... Capacity limits of audit trail test conditions and corresponding action

Object	Capacity limit	Corresponding action
SA Log	90%, Customizable	Send email notifications
DCC Console, DCA Log	90MB	Send email notifications
KMS, KMS Console Log	90%, Customizable	Send email notifications

FAU_STG.4 Prevention of audit data loss (DCC Console, DCA, SA, KMS, KMS Console)

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 audited events* and [Table 5-5] if the audit trail is full.

Table 5-5..... Action in case of possible audit data loss

Object	Capacity limit	Corresponding action
SA, KMS, KMS Console Log	100%	Send email notifications
DCC Console, DCA Log	100MB	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 [Table 5-6 cryptographic key generation algorithm] and specified cryptographic key sizes [Table 5-6 cryptographic key sizes] that meet the following: [Table 5-6].

Table 5-6..... Cryptographic key generation algorithm(Cryptographic algorithm, Key size)

	List of standards	Cryptographic key algorithm	Key size	Usage
#1	TTAK.KO-12.0190	Hash_DRBG	128, 256, 384, 512	Keys used to encrypt user data

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 [Table 5-7 cryptographic key generation algorithm] and specified cryptographic key sizes [Table 5-7 cryptographic key sizes] that meet the following: [Table 5-6].

Table 5-7..... Cryptographic key generation algorithm(Cryptographic algorithm, Key size)

	List of standards	Cryptographic key algorithm	Key size	Usage
#1	TTAK.KO-12.0190	Hash_DRBG	128, 256	Keys used to encrypt TSF data
#2	KS X ISO/IEC 18033-2	RSAES	2048	Encrypting the session key
#3	PKCS#5	PBKDF2	256	TSF data encryption

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 distribute cryptographic keys in accordance with a specified cryptographic key distribution method[Table 5-8 Cryptographic key distribution method(Encrypting user data)] that meets the following: [none].

Table 5-8..... Cryptographic key distribution method(Encrypting user data) – KMS

Main agent	Distribution target	Distribution method
KMS	Key used for user data	Verification Cipher module CIS-CC v3.3 is

Main agent	Distribution target	Distribution method
	encryption in FCS_CKM.1 (1)	used for communication encryption through mutual authentication.

FCS_CKM.2(2) Cryptographic key distribution (mutual authentication and encryption communication 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 distribute cryptographic keys in accordance with a specified cryptographic key distribution method[Table 5-9, Table 5-10 Cryptographic key distribution method(Mutual authentication and cryptographic communication between TOE components)] that meets the following: [none].

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

Main agent	Distribution target	Distribution method
between SA/KMS Console and KMS	Session key	Verification Cipher module CIS-CC v3.3 is used for communication encryption through mutual authentication.

Table 5-10 ..... Cryptographic key distribution method(Mutual authentication and cryptographic communication between TOE components) – between DCC Console and DCA, SA

Main agent	Distribution target	Distribution method
between DCC Console and DCA, SA	Session key	Verification Cipher module CIS-CC v3.3 is used for communication encryption through mutual authentication.

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 [Change all plaintext encryption keys and security-critical parameters in the device associated with the encryption key to '0x00, 0x55, 0xAA' (KMS), and '0x00' (non-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 [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [Table 5-11 cryptographic algorithm] and cryptographic key sizes [Table 5-11 cryptographic key sizes] that meet the following: [Table 5-11 list of standards].

Table 5-11 ..... Cryptographic operation list

	List of standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operation list
#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

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 [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [Table 5-12 cryptographic algorithm] and cryptographic key sizes [Table 5-12 cryptographic key sizes] that meet the following: [Table 5-12 list of standards].

Table 5-12 ..... Cryptographic operation list

	List of standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operation list
#1	TTAS.KO-12.0004/R1, TTAS.KO-12.0025	SEED	128	SA TSF data
#2	KS X 1213-1, KS X 1213-2	ARIA	256	1) KMS TSF data 2) DCC Console, DCA TSF data 3) KMS Console TSF data 4) SA TSF data 5) It is used for packet encryption with session key
#3	KS X ISO/IEC 18033-2	RSAES	2048	1) It is used for mutual authentication between DCC Console, DCA and SA 2) It is used for mutual authentication between KMS Console, KMS and SA 3) It is used to encrypt the KEK generated by KMS.
#4	ISO/IEC 14888-2,RFC 3447	RSA-PSS	2048	Electronic signature when distributing cryptographic keys
#5	KS X ISO/IEC 9797-2	HMAC_SHA	256	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 [Table 5-13 list of standards].

Table 5-13 ..... Random bit generation list

List of standards	Cryptographic algorithm
ISO/IEC 18031-3(2005)	Hash_DRBG

5.1.3 User 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].

5.1.4 Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.1 The TSF shall detect when *[5 times]* unsuccessful authentication attempts occur related to [[**DCC Security Manager, KMS Local Security Manager, KMS Security Manager, KMS Assistant Security Manager**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [Response actions that do not process identification and authentication requests for 10 minutes (account lockout)].

FIA_IMA.1(1) TOE Internal mutual authentication (Extended) (mutual authentication between DCC Console and DCA communication section)

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

FIA_IMA.1.1 The TSF shall perform mutual authentication using [Self-Implementation authentication protocol] in accordance with [none] between [DCC Console and DCA].

FIA_IMA.1(2) TOE Internal mutual authentication (Extended) (mutual authentication between DCA and SA communication section)

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

FIA_IMA.1.1 The TSF shall perform mutual authentication using [Self-Implementation authentication protocol] in accordance with [none] between [DCA and SA].

FIA_IMA.1(3) TOE Internal mutual authentication (Extended) (mutual authentication between SA console and KMS communication section)

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

FIA_IMA.1.1 The TSF shall perform mutual authentication using [Self-Implementation authentication protocol] in accordance with [none] between [SA and KMS].

FIA_IMA.1(4) TOE Internal mutual authentication (Extended) (mutual authentication between KMS and KMS Console communication section)

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

FIA_IMA.1.1 The TSF shall perform mutual authentication using [Self-Implementation 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 secrets meet [Table 5-14 The acceptance criteria for each TOE].

Table 5-14 ..... The acceptance criteria for each TOE

	TOE	Explanation
#1	DCC Console	a) Allowed characters - Uppercase (A ~ Z, 26 kinds) - Lowercase (a ~ z, 26 kinds) - Number (0 ~ 9, 10 kinds) - Special character (32 kinds): `~!@#$%^&*()-_=+₩|[]{};:'",.<>/? b) Combination rule - Uppercase, lowercase, number, and special characters must each contain at least one. - The same character cannot be used more than 3 times consecutively - Alphabets and numbers cannot be used in ascending or descending order three or more times in a row c) Minimum length: 9 characters (9byte) d) Maximum length: 15 characters (15byte)
#2	KMS	a) Allowed characters - Uppercase(A ~ Z, 26 kinds)

	TOE	Explanation
		- Lowercase(a ~ z, 26 kinds) - Number(0 ~ 9, 10 kinds) - Special character: *~!@#$%()-=+;|₩.,/? Available b) Combination rule - Uppercase, lowercase, number, and special characters must each contain at least one. - The same character cannot be used more than 3 times consecutively - Alphabets and numbers cannot be used in ascending or descending order three or more times in a row c) Minimum length: 9 characters (9byte) d) Maximum length: 15 characters (15byte)
#4	KMS Console	a) Allowed characters - Uppercase(A ~ Z, 26 kinds) - Lowercase(a ~ z, 26 kinds) - Number (0 ~ 9, 10 kinds) - Special character: Only special characters other than >& | ; can be used b) Combination rule - Uppercase, lowercase, number, and special characters must each contain at least one. - The same character cannot be used more than 3 times consecutively - Alphabets and numbers cannot be used in ascending or descending order three or more times in a row c) Minimum length: 9 characters (9byte) d) Maximum length: 15 characters (15byte)

FIA_UAU.1(1) Timing of authentication (DCC 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 **DCC Security Manager** to be performed before the **DCC Security Manager** is authenticated.[

a) Selection of the storage location / medium of the DCC Console certificate.

b) Entering the certificate password for running the DCC Console

c) I/M server settings]

FIA_UAU.1.2 The TSF shall require each **DCC Security Manager** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **DCC Security Manager**, except for the actions specified in FIA_UAU.1.1.

FIA_UAU.1(2) 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) Selection of the storage location / medium of the KMS Console certificate.]

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**, except for the actions specified in FIA_UAU.1.1.

FIA_UAU.1(3) 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) Selection of the storage location / medium of the KMS Console certificate]

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**, except for the actions specified in FIA_UAU.1.1.

FIA_UAU.2 User authentication before any action (KMS Local Security Manager)

Hierarchical to: FIA_UAU.1 Timing of 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 DCC Console's Security Manager
b) The authentication mechanism used to authenticate the KMS Security Manager, Assistant

Security Manager
c) 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 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [The following list of feedback] to the user while the authentication is in progress. [

a) When inputting secret information (password), change the converts input values to mock character (eg '•' character) and output it.

b) Displays an 'authentication failure message'(Must not distinguish between ID and / or password errors) that does not contain detailed information about the reason for the failure.]

FIA_UID.1(1) Timing of identification (DCC 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 **DCC Security Manager** to be performed before the **DCC Security Manager** is identified. [

a) Selection of the storage location / medium of the DCC Console certificate.

b) Entering the certificate password for running the DCC Console.

c) I/M server settings]

FIA_UID.1.2 The TSF shall require each **DCC Security Manager** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **DCC Security Manager** , except for the actions specified in FIA_UAU.1.1.

FIA_UID.1(2) 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) Selection of the storage location / medium of the KMS Console certificate.]

FIA_UID.1.2 The TSF shall require each **KMS Security Manager** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **KMS Security Manager** , except for the actions specified in FIA_UAU.1.1.

FIA_UID.1(3) 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) Selection of the storage location / medium of the KMS Console certificate.]

FIA_UID.1.2 The TSF shall require each **KMS Assistant Security Manager** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **KMS Assistant Security Manager ,** except for the actions specified in FIA_UAU.1.1.

FIA_UID.2 User identification before any 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.**

5.1.5 Security management (FMT)

FMT_MOF.1(1) Management of security functions behaviour (DCC Security Manager)

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 [The following list of functions] to [DCC Security Manager]. [

a) *enable* about actions to take when the capacity of the log repository reaches a set threshold.

b) *enable, disable* about Interworking between SA and KMS]

FMT_MOF.1(2) Management of security functions behaviour (KMS Security Manager)

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 [The following list of functions] to [KMS Security Manager]. [

a) *enable* about actions to take when the capacity of the log repository reaches a set threshold.

b) *enable, disable* about actions to take in case of authentication failure]

FMT_MTD.1(1) Management of TSF data (DCC 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 [DCC Security Manager]. [

a) *modify about DCC Security Manager password*

b) *query, delete about component information*

c) *query, modify about DCC Console, DCA, SA audit data storage capacity threshold notification setting*

d) *query about DCC Console, DCA, SA log*

e) *query, modify, delete about DCC Console access permission IP setting*

f) *query, modify about DCC Security Manager's maximum allowable value for inactivity period*

i) *query, modify, delete about encryption policy and service*]

FMT_MTD.1(2) 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) *modify about KMS Security Manager password*

b) *query, modify about KMS audit data storage capacity threshold notification setting*

c) *query about KMS log*

d) *query, modify about KMS Console access permission IP setting*

e) *query, modify about KMS Security Manager's maximum allowable value for inactivity period*

f) *query, modify, delete about encryption policy and service*]

FMT_MTD.1(3) 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) *query about KMS audit data storage capacity threshold notification setting*

b) *query about KMS log*

c) *query about KMS Console access permission IP setting*

d) *query about KMS Security Manager's maximum allowable value for inactivity period*

e) *query about encryption policy and service*]

FMT_MTD.1(4) 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, delete about KMS Console access permission IP setting*

b) *modify about 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 [DCC Security Manager, KMS Local Security Manager, KMS Security Manager].

1. [none]
2. [none]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [DCC Security Manager].

1. [none]
2. [none]

FMT_PWD.1.3 The TSF shall provide the capability for [setting ID and 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 of performing the following management functions: [

a) Security functional management list specified in FMT_MOF.1
b) List of TSF data management 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 [Table 5-15 Security roles of authorized administrator for each TOE].

Table 5-15 ..... Security roles of authorized administrator for each TOE

No.	TOE	Security roles	Explanation
#1	DCC Console	DCC Security Manager	Set security policies of TOE by accessing DCC console
#2	KMS	KMS Local Security Manager	This is the manager which has authority to create KMS Security Managers who can change the product's internal settings through the CLI.

No.	TOE	Security roles	Explanation
#3		KMS Security Manager	This is the manager added by 'KMS Local Security Manager' through CLI command. 'KMS Security Manager' can use all the functions of console.
#4		KMS Assistant Security Manager	This is the manager added by 'KMS Security Manager' through the console. The KMS assistant manager has the authority to query encryption keys, logs, etc.. Activity is restricted to queries through the management console.

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

5.1.6 Protection 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 TSF data list] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.[

a) SA> Data encryption key(Cryptographic key to be used for user data encryption)
b) SA> KMS interworking configuration file
c) SA> authority setting information of encryption / decryption (Information on setting encryption / decryption permission for user data encryption column)
d) SA> Log threshold email notification SMTP server settings information
e) DCA> DCC Security Manager ID, password information, component information
f) DCA> Configuration file
g) DCA> DCC Console, DCA log
h) DCA> DCC Console, DCA Log threshold email notification SMTP server settings information
i) KMS> Data encryption key(Cryptographic key to be used for user data encryption)
j) KMS> DB account connection 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 TSF list*].

a) *DCC Console executable*
b) *DCA executable*
c) *KMS executable*
d) *KMS Console executable*

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [*The following TSF data list*].

e) *SA policy log, access log, KMS interworking configuration file*
f) *DCA configuration file*
g) *KMS service log, system log, administrator log*

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [*The following TSF data list*].

a) *DCC Console executable*
b) *DCA executable*
c) *SA library*
d) *KeyWizard executable*
e) *CIS-CC v3.3 library*
f) *KMS executable*
g) *KMS Console executable*

[Precautions] The authorized administrator specified in this SFR shall mean the security administrator specified in FMT_SMR.1.1.

5.1.7 TOE 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 { Table 5-16 Number of sessions of administrators with query privileges for each TOE} 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 5-16 ..... Number of sessions of administrators with query privileges for each TOE

	List	No. of sessions by administrators with query privileges
#1	DCC Console	0 (none)
#2	KMS Console	2

c) [Table 5-17 Maximum number of concurrent sessions for each TOE]

Table 5-17 ..... Maximum number of concurrent sessions for each TOE

	List	Maximum no. of concurrent sessions
#1	DCC Console	DCC Security Manager: 1
#2	KMS Console	KMS Security Manager: 1 KMS Assistant Security Manager: 2

FTA_MCS.2.2 The TSF shall enforce a 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 no dependencies.

FTA_SSL.5.1 The TSF shall [*terminate*] the administrator's interactive session after a [Table 5-18 Time interval of the administrator inactivity for each TOE].

Table 5-18 ..... Time interval of the administrator inactivity for each TOE

		Period of inactivity for each TOE
#1	DCC Console	The initial value is 10 minutes, and the time can be adjusted from 10 minutes to 60 minutes after login of the console.
#2	KMS CLI	5 minutes fixed.
#3	KMS Console	KMS Security Manager: The initial value is 10 minutes, and the time can be adjusted from 10 minutes to 60 minutes after login of the console. KMS Assistant Security Manager: 10 minutes fixed.

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

ASE_INT.1 introduction

Dependencies: No dependencies.

Developer action elements

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 overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C TOE overview shall identify the TOE type.

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

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

ASE_INT.1.8C 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 elements

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 elements

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 elements

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 elements

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 statement of security requirements shall 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 elements

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

Content and presentation elements

ASE_TSS.1.1C 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.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements

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.

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements

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 elements

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.

5.2.4 Life-cycle support

ALC_CMC.1 TOE Lavelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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 elements

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.

5.2.5 Tests

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 elements

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

Content and presentation elements

ATE_IND.1.1C 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 test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability 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 elements

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

Content and presentation elements

AVA_VAN.1.1C 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

The following <Table 5-19> shows the dependencies of the functional components.

FAU_GEN.1 has the dependency on FPT_STM.1, but in the case of TOE of this Security Target, since the function is supported by the operating environment, the security objective (OE.TIMESTAMP) for the operating environment is added, therefore the dependency is satisfied.

FAU_STG.3, FAU_STG.4 have dependencies on FAU_STG.1. However, only the authorized administrator can access the place where the TOE is installed and operated. Therefore instead of FAU_STG.1, dependency of FAU_STG.3 and FAU_STG.4 is satisfied by OE.AUDIT_DATA_PROTECTION.

Table 5-19 ..... Dependency of TOE security functional requirements

Num	Security functional component	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	OE.TIMESTAMP
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
8	FAU_STG.3	FAU_STG.1	OE.AUDIT_DATA_PROTECTION
9	FAU_STG.4	FAU_STG.1	OE.AUDIT_DATA_PROTECTION
10	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	13, 16
		FCS_CKM.4	15
11	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	14, 17
		FCS_CKM.4	15
12	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	11
		FCS_CKM.4	15
13	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	12
		FCS_CKM.4	15
14	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	11,12
15	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	11
		FCS_CKM.4	15
16	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	12
		FCS_CKM.4	15

17	FCS_RBG.1	-	-
18	FDP_UDE.1	FCS_COP.1	16
19	FDP_RIP.1	-	-
20	FIA_AFL.1	FIA_UAU.1	27,28,29,30
21	FIA_IMA.1(1)	-	-
22	FIA_IMA.1(2)	-	-
23	FIA_IMA.1(3)	-	-
24	FIA_IMA.1(4)	-	-
25	FIA_SOS.1	-	-
26	FIA_UAU.1(1)	FIA_UID.1	33
27	FIA_UAU.1(2)	FIA_UID.1	34
28	FIA_UAU.1(3)	FIA_UID.1	35
29	FIA_UAU.2	FIA_UID.1	36
30	FIA_UAU.4	-	-
31	FIA_UAU.7	FIA_UAU.1	27,28,29,30
32	FIA_UID.1(1)	-	-
33	FIA_UID.1(2)	-	-
34	FIA_UID.1(3)	-	-
35	FIA_UID.2	-	-
36	FMT_MOF.1(1)	FMT_SMF.1	44
		FMT_SMR.1	45
37	FMT_MOF.1(2)	FMT_SMF.1	44
		FMT_SMR.1	45
38	FMT_MTD.1(1)	FMT_SMF.1	44
		FMT_SMR.1	45
39	FMT_MTD.1(2)	FMT_SMF.1	44
		FMT_SMR.1	45
40	FMT_MTD.1(3)	FMT_SMF.1	44
		FMT_SMR.1	45
41	FMT_MTD.1(4)	FMT_SMF.1	44
		FMT_SMR.1	45
42	FMT_PWD.1	FMT_SMF.1	44
		FMT_SMR.1	45
43	FMT_SMF.1	-	-
44	FMT_SMR.1	FIA_UID.1	33,34,35,36
45	FPT_ITT.1	-	-
46	FPT_PST.1	-	-
47	FPT_TST.1	-	-

48	FTA_MCS.2	FIA_UID.1	33,34,35,36
49	FTA_SSL.5	FIA_UAU.1	27,28,29,30
50	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 Specification summary

6.1 TOE security functions

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 generates audit data on the list of auditable events for follow-up in case of a potential security violation event. At this time, the TOE includes the date and time of occurrence of the event, the type of event, the identity (if possible) of the entity that caused the event, the details of the operation and the result (success / failure). Refer to <Table 5-3> described in FAU_GEN.1.1 of the ST for details related to TOE auditable event list.

TSS_AU.1.2 The TOE receives and uses the time information from the trusted operating system of the TOE operating environment to generate accurate time information about the event when generating the audit data.

TSS_AU.2 **Security violation event**

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

TSS_AU.2.1 The TSF detects potential violations of <Table 5-2> and performs corresponding action against the violation events.

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 function that the authorized administrator can read all the audit information through the DCC Console.

TSS_AU.3.2 The TOE provides a function to selectively review audit data according to [audit data type], [search criteria], [logical relationship between search criteria (AND)] when the authorized administrator reviews the audit data. The audit review criteria, selection / ordering methods, and ordering criteria items refer to the specification in FAU_SAR.3.1 of the ST.

TSS_AU.4 **Action in case of possible audit data loss**

Related SFR: FAU_STG.3 Action in case of possible audit data loss
FAU_STG.4 Prevention of audit data loss (DCC Console, DCA, Sa, KMS, KMS Console)

TSS_AU.4.2 SA, one of the TOE, sets the size of the audit data based on the total capacity of the DBMS tablespace, and notifies the authorized administrator to take action when the audit data size exceeds 90% or the limit set by the user, or exceeds 90MB in the case of the DCC console and DCA, or when KMS goes over 90% of the limit set by the user.

TSS_AU.4.3 Within the TOE, DCC console, DCA, and SA prevent the loss of audit data through a feature provided by the TOE's operating environment which prevents further recording of data when full audit data capacity is

reached.

6.1.2 Cryptograpic 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 encrypting the user data and a key for encrypting the TSF data using the validated cryptographic module CIS-CC v3.3.

Table 6-1..... validated cryptographic modules

Cryptographic module & version	Validation number	Validation date	Developer
CIS-CC v3.3	CM-145-2023.11	2018-11-07	Penta Security System Inc.

When generating the encryption key, it is generated using the random number generator provided in the validated cryptographic module CIS-CC v3.3. The following table describes the cryptographic algorithms, cryptographic key sizes, and cryptographic operations of the TOE.

Table 6-2..... User data cryptographic operation list

	List of standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operation list
#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

Table 6-3..... TSF data cryptographic operation list

	List of standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operation list
#1	TTAS.KO-	SEED	128	SA TSF data

	List of standards	Cryptographic algorithm	Cryptographic key sizes	Cryptographic operation list
	12.0004/R1, TTAS.KO-12.0025			
#2	KS X 1213-1, KS X 1213-2	ARIA	256	1) KMS TSF data 2) DCC Console, DCA TSF data 3) KMS Console TSF data 4) SA TSF data 5) It is used for packet encryption with session key
#3	KS X ISO/IEC 18033-2	RSAES	2048	1) It is used for mutual authentication between DCC Console, DCA and SA 2) It is used for mutual authentication between KMS Console, KMS and SA 3) It is used to encrypt the KEK generated by KMS.
#4	ISO/IEC 14888-2,RFC 3447	RSA-PSS	2048	Electronic signature when distributing cryptographic keys
#5	KS X ISO/IEC 9797-2	HMAC_SHA	256	Integrity verification

TSS_CS.1.2 The TOE distributes cryptographic keys in the manner specified in <Table 5-8> when encrypting user data.

TSS_CS.1.3 The TOE distributes cryptographic keys in the manner specified in <Table 5-9, Table 5-10> when mutual authentication and cryptographic communication between the TOE components.

TSS_CS.1.4 Keys used for user data encryption/decryption mentioned in Table 6-2 is immediately destroyed after user data encryption/decryption operation.
Session key mentioned in Table 6-3 is destroyed keys after the end of a trusted session.
For keys used for TSF data encryption/decryption, mutual authentication, digital signature and integrity, are immediately destroyed after completion of the actions in the list of encryption operations in Table 6-3.
Among the TOE components, KMS is changed to "0x00, 0x55 and 0xAA" and the rest except KMS is changed to "0" to destroy the encryption key.

TSS_CS.2 User data protection

Related SFR: FDP_UDE.1 User data encryption

FDP_RIP.1 Subset residual information protection

TSS_CS.2.1 The TOE provides the user with column encryption and column decryption functions.

TSS_CS.2.2 When the user migrates the encryption table to the initial plaintext value table for column encryption, the TOE deletes the initial plaintext value table to protect the information from further use.

6.1.3 Identification and authentication(TSS_IA)

TSS_IA.1 Identification and authentication processing

Related SFR: FIA_UID.1 Timing of identification
FIA_UAU.1 Timing of 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 number of failures (for example, 5). Locked accounts are rejected for identification and authentication requests for a specified period of time (for example, 10 minutes).

TSS_IA.1.2 The TOE performs mutual authentication using the validated cryptographic module CIS-CC v3.3 for each separated TOE component.

TSS_IA.1.3 The DCC Console provides identity and password based identification and authentication functions to verify the identity of an authorized administrator.
KMS Console provides certificate-based identification and authentication function.
KMS does not have an ID and provides identification and authentication via password.
DCC Console and KMS Console provide security management functions only after successful identification and authentication.

TSS_IA.1.5 The DCC Console and the KMS Console change the characters to imitation characters (for example, '*' character) when confidential information is input during identification and authentication.
The TOE does not provide detailed information on the reason for the failure when authentication is failed due to mismatch of the input ID and / or password (for example: Please check your ID or password).

TSS_IA.1.6 The TOE uses a unique ID to prevent reuse of authentication data used for administrator authentication.

TSS_IA.2 User (administrator) attribute definition

Related SFR: FIA_SOS.1 Verification of secrets
FMT_PWD.1(Extended) Management of ID and password

TSS_IA.2.1 TOE verifies if a password meets the requirements specified in <Table 5-14> when the password is being registered. If the password being registered does not meet the specified criteria, the administrator will be forced to enter another password.

TSS_IA.2.2 The TOE allows the authorized user to create a default administrator account (for example, admin) when first connecting to the DCC Console. If the account requested for enrollment does not meet the acceptance criteria, the administrator will be forced to re-enter the account.

TSS_IA.2.3 The password set by the administrator at the first access of the DCC management tool can be changed by the DCC Console by the authorized user.

6.1.4 Security management(TSS_MT)

TSS_MT.1 **Security functional management**

Related SFR: FMT_MOF.1 Management of security functions behaviour
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

TSS_MT.1.1 TOE provides features that allow authorized administrators to manage security functions such as 'Actions to Address Security Violations'. The security function management lists and capabilities are as follows.

- DCC Security Manager
  - ✓ enable about actions to take when the capacity of the log repository reaches a set threshold.
  - ✓ enable, disable about Interworking between SA and KMS
- KMS Security Manager
  - ✓ enable about actions to take when the capacity of the log repository reaches a set threshold.
  - ✓ enable, disable about actions to take in case of authentication failure
- KMS Assistant Security Manager
  - ✓ none
- KMS Local Security Manager
  - ✓ none

TSS_MT.2 **TSF data management**

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 With the TOE, authorized administrators can perform the following TSP data management functions through the console.

- DCC Security Manager
  - ✓ modify about DCC Security Manager password
  - ✓ query, delete about component information
  - ✓ query, modify about DCC Console, DCA, SA audit data storage capacity threshold notification setting
  - ✓ query about DCC Console, DCA, SA log
  - ✓ query, modify, delete about DCC Console access permission IP setting
  - ✓ query, modify about DCC Security Manager's maximum allowable value for inactivity period
  - ✓ query, modify, delete about encryption policy and service
- KMS Security Manager
  - ✓ modify about KMS Security Manager password
  - ✓ query, modify about KMS audit data storage capacity threshold notification setting

- ✓ query about KMS log
- ✓ query, modify about KMS Console access permission IP setting
- ✓ query, modify about KMS Security Manager's maximum allowable value for inactivity period
- ✓ query, modify, delete about encryption policy and service

- KMS Assistant Security Manager
  - ✓ query about KMS audit data storage capacity threshold notification setting
  - ✓ query about KMS log
  - ✓ query about KMS Console access permission IP setting
  - ✓ query about KMS Security Manager's maximum allowable value for inactivity period
  - ✓ query about encryption policy and service
- KMS Local Security Manager
  - ✓ query, delete about KMS Console access permission IP setting
  - ✓ modify about KMS Local Security Manager password

6.1.5 TSF Protection(TSS_PT)

TSS_PT.1 **Integrity verification**

Related SFR: FPT_TST.1 TSF testing

TSS_PT.1.1 TOE provides the integrity verification capabilities needed to guarantee the secure management and integrity of mechanisms that enable security functions. TOE performs integrity verification upon startup, and periodically during operation, to ensure correct functioning of the TOE. Main executable files, and security policy/configuration files are subject to this integrity checks.

- DCC Console executable
- DCA executable
- SA library
- KeyWizard executable
- KMS executable
- KMS Console executable
- SA policy log, access log, KMS interworking configuration file
- DCA configuration file
- KMS service log, system log, administrator log

TSS_PT.2 **Protection of stored TSF data**

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

TSS_PT.2.1 TOE protects important TSF data from unauthorized exposure and tampering, by storing the data after encryption with the CIS-CC v3.3 validated encryption module.

- Important TSF data
  - ✓ SA> data encryption key(Cryptographic key to be used for user data

encryption)

- ✓ SA> KMS interworking configuration file
- ✓ SA> authority setting information of encryption / decryption (Information on setting encryption / decryption permission for user data encryption column)
- ✓ SA> Log threshold email notification SMTP server settings information
- ✓ DCA> DCC Security Manager ID, password information, component information
- ✓ DCA> Configuration file
- ✓ DCA> DCC Console, DCA log
- ✓ DCA> DCC Console, DCA Log threshold email notification SMTP server settings information
- ✓ KMS> Data encryption key(Cryptographic key to be used for user data encryption)s
- ✓ KMS> DB account connection information

TSS_PT.3 Mutual authentication between components and protection of transmission data

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

TSS_PT.3.1 When the authorized administrator accesses SA from the DCC console, TOE will encrypt all transmitted data using the CIS-CC v3.3 validated encryption module, protecting data from tampering or exposure.

6.1.6 TOE Access

TSS_TA.1 Session limitation and termination

Related SFR: FTA_TSE.1 TOE session establishment
FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions
FTA_SSL.5 Management of TSF-initiated sessions

TSS_TA.1.1 The DCC Console limits the number of simultaneously accessible sessions to 1. The KMS management tool restricts the number of simultaneously accessible sessions of the KMS Security Manager to 1 and the number of simultaneously accessible sessions of the KMS Assistant Security Manager to 2. The TOE enforces the identification and authentication procedure even when the connection is through a terminal with an IP address for which access is permitted. If the administrator has already successfully logged in and attempts to log in from another terminal, the existing connection is maintained and the new connection is not allowed.

TSS_TA.1.2 The TOE terminates the session when the authorized administrator who logged in to the DCC management tool or KMS management tool exceeds the inactivity time

- DCC console: The initial value is 10 minutes, and the time can be adjusted from 10 minutes to 60 minutes after login of the console.
- KMS CLI: 5 minutes fixed.
- KMS console:

- KMS Security Manager: The initial value is 10 minutes, and the time can be adjusted from 10 minutes to 60 minutes after login of the console.
- KMS Assistant Security Manager: 10 minutes fixed.