D'Amo v5.0

Security Target

v1.2

The Security Target related to the certified TOE.

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

Penta SECURITY

Revision History

Version	Revision Date	Reason for Revision
1.0	2022.01.12	- First issue
1.1	2023.04.18	- Modification requests reflected
1.2	2023.05.04	- Modification requests reflected and submit to evaluation body

Index

Figure Index

Table Index

1. SECURITY TARGET INTRODUCTION

This document is Penta Security Systems' D'Amo v5.0 Security Target that complies with the **EAL1+** level of the Common Criteria for information protection systems.

1.1. SECURITY TARGET REFERENCES

This ST is identified as follows.

Title	D'Amo v5.0 Security Target
Version	1.2
Evaluation Assurance Level	EAL1+ (ATE_FUN.1 augmented)
Author	Penta Security Systems Inc. Quality Management Division, Quality Team 2
CC Version	CC V3.1 r5
Protection Profile Compliance	Korean National Protection Profile for Database Encryption V1.1
Keyword	Databases, Encryption

[Table 1-1] ST References

1.2. TOE REFERENCES

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

TOE identification		D'Amo v5.0	
TOE detailed version		v5.0.3	
TOE Component	**D'Amo API Agent**	D'Amo API Agent v5.0.2 (install_D'Amo_API_Agent_v5.0.2.zip)	S/W (CD distribution)
	D'Amo Plug-in Agent	D'Amo Plug-in Agent for Tibero v5.0.2 (install_D'Amo_Plug-in_Agent_Tibero_Linux_64_v5.0.2.zip) D'Amo Plug-in Agent for CUBRID v5.0.2 (install_D'Amo_Plug-in_Agent_Cubrid_Linux_64_v5.0.2.zip) D'Amo Plug-in Agent for Oracle v5.0.2 (install_D'Amo_Plug-in_Agent_Oracle_Linux_64_v5.0.2.zip) D'Amo Plug-in Agent for MSSQL v5.0.2 (install_D'Amo_Plug-in_Agent_MSSQL_Windows_x64_v5.0.2.zip)	
	D'Amo KMS	D'Amo KMS v5.0.3 (install_D'Amo_KMS_v5.0.3.nkip, install_kms.sh)	
Manual		D'Amo v5.0 Preparation procedure and user operation manual v1.1(D'Amo API Agent) (D'Amo v5.0 Preparation procedure and user operation manual v1.1(D'Amo API Agent).pdf)	PDF (CD distribution)
		D'Amo v5.0 Preparation procedure and user operation manual	

	v1.1(D'Amo Plug-in Agent) (D'Amo v5.0 Preparation procedure and user operation manual v1.1(D'Amo Plug-in Agent).pdf)	
	D'Amo v5.0 Preparation procedure and user operation manual v1.1(D'Amo KMS) (D'Amo v5.0 Preparation procedure and user operation manual v1.1(D'Amo KMS).pdf)	
Developer	Penta Security Systems Inc.	

[Table 1-2] TOE References

1.3. TOE OVERVIEW

1.3.1. TOE OVERVIEW

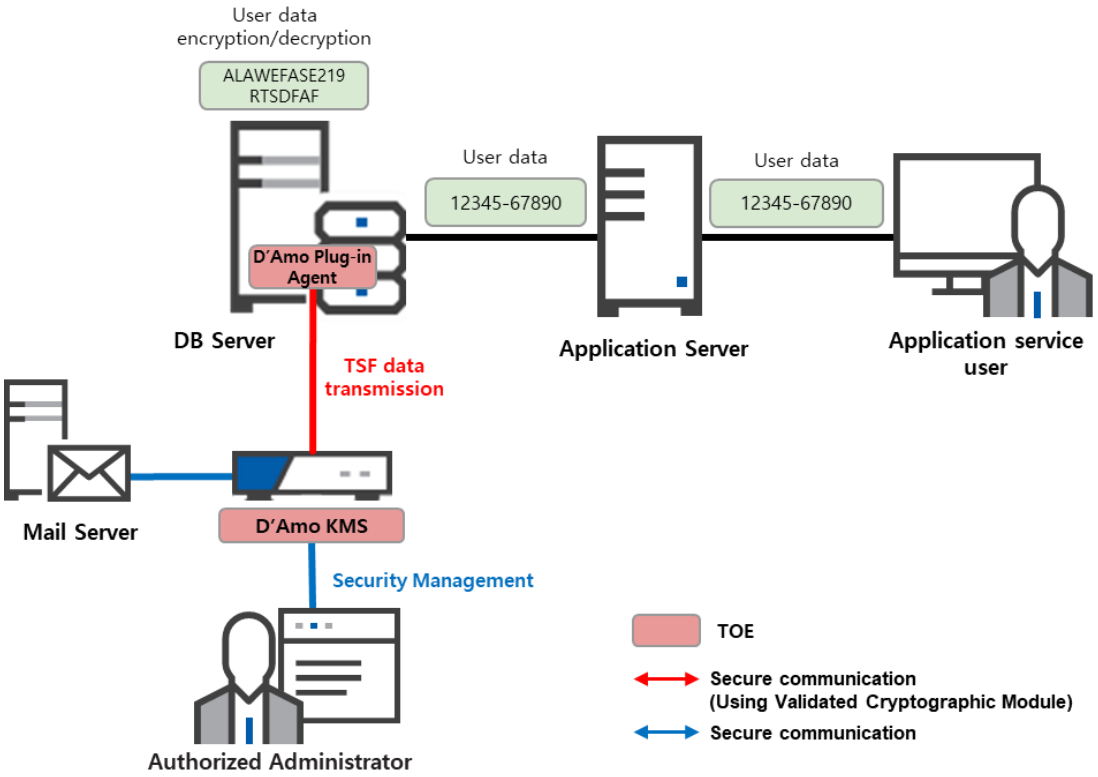
D'Amo v5.0 performs the function of preventing the unauthorized disclosure of confidential information by encrypting the database (hereinafter referred to as "DB").

The encryption target of D'Amo v5.0 is the DB managed by the database management system (hereinafter referred to as "DBMS") in the operational environment of the organization, and the security target defines the user data as all data before/after encrypted and stored in the DB. Part or all of the user data can be the encryption target, depending on the organizational security policies that runs the TOE.

1.3.2. TOE operating environment

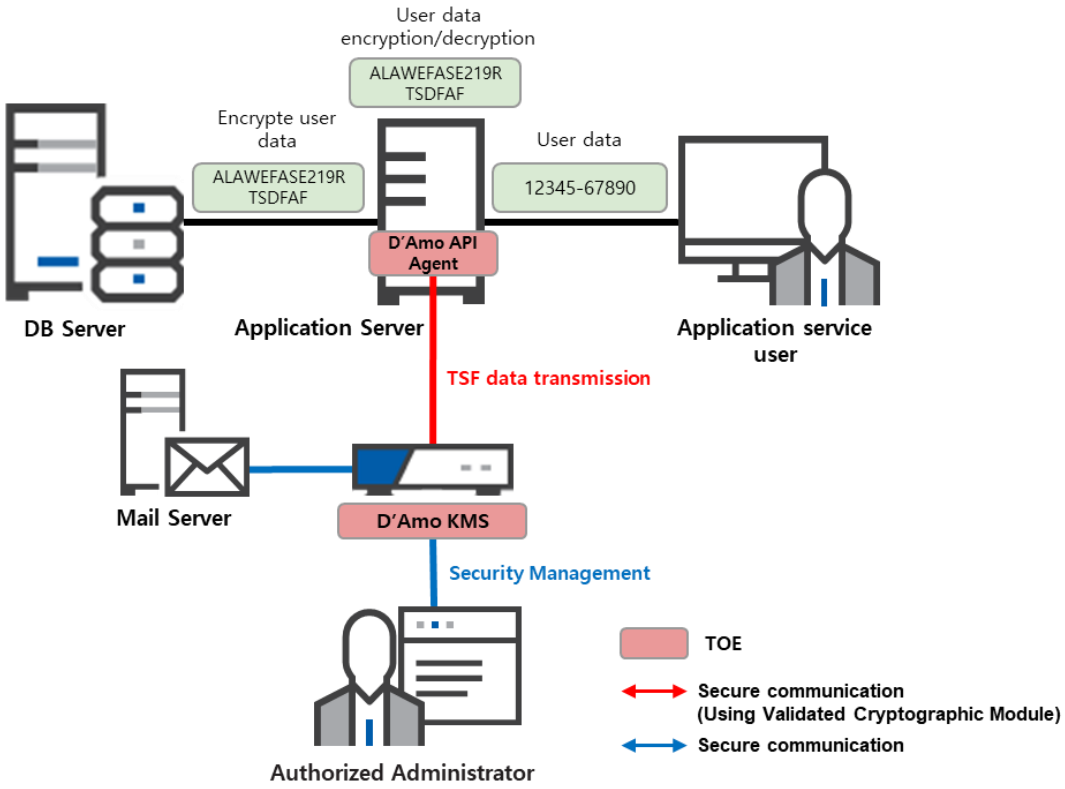
The TOE operational environment can be classified into two: plug-in type and API type.

[Figure 1-1] show the operational environment of the plug-in type. The agent, which is installed in the protected database server of the DB, encrypts the user data of the application server before storing it in the DB according to the policy configured by the authorized administrator, and decrypts the encrypted user data sent from the database server to the application server.



[Figure 1-1] TOE operational environment: Plug-in type (D'Amo Plug-in Agent, D'Amo KMS separate type)

[Figure 1-2] show the operational environment of the API type. The application, which is installed in the application server and provides application services, is developed using the API provided by API module in order to use the cryptographic function of the TOE. D'Amo API Agent is installed in the application server and performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by D'Amo API Agent, which is installed in the application server, and sent to the database server. The encrypted user data received from the database server is decrypted by D'Amo API Agent, which is installed in the application server, and sent to the application service user.



[Figure 1-2] TOE operational environment: API type (D'Amo API Agent, D'Amo KMS separate type)

The communication among the TOE components is based on the encrypted communication using the approved cryptographic algorithm of the validated cryptographic module.

The use of OpenSSL that implements the security protocol is allowed when the authorized administrator accesses D'Amo KMS using the web browser, or the communication among the mail server and D'Amo KMS.

For the plug-in type, the authorized administrator who performs security management on the TOE using D'Amo KMS is identified as the human user of the TOE. The DBMS that manages the DB in the database server and the application which is developed to provide application service in the application server can be the user of the TOE as the external IT entity, if the security function provided by D'Amo Plug-in Agent is used.

For the API type, the authorized administrator who performs security management on the TOE using D'Amo KMS is the human user of the TOE. The application developed to provide application service in the application server becomes the user of the TOE as the external IT entity when the security function provided by D'Amo API Agent is used.

The external IT entity needed to operate the TOE includes email server to send alert mail the authorized administrator.

1.3.3. TOE type and scope

The TOE is provided as software and provide the encryption/decryption function for the user data by each column. The TOE type defined in this ST can be grouped into the 'plug-in type' and 'API type', depending on the TOE operation type. The TOE supports both types. The TOE developed by the plug-in type is composed of the agent(D'Amo API Agent) and management server(D'Amo KMS), and the TOE developed by the API type is composed of the API module(D'Amo API Agent) and management server(D'Amo KMS).

1.3.4. TOE usage and major security features

The TOE is used to encrypt the user data according to the policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information. In order that the authorized administrator can operate the TOE securely in the operational environment of the organization, the TOE provides various security features such as the security audit function that records and manages major auditable events; cryptographic support function such as cryptographic key management to encrypt the user and the TSF data, and cryptographic operation; user data protection function that encrypts the user data and protects the residual information; identification and authentication function such as verifying the identity of the authorized administrator, authentication failure handling, and mutual authentication among the TOE components; security management function for security functions, role definition, and configuration; TSF protection functions including protecting the TSF data transmitted among the TOE components, protecting the TSF data stored in the storage that is controlled by the TSF, and TSF self-test; and TOE access function to manage the access session of the authorized administrator.

1.3.5. Non-TOE required by TOE

The minimum requirements for the operating environment of the TOE are as follows.

			Minimum requirements
D'Amo API Agent	H/W	CPU	Intel-Pentium-Processor-G4600-3M-Cache-3.60 GHz or higher
		RAM	8GB or higher
		HDD	50GB or higher of space required for TOE installation
		NIC	10/100/1000 Mbps x 1EA or higher
	S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-135)
		Java	java 1.8.0
D'Amo Plug-in Agent	H/W	CPU	Intel-Pentium-Processor-G4600-3M-Cache-3.60 GHz or higher
		RAM	8GB or higher
		HDD	50GB or higher of space required for TOE installation
		NIC	10/100/1000 Mbps x 1EA or higher
	S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-135) * Oracle Linux 8.4 64bit (Kernel 5.4.17-2102.201.3.el8uek) ** Windows Server 2019 64bit ***
		DBMS	Tibero 6 CUBRID 10.2 Oracle 19.3

			Minimum requirements
			SQL Server 2019 Enterprise
		Java	java 1.8.0
		remark	* Ubuntu can only install Tibero and CUBRID ** Oracle Linux can only install Oracle *** Windows Server can only install SQL Server
D'Amo KMS	H/W	CPU	Intel® Core™ I3-9100 Processor 3.6 GHz or higher
		RAM	16GB or higher
		HDD	50GB or higher of space required for TOE installation
		NIC	10/100/1000 Mbps x 1EA or higher
	S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-144)
		DBMS	Postgresql 15.1
		3rd Party S/W	OpenSSL 1.1.1t Nginx 1.24.0 Node.js 18.12.1 libwrap0 7.6
Administrator's PC	S/W	Browser	Chrome 108 64bit

[Table 1-3] Minimum H/W and S/W requirements for TOE installation and operation

The 3rd party S/W used in the TOE is as follows.

3rd party S/W	roles
Tibero 6	DBMS service that is the target of database encryption in the Ubuntu environment using the plug-in type
CUBRID 10.2	DBMS service that is the target of database encryption in the Ubuntu environment using the plug-in type
Oracle 19.3	DBMS service that is the target of database encryption in the Oracle Linux environment using the plug-in type
SQL Server 2019 Enterprise	DBMS service that is the target of database encryption in the Windows environment using the plug-in type
Postgresql 15.1	DBMS used to store cryptographic keys and TOE setting value etc. within D'Amo KMS
OpenSSL 1.1.1t	Encryption communication library used when accessing D'Amo KMS from the administrator's PC

3rd party S/W	roles
	Library used by D'Amo KMS to communicate with the mail server
Nginx 1.24.0	A web-based dynamic application server that provides management services using an encrypted SSL secure channel through the management interface of D'Amo KMS
Node.js 18.12.1	JavaScript runtime environment required for D'Amo KMS to operate in Ubuntu environment
libwrap0 7.6	Libraries used by sshd for TCP connections
java 1.8.0	Java runtime environment required for D'Amo Agent to operate in the operating system environment
Chrome 108	Web browser used to access the administrator interface

[Table 1-4] Role of 3rd party S/W used in TOE

Separate external IT entity is needed to operate the TOE. The external IT entity is as follows.

Category	Description
Mail Server	Mail server used by D'Amo KMS to send alert mail

[Table 1-5] The external IT entity

1.4. TOE description

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

1.4.1. Physical scope of the TOE

The physical scope of the TOE is composed of S/W and guidance documents as shown in **[Table** 1-6**]** below.

Category		Identification	TOE Scope	File Format	Distribution Format
TOE identification		D'Amo v5.0			
TOE detailed version		v5.0.3			
TOE Component	D'Amo API Agent	D'Amo API Agent v5.0.2 - install_D'Amo_API_Agent_v5.0.2.zip	O	S/W	CD
	D'Amo Plug-in Agent	D'Amo Plug-in Agent for Tibero v5.0.2 - install_D'Amo_Plug-in_Agent_Tibero_Linux_64_v5.0.2.zip D'Amo Plug-in Agent for CUBRID v5.0.2 - install_D'Amo_Plug-in_Agent_Cubrid_Linux_64_v5.0.2.zip D'Amo Plug-in Agent for Oracle v5.0.2 - install_D'Amo_Plug-in_Agent_Oracle_Linux_64_v5.0.2.zip D'Amo Plug-in Agent for MSSQL v5.0.2 - install_D'Amo_Plug-in_Agent_MSSQL_Windows_x64_v5.0.2.zip	O	S/W	CD
	D'Amo KMS	D'Amo KMS v5.0.3 - install_D'Amo_KMS_v5.0.3.nkip, install_kms.sh	O	S/W	CD
Guidance documents		D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo API Agent) - D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo API Agent).pdf	O	PDF	CD
		D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo Plug-in Agent) - D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo Plug-in Agent).pdf	O		
		D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo KMS) - D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo KMS).pdf	O		
Validated cryptographic module		CIS-CC V4.0	O	S/W	Part of the TOE component

[Table 1-6] The physical scope of the TOE

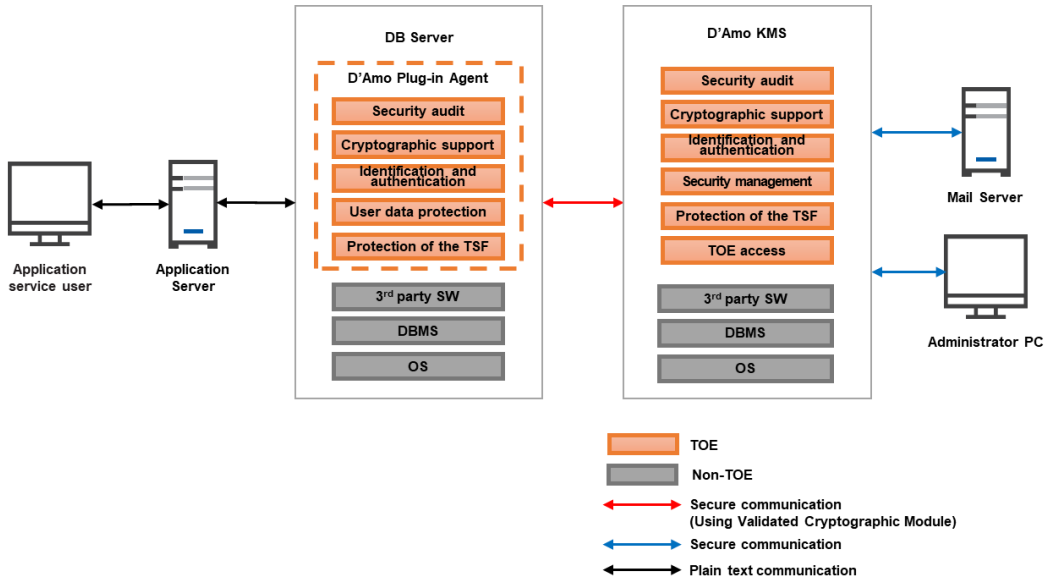
The validated cryptographic modules included in the TOE are as follows.

Category	SubCategory	Contents	TOE used
Validated cryptographic module	cryptographic module name	CIS-CC V4.0	D'Amo KMS D'Amo API Agent D'Amo Plug-in Agent
	Certificate No.	CM-213-2027.10	
	Developer	Penta Security System Inc.	
	Certificate Date.	2022-10-04	

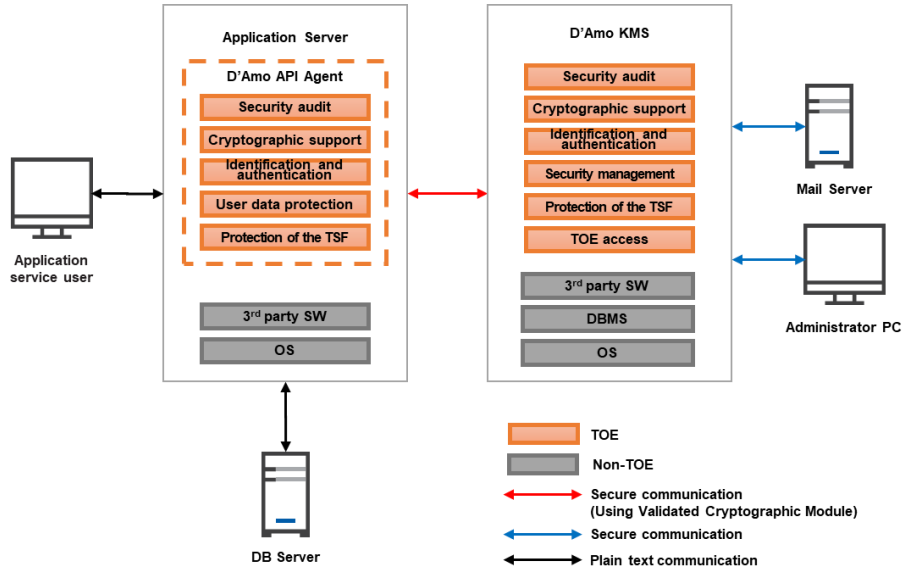
[Table 1-7] Validated cryptographic module

1.4.2. Logical scope of the TOE

The TOE provides security functionality such as **[Security audit, Cryptographic support, User data protection, Identification and authentication, Security management, Protection of the TSF, TOE access]** as shown in **[Figure 1-3], [Figure 1-4]**.



[Figure 1-3] Logical scope of the TOE: Plug-in type (D'Amo Plug-in Agent, D'Amo KMS separate type)



[Figure 1-4] Logical scope of the TOE: API type (D'Amo API Agent, D'Amo KMS separate type)

1.4.2.1. Logical scope of D'Amo Agent

D'Amo Agent is the entity that actually performs encryption/decryption with the encryption policy created by D'Amo KMS. The security function provided through D'Amo Agent are as follows.

Security audit

D'Amo Agent generates audit records during D'Amo Agent operation and sends them to D'Amo KMS to track responsibility for security-related actions.

Cryptographic support

D'Amo Agent performs cryptographic key generation, distribution, and cryptographic operations using the cryptographic algorithm provided by the verified cryptographic module(CIS-CC V4.0). D'Amo Agent generates a session key (D'Amo Agent) used for cryptographic communication with D'Amo KMS using the random number generator of the verified cryptographic module. D'Amo Agent distributes the session key(D'Amo Agent) to D'Amo KMS through the Penta Key Transfer Protocol. D'Amo Agent performs encrypts and digital signing the request message through the Penta Key Transfer Protocol and transmits it to D'Amo KMS. D'Amo Agent decrypts the response message sent from D'Amo KMS using the D'Amo KMS session key distributed from D'Amo KMS through the Penta Key Transfer Protocol and perform encryption/decryption operation or one-way encryption operation on user data using user data encryption key acquired through decryption and digital signature verification. D'Amo Agent destroys all encryption keys by overwriting specific values immediately after encryption/decryption.

Identification and authentication

D'Amo Agent performs mutual authentication based on the Penta Key Transfer Protocol-request/response protocol during encrypted communication with D'Amo KMS. D'Amo KMS performs mutual authentication for D'Amo Agent through verification of the signature value of the Penta Key Transfer Protocol-request message sent from D'Amo Agent.

User data protection

D'Amo Agent provides the ability to encrypt/decrypt user data stored in the DB in column units. And removes the plain text data entered by the application service user so that it does not remain in memory when user data encryption is executed. When user data is encrypted, the same ciphertext is not generated for the same plaintext.

Protection of the TSF

When D'Amo Agent transmits TSF data to D'Amo KMS, it uses the Penta Key Transfer Protocol to safely protect the transmitted TSF data. D'Amo Agent encrypts the request message sent to D'Amo KMS and generates a signature value. D'Amo KMS decrypts the received request message and verifies the signature value. D'Amo Agent ensures its correct operation by performing self-tests on the validated cryptographic module library files and encryption/decryption library files periodically(1 hour) during operation and start-up. And performs integrity verification on major TSF data and execution files (hash value list file for integrity verification, encryption/decryption library, and validated cryptographic module).

1.4.2.2. Logical scope of D'Amo KMS

D'Amo KMS is a key management system that performs key management such as generation, distribution, and destruction of encryption keys. The security features provided through D'Amo KMS are as follows.

Security audit

D'Amo KMS stores audit records generated during the operation of D'Amo KMS and D'Amo Agent to track responsibility for security-related actions.

D'Amo KMS provides the authorized administrator with an interface for reviewing all audit data generated from the TOE. And provides a selective review function according to criteria having a specific logical relationship for stored audit data and a function of sequencing according to time.

D'Amo KMS analyzes potential violations based on the audit records generated by the TOE and takes countermeasures as follows.

- Notifies by e-mail designated by the authorized administrator when an event occurs where the audit trail exceeds a specified threshold or the audit trail is saturated.
- Notifies by e-mail designated by the authorized administrator when integrity violations and self-test failures occur.
- Locks the administrator account for 10 minutes when 5 administrator authentication failures are accumulated.

Cryptographic support

D'Amo KMS uses the cryptographic algorithm provided by the validated cryptographic module(CIS-CC V4.0) to generate and distribute encryption keys and perform cryptographic operations. D'Amo KMS generates user data encryption keys and distributes them to D'Amo Agents through the Penta Key Transfer Protocol. And generates a session key used for cryptographic communication with D'Amo Agent and distributes it to D'Amo Agent through the Penta Key Transfer Protocol. In addition, D'Amo KMS generates an encryption key used to encrypt TSF data and stores it in a DB or file, and uses it for encryption operation. And D'Amo KMS generates KEK2 derived from the password entered when running D'Amo KMS and uses it for cryptographic operation.

D'Amo KMS performs cryptographic operations that generate administrator password hash value, encrypt and decrypt TSF data, digital signature and signature verification during mutual authentication, digital signature and signature verification subject to integrity verification, and generation of hash value subject to integrity verification. And immediately after using all encryption keys, a specific value is overwritten and destroyed.

Identification and authentication

D'Amo KMS requires identification and authentication mechanisms based on ID and password methods for administrators performing security management functions. D'Amo KMS ensures that D'Amo KMS has sufficient security strength by forcing the administrator password acceptance criteria to be met when registering or changing the administrator password. D'Amo KMS masks the authentication data entered by the administrator with specific characters and outputs it, and processes it so that detailed reasons for failure are not provided in case of authentication failure.

D'Amo KMS provides a function to prevent reuse of authentication data through timestamp verification upon administrator login. In addition, if administrator authentication failure reaches 5 times, the administrator

account is locked for 10 minutes.

D'Amo KMS performs mutual authentication based on the Penta Key Transfer Protocol-request/response protocol during encrypted communication with D'Amo Agent. D'Amo Agent performs mutual authentication for D'Amo KMS through verification of the signature value of the Penta Key Transmission Protocol-response message transmitted from D'Amo KMS.

Security management

D'Amo KMS provides security management functions so that authorized administrators can set and manage security functions and TSF data. And the authorized administrator(default administrator) is forced to change the ID and password when accessing D'Amo KMS for the first time. In addition, authorized administrators(added administrators) are forced to change their passwords when accessing D'Amo KMS for the first time.

Protection of the TSF

D'Amo KMS transmits TSF data to D'Amo Agent using the Penta Key Transfer Protocol to safely protect transmitted TSF data. D'Amo KMS encrypts the response message sent to D'Amo Agent and generates a signature value. D'Amo Agent decrypts the received response message and verifies the signature value.

D'Amo KMS conducts self-tests on validated cryptographic modules and key generation/destruction/distribution processes at start-up and periodically(5 minutes) during regular operation to ensure its correct operation. And performs integrity verification on major TSF data and execution files(hash value list file for integrity verification, encryption/decryption library, and validated cryptographic module). In addition, D'Amo KMS protects from unauthorized exposure and modification through encryption of TSF data stored in storage(DBMS and files) controlled by TSF.

D'Amo KMS performs tests on external entities through DBMS and web server availability checks performed at initial start-up and mail server availability checks performed at the request of an authorized administrator.

TOE access

D'Amo KMS maintains the existing connection and blocks new access if the same or another administrator attempts to log in while the administrator is logged in. And allows only manager access sessions requested from terminals with access allowed IP addresses registered in D'Amo KMS.

D'Amo KMS prevents access by unauthorized administrators by forcibly terminating the administrator's session when 10 minutes of administrator inactivity elapse.

1.5. Conventions

The notation, formatting and conventions used in this Security Target 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 Security Target.

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**.

Security Target (ST) Author
This is used to represent the final decision of attributes being made by the ST author. The ST author's operation is denoted in braces, as in {decided by the ST author}. In addition, operations of SFR not completed in the Protection Profile must be completed by the ST author.

1.6. Terms and definitions

Terms used in this ST, which are the same as in the CC, must follow those in the CC.

Agent public key/private key
A key pair issued by D'Amo KMS to work with D'Amo KMS and used for mutual authentication between D'Amo KMS and D'Amo Agent.

Approved cryptographic algorithm
A cryptographic algorithm selected by Korea Cryptographic Module Validation Authority for block cipher, secure hash algorithm, message authentication code, random bit generation, key agreement, public key cipher, digital signatures cryptographic algorithms considering safety, reliability and interoperability

Application Server
The application server defined in this ST refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DBMS to the database server.

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

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

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

Authorized Administrator
Authorized user to securely operate and manage the TOE

Authentication Data
Information used to verify the claimed identity of a user

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

Can/could
The 'can' or 'could' presented in Application notes indicates optional requirements applied to the TOE by ST author's choice

Column
A set of data values of a particular simple type, one for each row of the table in a relational database

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

Class
Set of CC families that share a common focus

Database
A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this ST, refers to the relational database.

Database Server
The database server defined in this ST refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

DBMS (Database Management System)
A software system composed to configure and apply the database. The DBMS related to encryption by

column, which is required by this ST, refers to the database management system based on the relational database model.

Data Encryption Key (DEK)
Key that encrypts and decrypts the data

Decryption
The act that restoring the ciphertext into the plaintext using the decryption key

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

D'Amo KMS
Key management server. An entity that creates and manages symmetric keys, which are user data encryption key, and security policies

D'Amo Agent
A term combining D'Amo API Agent and D'Amo Plug-in Agent that encrypts and decrypts data

Encryption
The act that converts the plaintext into the ciphertext using the encryption key

Element
Indivisible statement of a security need

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

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 components that share a similar goal but differ in emphasis or rigour

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

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

KEK1
Key encryption key that encrypts DB encryption key that encrypts TSF data stored in DB

KEK2
A key derived by entering a password, a key encryption key that encrypts the KMS site private key password encryption key, DB account encryption key, and process configuration file encryption key

KMS Site Public/private key
The key pair generated by D'Amo KMS. Key used for encryptiion/decryption of session key and digital signature, etc.

Management access
The access to the TOE by using the HTTPS, SSH, TLS, etc. to manage the TOE by administrator, remotely

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

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

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

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

Penta Key Transfer Protocol (PKP)
Self-implemented security protocol by Penta Security Systems Inc.

Private Key
A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

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

Public Key
A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm
A cryptographic algorithm that uses a pair of public and private keys

Random bit generator
A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Record IV(Record Initial Vector)
Data of random value used when encrypting the first block when encrypting a block. When the same plaintext is encrypted, different encrypted data is generated each time.

Refinement
Addition of details to a component

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

Secret Key
A cryptographic key which is used in a symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

Security Target (ST)
Implementation-dependent statement of security needs for a specific identified TOE

Security attribute
The characteristics of the subject used to define the SFR, user (including the external IT product), object, information, session and/or resources. These values are used to perform the SFR

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

Self-test
Pre-operational or conditional test executed by the cryptographic module

Session key
A key that encrypts data transmitted between D'Amo Agent and D'Amo KMS.

SSL (Secure Sockets Layer)
This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network

Symmetric cryptographic technique
Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique

Subject
Active entity in the TOE that performs operations on objects

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

TLS (Transport Layer Security)
This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246

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

User
Refer to "External entity"

User Data
Data for the user that does not affect the operation of the TSF

1.7. ST organization

Chapter 1 introduces to the Security Target, providing Security Target references, the TOE references, the TOE overview, the TOE explanation, conventions, terms and definitions, ST organization.

Chapter 2 provides the conformance claims to the CC, PP and package; and describes the claim's conformance rationale and PP conformance statement.

Chapter 3 describes the security objectives for the operational environment.

Chapter 4 defines the extended components for the database encryption.

Chapter 5 describes the security functional and assurance requirements, and security requirements rationale

Chapter 6 describes how the TOE meets each security functional requirements.

2. Conformance claim

2.1. CC conformance claim

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)
Conformance claim	Part 2 Security functional components	Extended: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security assurance components	Conformant
	Package	Augmented: EAL1 augmented (ATE_FUN.1)

2.2. PP conformance clam

This Security Target complies with Korean National Protection Profile for Database Encryption V1.1

2.3. Package conformance claim

This Security Target claims conformance to assurance package EAL1 augmented with ATE_FUN.1.

2.4. Conformance claim rationale

Conformance claim rationale for Korean National Protection Profile for Database Encryption V1.1 that this ST complying are as follows,

Category	ST	Korean National Protection Profile for Database Encryption V1.1
TOE type	Database Encryption - Plug-in type - API type	Database Encryption - Plug-in type - API type

3. Security objectives

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

3.1. Security objectives for the operational environment

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.TIME_STAMP
The operational environment of the TOE must provide reliable time information to the TOE.
OE.SECURE_PATH

In order to protect data from unauthorized modification or exposure when authorized administrators perform security management, a secure channel must be provided between the web browser of the administrator PC and the web server that is the operational environment of D'Amo KMS through TLS communication.

4. Extended components definition

4.1. Cryptographic support

4.1.1. Cryptographic support

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 Random bit generation	1

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 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 TOE Internal mutual authentication	1

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

Management: FIA_IMA.1
There are no management activities foreseen

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

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.
Dependencies No dependencies.

FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: *authentication protocol]* that meets the following [assignment: *list of standards*].

4.3. User data protection

4.3.1. User data encryption

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

Component leveling

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

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

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

4.3.1.1. FDP_UDE.1 User data encryption

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

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

4.4. Security Management

4.4.1. ID and password

Family Behaviour

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

Component leveling

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

Management: FMT_PWD.1

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

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password.

4.4.1.1. FMT_PWD.1 Management of ID and password

Hierarchical to	No other components.
Dependencies	FMT_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 Protection of stored TSF data	1

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 ST, 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) Minimal: Locking or termination of interactive session

4.6.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to	No other components.
Dependencies	[FIA_UAU.1 authentication or 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

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to PP.
The security functional requirements included in this ST are derived from CC Part 2 and Chapter 4 Extended Components Definition.

5.1. Security functional requirements

The following table summarizes the security functional requirements used in this security target.

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
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 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
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(Extended)	TOE Internal mutual authentication

Security functional class	Security functional component	
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)(1)	Management of ID and password (Default administrator)
	FMT_PWD.1(Extended)(2)	Management of ID and password (Additional administrator)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TEE.1	Testing of external entities
	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

[Table 5-1] Security functional requirements

5.1.1. Security audit (FAU)

5.1.1.1. 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 [Notified by e-mail designated by the authorized administrator, Account lockout upon accumulating 5 authentication failures] upon detection of a potential security violation.

5.1.1.2. 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 5-2] Audit events, *no other components*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [Refer to the contents of "additional audit record" in [Table 5-2] Audit events, *no other components*].

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	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	Success and failure of mutual authentication	
FIA_UAU.2	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	All use of the user identification mechanism,	

	including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1(1)(2)	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_TEE.1	External entity test execution and test results	
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 session	
FTA_SSL.5	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism, All attempts at establishment of a user session	

[Table 5-2] Audit event

5.1.1.3. 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.2, integrity violation audit event and selftest failure event of validated cryptographic module among auditable events of FPT_TST.1, [No other components] known to indicate a potential security violation

b) [No other components]

5.1.1.4. FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1: The TSF shall provide [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR.1.2: The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

5.1.1.5. 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 [methods of selection and/or ordering in [Table 5-3]] of audit data based on [criteria with logical relations in [Table 5-3]]

Log type	Criteria with logical relation	methods of selection	methods of ordering
Audit log	Filtering period, Number of filterings	AND	-
	Log level, ID, Client IP	OR	-
	Time	-	Ascending order Descending order
Access log	Filtering period, Number of filterings	AND	-
	Log level, Agent, Result, Error code, Client IP	OR	-
	Time	-	Ascending order Descending order
System log	Filtering period, Number of filterings	AND	-
	Log level	OR	-
	Time	-	Ascending order Descending order

[Table 5-3] Criteria with logical relationships by log type

5.1.1.6. FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

5.1.1.7. 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 [Notified by e-mail designated by the authorized administrator, [No other components]] if the audit trail exceeds [*59% of audit storage capacity*]].

5.1.1.8. FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall *ignore audited events* and [Notified by e-mail designated by the authorized administrator] if the audit trail is full.

5.1.2. Cryptographic support (FCS)

5.1.2.1. 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 [CTR-DRBG, HASH-DRBG] and specified cryptographic key sizes [128, 256, 384, 512bit] that meet the following: [TTAK.KO-12.0189/R1, KS X ISO/IEC 18031, TTAK.KO-12.0331-Part2].

List of standards	Cryptographic key generation algorithm	Cryptographic key sizes
TTAK.KO-12.0189/R1 KS X ISO/IEC 18031	CTR-DRBG	128, 256bit
TTAK.KO-12.0331-Part2	HASH-DRBG	384, 512bit

[Table 5-4] Algorithm and key size that generate the cryptographic key used to encrypt user data

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

Hierarchical to	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [cryptographic key generation algorithm in [Table 5-5]] and specified cryptographic key sizes [cryptographic key sizes in [Table 5-5]] that meet the following: [list of standards in [Table 5-5]].

List of standards	Cryptographic key generation algorithm	Cryptographic key sizes
TTAK.KO-12.0189/R1 KS X ISO/IEC 18031	CTR-DRBG	256bit
KS X ISO/IEC 14888-2	RSA-PSS	2048bit
TTAK.KO-12.0334-Part2	PBKDF	256bit

[Table 5-5] Algorithm and key size that generate the cryptographic key used to encrypt TSF data

5.1.2.3. 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 [Penta Key Transfer Protocol] that meets the following: [No other components].

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

Hierarchical to	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Penta Key Transfer Protocol] that meets the following: [No other components].

5.1.2.5. 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 [key destruction method in [Table 5-6]] that meets the following: [No other components].

Cryptographic key	Cryptographic key destruction method
user data encryption key	0x00 Overwrite
Log key	0x00 Overwrite
DB encryption key	0x00 Overwrite
KEK1	0x00 Overwrite
KMS site key pair	0x00 Overwrite
KMS site private key password encryption key	0xAA, 0x55, 0x00 Overwrite
DB account encryption key	0xAA, 0x55, 0x00 Overwrite

Cryptographic key	Cryptographic key destruction method
Process configuration file encryption key	0xAA, 0x55, 0x00 Overwrite
Session key	D'Amo KMS: 0x00 Overwrite D'Amo Agent: 0xAA, 0x55, 0x00 Overwrite
Agent key pair	0x00 Overwrite
KEK2	0xAA, 0x55, 0x00 Overwrite

[Table 5-6] Cryptographic key destruction list

5.1.2.6. 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 [list of cryptographic operations in [Table 5-7]] in accordance with a specified cryptographic algorithm [cryptographic algorithm in [Table 5-7]] and cryptographic key sizes [cryptographic key sizes in [Table 5-7]] that meet the following: [list of standards in [Table 5-7]].

List of standards	Cryptographic algorithm	Operation mode	Cryptographic key sizes	Cryptographic operations list
KS X 1213-1 KS X 1213-2	ARIA	CBC/CFB	128, 256bit	User data encryption/decryption operations
TTAS.KO-12.0004/R1 KS X ISO/IEC 18033-3	SEED	CBC/CFB	128bit	User data encryption/decryption operations
KS X ISO/IEC 9797-2	HMAC	-	SHA-256, 384, 512	User data one-way encryption operation

[Table 5-7] List of cryptographic operations for cryptographic key used to encrypt user data

5.1.2.7. 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 [list of cryptographic operations in [Table 5-8]] in accordance with a specified cryptographic algorithm [cryptographic algorithm in [Table 5-8]] and cryptographic key sizes [cryptographic key sizes in [Table 5-8]] that meet the following: [list of standards in [Table 5-8]].

List of standards	Cryptographic algorithm	Operation mode	Cryptographic key sizes	Cryptographic operations list
KS X ISO/IEC 10118-3	SHA2	-	256bit	- Generate hash value of administrator password (with SALT) - Generate hash value of integrity verification target list file (checksum.list)
KS X 1213-1 KS X 1213-2	ARIA	CBC	256bit	- DB encryption key: Encrypt the user data encryption key, agent private key, encryption policy, mail setting value, administrator account information, log key and store them in DBMS - KEK1: Encrypt the DB encryption key and store it in DBMS - KMS site private key password encryption key: Encrypt the KMS site private key password and save it to a file - DB account encryption key: Encrypt the D'Amo KMS DB account and save it to a file - process configuration file encryption key: Encrypt the process configuration file and save it to a file - KEK2: Encrypt KMS site private key password encryption key, DB account encryption key of D'Amo KMS and process configuration file encryption key and save them to a file
KS X 1213-1 KS X 1213-2	ARIA	CTR	256bit	- Session key: Encrypt transmission data between D'Amo KMS and D'Amo Agent
KS X ISO/IEC 18033-2	RSAES	-	2048bit	- KMS site public key: Encrypt KEK1 and store it in DBMS - Agent public key, KMS site public key: Session key encryption during communication between D'Amo KMS and D'Amo Agent - Agent private key, KMS site private key: Session key decryption during communication between D'Amo KMS and D'Amo Agent

List of standards	Cryptographic algorithm	Operation mode	Cryptographic key sizes	Cryptographic operations list
KS X ISO/IEC 14888-2	RSA-PSS	-	2048bit	- Agent private key, KMS site private key: electronic signature for mutual authentication, electronic signature subject to integrity verification - Agent public key, KMS site public key: Signature verification during mutual authentication, integrity verification target signature verification
KS X ISO/IEC 9797-2	HMAC	-	SHA-256	- Log key: Generate hash value of audit log for integrity verification

[Table 5-8] List of cryptographic operations for cryptographic key used to encrypt TSF data

5.1.2.8. 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 a cryptographic key using the specified random bit generator that meets the following [TTAK.KO-12.0331-Part2, TTAK.KO-12.0189/R1, KS X ISO/IEC 18031].

5.1.3. User data protection (FDP)

5.1.3.1. 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, [no other components]]

5.1.3.2. 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

5.1.4.1. 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]* unsuccessful authentication attempts occur related to [Administrator Authentication Attempt]
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall [response action of not processing administrator identification and authentication requests for 10 minutes (account lockout)].

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication (Extended)

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_IMA.1.1	The TSF shall perform mutual authentication using [PKP, Penta Key Transfer Protocol] in accordance with [no other components] between [D'Amo Agent and D'Amo KMS].

5.1.4.3. FIA_SOS.1 Verification of secrets

Hierarchical to	No other components.
Dependencies	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [a defined quality metric in [Table 5-9]]

Category		quality metric
Input character	Uppercase letters	A ~ Z, 26 letters
	Lowercase letters	a ~ z, 26 letters
	Number	0 ~ 9, 10 strings
	Special Characters	#?!@$%^&*-,./()=+₩~
Combination rules		- Must contain at least one uppercase letter, lowercase letter, number, and special character - The same character cannot be used more than 3 times in a row - Uppercase/lowercase letters and numbers cannot be used in ascending or descending order more than 3 times in a row.
Minimum length		9 letters(9byte)
Maximum length		15 letters(15byte)

[Table 5-9] Administrator password complexity requirements

5.1.4.4. FIA_UAU.2 User authentication before any action

Hierarchical to	FIA_UAU.1 Timing of authentication

Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each **authorized administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **authorized administrator**.

5.1.4.5. 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 [Authentication mechanism used to authenticate the administrator of D'Amo KMS].

5.1.4.6. 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 [•, authentication failure message] to the user while the authentication is in progress.

5.1.4.7. FIA_UID.2 User identification before any action

Hierarchical to	FIA_UID.1 Timing of identification
Dependencies	No dependencies.
FIA_UID.2.1	The TSF shall require each **authorized administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **authorized administrator**.

5.1.5. Security management (FMT)

5.1.5.1. FMT_MOF.1 Management of security functions behaviour

Hierarchical to	No other components.
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_MOF.1.1	The TSF shall restrict the ability to ***conduct management actions of*** the functions [list of functions in [Table 5-10]] to [authorized administrator].

Authority	Security functions	Management actions			
		determine the behavior	disable	enable	modify the behaviour of
Administrator	Policy-Agent apply	-	O	O	-
	Export agent key	-	-	O	-
	Logout	-	-	O	-
	Mail configuration test	-	-	O	-

[Table 5-10] Management behavior by security functions

5.1.5.2. FMT_MTD.1 Management of TSF data

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*** [list of TSF data in [Table 5-11]] to [authorized administrator].

Authority	TSF data	Management			
		Query	Modify	Delete	Add
Authorized administrator	Symmetric key	O	-	O	O
	Policy management	O	-	O	O
	Agent management	O	-	O	O
	Agent management – Access authority (period)	O	O	-	-
	Agent management – Access authority (IP, account)	O	-	O	O
	Audit/Access/System log	O	-	-	-
	Account(Administrator)	O	-	O	O
	Administrator password	-	O	-	-
	KMS access allowed IP	O	-	O	O
	Administrator e-mail	O	O	-	O
	Mail account	O	O	-	O
	System	O	-	-	-

[Table 5-11] Management behavior by TSF data

5.1.5.3. FMT_PWD.1(1) Management of ID and password(Extended)(Default Administrator)

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 [no other components] to [no other components] 1. [No other components] 2. [No other components]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [no other components] to [no other components]
1. [No other components]
2. [No other components]

FMT_PWD.1.3 The TSF shall provide the capability for *changing the ID and password when the **authorized administrator(default administrator)** accesses for the first time.*

5.1.5.4. FMT_PWD.1(2) Management of ID and password(Extended)(Added Administrator)

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 [no other components] to [no other components]
1. [No other components]
2. [No other components]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [no other components] to [no other components]
1. [No other components]
2. [No other components]

FMT_PWD.1.3 The TSF shall provide the capability for *changing the password when the **authorized administrator(added administrator)** accesses for the first time.*

5.1.5.5. 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 function management list specified in FMT_MOF.1
b) TSF data management list specified in FMT_MTD.1
]

5.1.5.6. 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 [the authorized identified roles in [Table 5-12]].

Role	Authorized role
Authorized administrator	Can use all functions of the D'Amo KMS management screen

[Table 5-12] Security role of authorized administrator

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)

5.1.6.1. 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

5.1.6.2. FPT_TEE.1 Testing of external entities

Hierarchical to No other components.

Dependencies No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *during initial start-up, at the request of an authorised **administrator*** to check the fulfillment of [list of external entities in [Table 5-14]]

External entities list	Selection operation
Mail server availability	at the request of the authorized administrator
Availability of D'Amo KMS DBMS(Postgresql) Availability of D'Amo KMS Web server(nginx)	during initial start-up

[Table 5-13] External entities list

FPT_TEE.1.2 If the test fails, the TSF shall [notified by e-mail designated by the authorized administrator].

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

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PST.1.1 he TSF shall protect [the following TSF data] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

[

Administrator password

User data encryption key

Agent private key

Encryption policy

Mail setting value

Administrator account information

Log key

DB encryption key
KEK1
KMS site private key
KMS site private key password
KMS site private key password encryption key
DB account
DB account encryption key
Process configuration file
Process configuration file encryption key
Audit log
]

5.1.6.4. 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 TSF in [Table 5-14]]*.

TOE components	TSF
D'Amo Agent	Validated cryptographic module, encrypt/decrypt process
D'Amo KMS	Validated cryptographic module, key generation/destruction/distribution process

[Table 5-14] The self tests list of the TSF

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of *[TSF data in [Table 5-15]]*.

TOE components	TSF data
D'Amo Agent	Integrity verification target list file (checksum.list)
D'Amo KMS	Access log, system log, audit log, DB account

[Table 5-15] The integrity verification list of the TSF data

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of *[TSF data in [Table 5-16]]*.

TOE components	TSF
D'Amo Agent	Encryption/decryption library, validated cryptographic module
D'Amo KMS	Key transfer demon, key management demon, validated cryptographic module

[Table 5-16] The integrity verification list of the TSF

5.1.7. TOE access (FTA)

5.1.7.1. 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 {no other components} 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

c) [no other components]

]

FTA_MCS.2.2: The TSF shall enforce a limit of [1] session per administrator by default.

5.1.7.2. 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 [10 minutes].

5.1.7.3. 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

Assurance requirements of this Security Target are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational

Security assurance class	Security assurance component	
		environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 5-17] Security assurance requirements

5.2.1. Security Target evaluation

5.2.1.1. 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 The TOE reference shall uniquely identify the TOE.

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

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

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

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

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

Evaluator action elements

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

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

5.2.1.2. 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.

5.2.1.3. 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.

5.2.1.4. 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.

5.2.1.5. 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.

5.2.1.6. 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 The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

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

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2. Development

5.2.2.1. 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

5.2.3.1. 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.

5.2.3.2. 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_PRE1.1C 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_PRE1.2C 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

5.2.4.1. 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 The 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.

5.2.4.2. 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

5.2.5.1. 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.

5.2.5.2. 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 The TOE shall be suitable for testing.

Evaluator action Elements

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6. Vulnerability assessment

5.2.6.1. 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 The TOE shall be suitable for testing.

Evaluator action elements

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

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

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

5.3. Security requirements rationale

5.3.1. Dependency rationale of security functional requirements

The following table shows dependency of security functional requirements.

No.	Security functional requirements	Dependency
1	FAU_ARP.1	FAU_SAA.1
2	FAU_GEN.1	FPT_STM.1
3	FAU_SAA.1	FAU_GEN.1
4	FAU_SAR.1	FAU_GEN.1
5	FAU_SAR.3	FAU_SAR.1
6	FAU_STG.1	FAU_GEN.1
7	FAU_STG.3	FAU_STG.1
8	FAU_STG.4	FAU_STG.1
9	FCS_CKM.1(1)(2)	[FCS_CKM.2(1)(2) or FCS_COP.1(1)(2)]
		FCS_CKM.4
10	FCS_CKM.2(1)(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)(2)]
		FCS_CKM.4
11	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]
12	FCS_COP.1(1)(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)(2)]
		FCS_CKM.4
13	FCS_RBG.1	-
14	FDP_UDE.1	FCS_COP.1(1)
15	FDP_RIP.1	-
16	FIA_AFL.1	FIA_UAU.1
17	FIA_IMA.1	-
18	FIA_SOS.1	-
19	FIA_UAU.2	FIA_UID.1
20	FIA_UAU.4	-
21	FIA_UAU.7	FIA_UAU.1
22	FIA_UID.2	-
23	FMT_MOF.1	FMT_SMF.1
		FMT_SMR.1
24	FMT_MTD.1	FMT_SMF.1
		FMT_SMR.1
25	FMT_PWD.1(1)(2)	FMT_SMF.1
		FMT_SMR.1
26	FMT_SMF.1	-
27	FMT_SMR.1	FIA_UID.1

28	FPT_ITT.1	-
29	FPT_TEE.1	-
30	FPT_PST.1	-
31	FPT_TST.1	-
32	FTA_MCS.2	FIA_UID.1
33	FTA_SSL.5	FIA_UAU.1
34	FTA_TSE.1	-

[Table 5-18] Rationale for the dependency of the security functional requirements

Rationale (1) : FAU_GEN.1 has the dependency on FAU_STG.1. However, TOE is supported by the operational environment reliable timestamp, the security objective OE.timestamp for the operating environment instead of FPT_STM.1 subordinate relationship is satisfied.

Rationale (2) : FIA_AFL.1, FIA_UAU.7, FTA_SSL.5 has the dependency on FIA_UAU.1, However this is satisfied by FIA_UAU.2, which has a hierarchical relationship with FIA_UAU.1.

Rationale (3) : FIA_UAU.2, FMT_SMR.1, FTA_MCS.2 has the dependency on FIA_UID.1, However this is satisfied by FIA_UID.2, which has a hierarchical relationship with FIA_UID.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 ST since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE summary specification

6.1. Security audit(TSS_AU)

6.1.1. TSS_AU.1 Audit data generation

Related SFR FAU_GEN.1 Audit data generation

Audit data for the start-up and shut-down of the TOE and audit data generated from each TOE component(D'Amo Agent, D'Amo KMS) for audit events in the **[Table 5-2]** are stored as files in the audit data partition(/opt/penta/data2) of D'Amo KMS.

The information to be recorded when creating an audit record is the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. And in the case of audit records for some auditable events, additional audit record contents in the **[Table 5-2]** are included.

6.1.2. TSS_AU.2 Response to security violations

Related SFR FAU_ARP.1 Security alarms

FAU_SAA.1 Potential violation analysis

TSF detects the 'potential security violation event' in the table below and performs 'response actions' for the violation events.

When the D'Amo Agent and D'Amo KMS start up, if the self-test of the validated cryptographic module fails or an integrity verification failure event occurs, the authorized administrator sends a notification to the designated e-mail.

And if an integrity verification failure event of the TOE executable file or configuration file, etc. occurs, the TOE takes response actions to notify the specified e-mail designated by the authorized administrator. In addition, integrity verification is periodically performed on the corresponding files, and when integrity verification fails, it is also notified by an e-mail designated by the authorized administrator. D'Amo Agent performs self-test and integrity verification every hour from successful initialization, and D'Amo KMS performs self-test and integrity verification every 5 minutes on the hour.

If administrator authentication failure audit events occur cumulatively more than 5 times, the account is locked for 10 minutes.

TOE component	Potential security violation event	Response action
D'Amo Agent	Self-test failure of validated cryptographic module	Notified by e-mail designated by the authorized administrator
	Self-test failure of encryption/decryption process	
	Integrity verification failure of the validated cryptographic module	
	Integrity verification failure of other TSF data and executable files	
D'Amo KMS	Self-test failure of validated cryptographic module	Notified by e-mail designated by the authorized administrator
	Self-test failure of key	

TOE component	Potential security violation event	Response action
	generation/destruction/distribution process	
	Integrity verification failure of the validated cryptographic module	
	Integrity verification failure of other TSF data and executable files	
	Administrator authentication failure audit event	Account lockout upon accumulating 5 authentication failures

[Table 6-1] List of security alarm actions

6.1.3. TSS_AU.3 Audit review

Related SFR FAU_SAR.1 Audit review
FAU_SAR.3 Selectable audit review

When an authorized administrator successfully identified and authenticated by the D'Amo KMS, logs in, and reviews the log through the log menu on the management screen, the audit data transmitted to the D'Amo KMS and stored in the partition(/opt/penta/data2) is displayed on the management screen so that all logs(audit log, access log, system log) can be checked.

When an authorized administrator retrieves audit data from the TOE, if conditions are set according to the **[Table 5-3]** for each item in the log, audit data corresponding to the set conditions is output, and the criteria(time) with a specific logical relationship are displayed. They are ordered and searched in ascending or descending order.

6.1.4. TSS_AU.4 Audit data protection and loss response

Related SFR FAU_STG.1 Protected audit trail storage
FAU_STG.3 Action in case of possible audit data loss
FAU_STG.4 Prevention of audit data loss

The audit data of D'Amo KMS is stored as a file in the audit data partition(/opt/penta/data2). At this time, the audit data file is protected from unauthorized modification or deletion because read and write privileges are set only for the root authority, and other users cannot read or write.

The sgkms-apisvr daemon of D'Amo KMS checks the audit data partition(/opt/penta/data2) usage every 5 minutes. If the usage exceeds 59%, audit data loss is predicted, so the D'Amo KMS takes action to notify the e-mail designated by the authorized administrator. When the audit data partition usage exceeds 90% and the audit trail is saturated, D'Amo KMS notifies by e-mail designated by the authorized administrator. And prevents audit data loss by ignoring and not storing the audit data any more. At this time, D'Amo Agent generates audit data and continuously transmits them to D'Amo KMS, but D'Amo KMS does not store them. D'Amo KMS does not generate audit data.

For the usage of the audit data partition, use the use (%) item of the result of checking audit data partition(/opt/penta/data2) with the df command.

6.2. Cryptographic Support(TSS_CS)

6.2.1. TSS_CS.1 Cryptographic key and random bit generation

Related SFR FCS_CKM.1(1) Cryptographic key generation(User data encryption)
FCS_CKM.1(2) Cryptographic key generation(TSF data encryption)
FCS_RBG.1 Random bit generation

D'Amo KMS uses a validated cryptographic module (CIS-CC V4.0) to generate keys for user data encryption and TSF data encryption.

The standard list for generating keys for user data encryption, cryptographic algorithm(random bit generator), encryption key length, encryption key type and purpose of use are as follows.

Standard	Cryptographic algorithm (random bit generator)	Encryption key length	Types of encryption keys and purpose of use
TTAK.KO-12.0189/R1 KS X ISO/IEC 18031	CTR-DRBG	128, 256bit	- User data encryption/decryption operation (ARIA 128/256, SEED 128) - User data one-way encryption operation (HMAC_SHA 256)
TTAK.KO-12.0331-Part2	HASH-DRBG	384, 512bit	- User data one-way encryption operation (HMAC_SHA 384/512)

The standard list for generating keys for TSF data encryption, cryptographic algorithm(random bit generator), encryption key length, encryption key type and purpose of use are as follows.

Standard	Cryptographic algorithm (random bit generator)	Encryption key length	Types of encryption keys and purpose of use
TTAK.KO-12.0189/R1 KS X ISO/IEC 18031	CTR-DRBG	256bit	- Log key: Generate log integrity verification value - DB encryption key: Encrypt the user data encryption key, agent key pair, encryption policy, mail settings, administrator account information, and log key and store them in the DBMS - KEK1: Encrypt the DB encryption key and store it in the DBMS - KMS site private key password encryption key: Encrypt the KMS site private key password and store it in the file - DB account encryption key: Encrypt DB account of D'Amo KMS and store it in the file - Process configuration file encryption key:

Standard	Cryptographic algorithm (random bit generator)	Encryption key length	Types of encryption keys and purpose of use
			Encrypt the process configuration file and store it in the file - Session key: Encrypt transmission data between D'Amo KMS and D'Amo Agent
KS X ISO/IEC 14888-2	RSA-PSS	2048bit	- Agent key pair • D'Amo KMS encrypts the session key with agent public key and transmits it to D'Amo Agent, and D'Amo Agent decrypts the received encrypted session key with agent private key • D'Amo Agent digitally signs the request message with agent private key and sends it to D'Amo KMS, and D'Amo KMS verifies the signature of the received request message with agent public key - KMS site key pair • D'Amo Agent encrypts the session key with the KMS site public key and sends it to D'Amo KMS, and D'Amo KMS decrypts the received encrypted session key with the KMS site private key • D'Amo KMS digitally signs the response message with the KMS site private key and sends it to D'Amo KMS, and D'Amo KMS verifies the signature of the received request message with the KMS site public key
TTAK.KO-12.0334-Part2	PBKDF	256bit	- KEK2 • Encrypt the KMS site private key password encryption key and store it in the file • Encrypt the DB account encryption key of D'Amo KMS and store it in the file • Encrypt the process configuration file encryption key and store it in the file

6.2.2. TSS_CS.2 Cryptographic key distribution

Related SFR 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)

TOE uses the Penta Key Transfer Protocol when distributing encryption keys (session keys) used for mutual authentication and cryptographic communication between TOE components(D'Amo Agent, D'Amo KMS) or distributing user data encryption keys. D'Amo Agent requests the user data encryption key from D'Amo KMS through the request protocol, and upon receiving the request, D'Amo KMS delivers the requested user data encryption key through the response protocol.
In this process, the session key generated by D'Amo Agent and D'Amo KMS is distributed through the request and response protocol of the Penta Key Transfer Protocol, and mutual authentication is performed by verifying the signature value of request message and response message of the other side. The detailed encryption key distribution mechanism is as follows.

Category	Distribution target	Distribution method
Request protocol (D'Amo Agent → D'Amo KMS)	Session key	When D'Amo Agent encrypts the session key generated by D'Amo Agent with the KMS site public key and sends it to D'Amo KMS, D'Amo KMS decrypts it with the KMS site private key and receives the session key.
Response protocol (D'Amo KMS→ D'Amo Agent)	User data encryption key Session key	When D'Amo KMS encrypts the session key generated by D'Amo KMS with Agent public key and sends the response message (user data encryption key and policy) encrypted with session key to D'Amo Agent, D'Amo Agent decrypts the session key encrypted with the agent private key to receive the session key, and decrypts the response message with the session key to receive the user data encryption key

6.2.3. TSS_CS.3 Cryptographic key destruction

Related SFR FCS_CKM.4 Cryptographic key destruction

User data encryption key, log key, DB encryption key, KEK1, KEK2, KMS site key pair, KMS site private key password encryption key, DB account encryption key, process configuration file encryption key, session key, agent key pair are destroyed by overwriting once (0x00) or overwriting three times (0xAA, 0x55, 0x00), and all encryption keys are destroyed immediately after use. The encryption key, time of encryption key destruction, and method of destruction encryption key are as follows.

Encryption key	Time of encryption key destruction	Method of destruction encryption key
User data encryption key	Immediately after user data encryption/decryption	overwrite with 0x00
Log key	Immediately after log XOR encoding/decoding, Immediately after creating integrity verification value of log	overwrite with 0x00

Encryption key	Time of encryption key destruction	Method of destruction encryption key
DB encryption key (Data stored in DB: user data encryption key, agent key pair, encryption policy, mail configuration value, Administrator account information)	Immediately after encryption/decryption of data stored in DBMS	overwrite with 0x00
KEK1	Immediately after DB encryption key encryption/decryption	overwrite with 0x00
KMS site key pair	Immediately after encryption/decryption	overwrite with 0x00
KMS site private key password encryption key	Immediately after KMS site private key password encryption/decryption	overwrite with 0xAA, 0x55, 0x00
DB account encryption key	Immediately after DB account encryption/decryption	overwrite with 0xAA, 0x55, 0x00
Process configuration file encryption key	Immediately after process configuration file encryption/decryption	overwrite with 0xAA, 0x55, 0x00
Session key	Immediately after encryption/decryption	D'Amo KMS: overwrite with 0x00 D'Amo Agent: overwrite with 0xAA, 0x55, 0x00
Agent key pair	Immediately after encryption/decryption	overwrite with 0x00
KEK2	Immediately after encryption/decryption of the keys below • KMS site private key password encryption key • DB account encryption key • process configuration file encryption key	overwrite with 0xAA, 0x55, 0x00

6.2.4. TSS_CS.4 Cryptographic operation(User data)

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

- User data encryption/decryption

D'Amo Agent uses ARIA, a cryptographic algorithm that complies with the standards KS X 1213-1 and KS X 1213-2. The operating mode can be selected from CBC/CFB, and the user data encryption key length can be selected from 128 bits and 256 bits to perform encryption and decryption of user data stored in the DBMS.

In addition, D'Amo Agent uses the cryptographic algorithm SEED that complies with standard TTAS.KO-12.0004/R1 and KS X ISO/IEC 18033-3. The operating mode can be selected from CBC/CFB, and

encryption/decryption operations are performed on user data stored in the DBMS with a 128-bit user data encryption key.

- User data one-way encryption

D'Amo Agent uses the cryptographic algorithm HMAC that complies with standard KS X ISO/IEC 9797-2. The hash function selects among SHA-256, 384, and 512 and performs an encryption operation on user data stored in the DBMS.

6.2.5. TSS_CS.5 Cryptographic operation(TSF data)

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

- Generate hash value of administrator password

D'Amo KMS uses the cryptographic algorithm SHA256(with SALT) that complies with the standard KS X ISO/IEC 10118-3 to generate the hash value of the administrator password and stores it in the DBMS.

- Encryption and decryption of TSF data stored in DBMS

D'Amo KMS encrypts TSF data and stores it in DBMS with a 256-bit DB encryption key generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with standard KS X 1213-1, KS X 1213-2. TSF data encrypted with DB encryption key includes user data encryption key, Agent private key, encryption policy, mail configuration value, administrator account information, and log key.

- Encryption/decryption of DB encryption key

D'Amo KMS encrypts the DB encryption key using the 256-bit KEK1 generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with the standard KS X 1213-1, KS X 1213-2 and stores it in the DBMS.

- Encryption/decryption of DB account

D'Amo KMS encrypts a DB account with a 256-bit DB account encryption key generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with standard KS X 1213-1 and KS X 1213-2 and stores it as a file.

- Encryption and decryption of KMS site private key password

D'Amo KMS encrypts the KMS site private key password with a 256-bit KMS site private key password encryption key generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with standard KS X 1213-1, KS X 1213-2 and stores it as a file.

- Encryption/decryption of process configuration file

D'Amo KMS encrypts the process configuration file with a 256-bit process configuration encryption key generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that

complies with standard KS X 1213-1, KS X 1213-2 and stores it as a file.

- Encryption and decryption of TSF data stored as file

D'Amo KMS encrypts the KMS site private key password encryption key, DB account encryption key, process configuration file encryption key with a 256-bit KEK2 generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with standard KS X 1213-1, KS X 1213-2 and stores it as a file.

- Encryption/decryption of transmitted data

D'Amo Agent encrypts and transmits transmission data(request message) to D'Amo KMS with a 256-bit session key generated by the Record IV method using ARIA(Mode=CTR) which is a cryptographic algorithm that complies with standard KS X 1213-1, KS X 1213-2. And D'Amo KMS decrypts the transmitted data(request message) using the session key.
D'Amo KMS encrypts and transmits transmission data(response message) to D'Amo Agent with a 256-bit session key generated by the Record IV method using ARIA(Mode=CBC) which is a cryptographic algorithm that complies with standard KS X 1213-1, KS X 1213-2. And D'Amo Agent decrypts the transmitted data(response message) using the session key.

- Encryption/decryption of KEK1

TOE encrypts KEK1 with the 2048-bit KMS site public key generated using the cryptographic algorithm RSAES that complies with the standard KS X ISO/IEC 18033-2, stores it in the DBMS, and performs decryption upon inquiry.

- Encryption/decryption of session key

D'Amo Agent encrypts the session key with the 2048-bit KMS site public key using the cryptographic algorithm RSAES that complies with standard KS X ISO/IEC 18033-2 and transmits it to D'Amo KMS. And D'Amo KMS uses the KMS site private key to decrypt the transmitted encrypted session key. D'Amo KMS encrypts the session key with the agent public key of 2048 bits using the cryptographic algorithm RSAES that complies with standard KS X ISO/IEC 18033-2 and transmits it to D'Amo Agent, and D'Amo Agent uses the agent private key to decrypt the transmitted encrypted session key.

- Digital signature and signature verification during mutual authentication

When D'Amo Agent transmits data to D'Amo KMS, the transmission data(request message) is signed with the 2048-bit agent private key generated using the cryptographic algorithm RSA-PSS that complies with the standard KS X ISO/IEC 14888-2. D'Amo KMS verifies the signature of the transmission data(request message) received from the D'Amo Agent with the 2048-bit agent public key generated using the cryptographic algorithm RSA-PSS that complies with the standard KS X ISO/IEC 14888-2.
D'Amo KMS signs the transmission data(response message) with the 2048-bit KMS site private key generated using the cryptographic algorithm RSA-PSS that complies with the standard KS X ISO/IEC 14888-2, when D'Amo KMS transmits data to D'Amo agent. D'Amo Agent verifies the signature of the

transmission data(response message) received from D'Amo KMS with the 2048-bit KMS site public key generated using the cryptographic algorithm RSA-PSS that complies with standard KS X ISO/IEC 14888-2.

- Integrity verification target digital signature and signature verification

When D'Amo Agent is installed, D'Amo Agent digitally signs the integrity verification target list file(checksum.list) with the 2048-bit agent private key generated using the cryptographic algorithm RSA-PSS that complies with the standard KS X ISO/IEC 14888-2 to generate checksum.list.sig file. When verifying integrity, D'Amo Agent verifies the signature of the checksum.list.sig file with the agent public key.

- Generate integrity verification target hash value

D'Amo Agent and D'Amo KMS use cryptographic algorithm SHA256 that complies with the standard KS X ISO/IEC 10118-3 to generate hash values of integrity verification targets and store them in integrity verification target list file(checksum.list). D'Amo Agent and D'Amo KMS generate hash values with the same algorithm when verifying integrity.

D'Amo KMS uses the cryptographic algorithm HMAC(SHA-256) that complies with the standard KS X ISO/IEC 9797-2 to generate integrity verification value of audit log. The encryption key used at this time is the log key.

6.3. User data protection(TSS_DP)

6.3.1. TSS_DP.1 User data protection

Related SFR FDP_UDE.1 User data encryption
FDP_RIP.1 Subset residual information protection

D'Amo Agent provides column-specific encryption for the plain text entered by application service users, and provides a decryption function for user data when queried from DBMS. At this time, since Record IV is used, the same ciphertext is not generated for the same plaintext when user data is encrypted using the same symmetric key.

When D'Amo Agent encrypts the plain text entered by the application service user, it allocates the plain text data entered by the application service user to memory and uses it for encryption. After use, the allocated memory is released so that plain text, which is work residual data, is not left separately in memory, and the information is protected so that it cannot be used any more.

6.4. Identification and authentication(TSS_IA)

6.4.1. TSS_IA.1 Identification and authentication handling

Related SFR FIA_UID.2 User identification before any action
FIA_UAU.2 User authentication before any action
FIA_AFL.1 Authentication failure handling
FIA_UAU.4 Single-use authentication mechanisms
FIA_UAU.7 Protected authentication feedback

D'Amo KMS provides an identification and authentication mechanism based on ID and password methods.

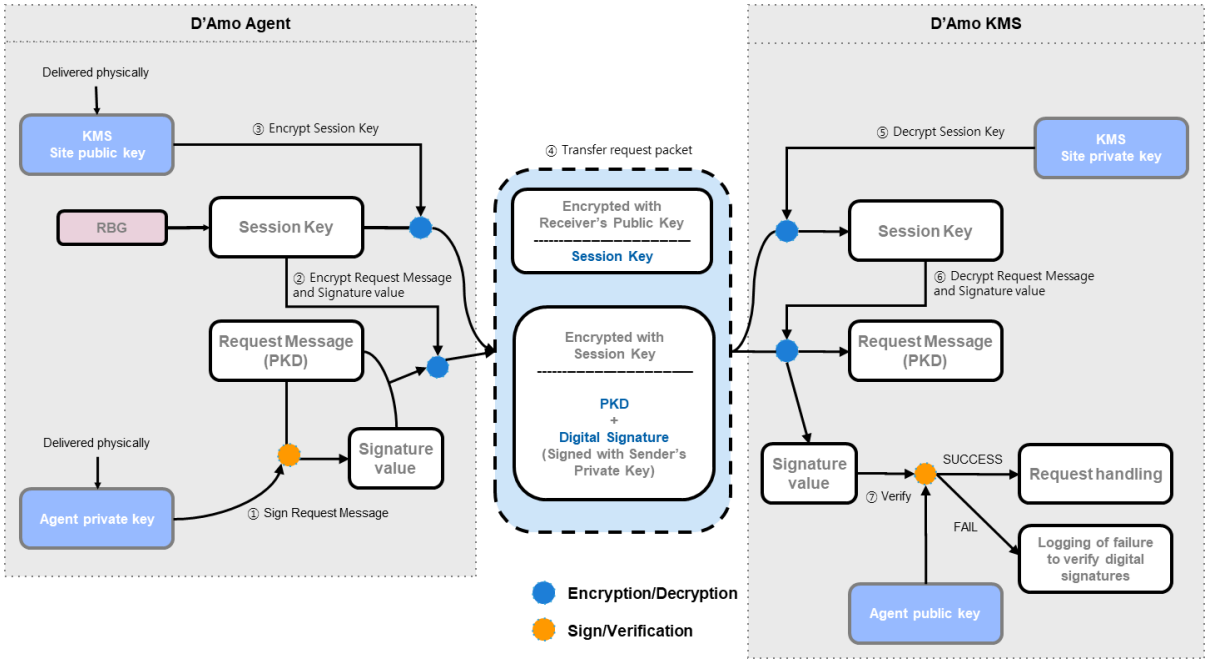
An administrator who has successfully identified and authenticated can access the management screen of D'Amo KMS and perform security management.
D'Amo KMS locks the account when the number of failed administrator authentication attempts reaches the maximum number of failures(5 times). For a locked account, identification and authentication requests are rejected for a specified period of time(10 minutes), and administrator authentication requests are allowed after 10 minutes have elapsed.
When the administrator accesses the D'Amo KMS management screen, if confidential information is entered while identification and authentication are in progress, it is changed to masking characters(•) and output.
D'Amo KMS outputs 'Failed to log in' or 'Connection timed out' when authentication fails, and does not provide detailed information on the reason for the failure. In addition, if authentication fails in D'Amo KMS, login is not possible, so all TSF functions cannot be used.
TOE uses timestamp to prevent re-use of authentication data used for administrator authentication. When an administrator enters and sends a timestamp to the requested packet when logging in, and when a request is received from D'Amo KMS, if there is a difference of more than 3 seconds from the timestamp of D'Amo KMS, it is judged as reused authentication data. handles authentication failures.

6.4.2. TSS_IA.2 TOE Internal(D'Amo Agent and D'Amo KMS) mutual authentication

Related SFR FIA_IMA.1 TOE Internal mutual authentication
FPT_ITT.1 Basic internal TSF data transfer protection

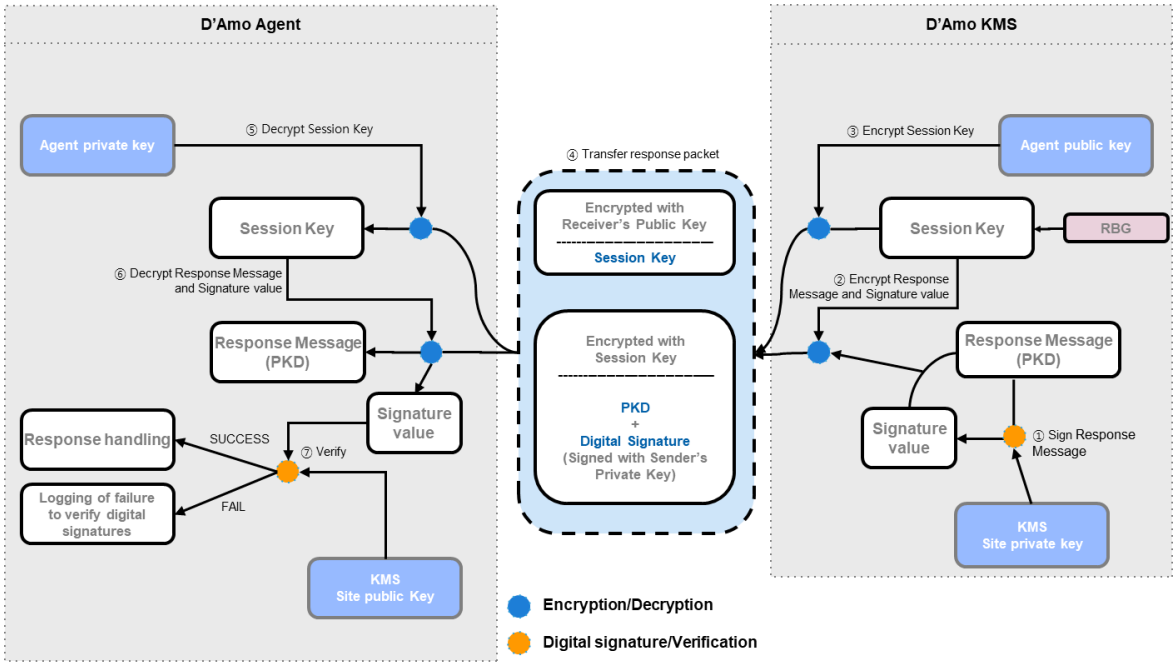
TOE performs mutual authentication for each section between separated TOE components. Mutual authentication between TOE components uses the Penta Key Transfer Protocol. The Penta Key Transfer Protocol is a security protocol implemented by Penta Security Systems, Inc., and is divided into a request protocol and a response protocol.

The mechanism of the Penta Key Transfer Protocol-Request Protocol is as follows. D'Amo Agent encrypts the request message with the session key encrypted with the KMS site public key, signs the request data with the agent private key, and delivers the encrypted request message and signature value to D'Amo KMS. The request message is decrypted with the session key obtained by decrypting the request message with the KMS site private key to obtain the request message, and the signature value is verified with the agent public key. Refer to the figure below for the flow of the request protocol.



[Figure 6-1] Penta Key Transfer Protocol - Request Protocol

The mechanism of the Penta Key Transfer Protocol-response protocol is as follows. D'Amo KMS encrypts the response message with the session key encrypted with the agent public key, signs the response data with the KMS site private key, and delivers the encrypted response message and signature value to D'Amo Agent. D'Amo Agent decrypts the encrypted response message with the agent private key and decrypts it with the acquired session key to obtain the request message and verifies the signature value with the KMS public key. Refer to the figure below for the flow of the response protocol.



[Figure 6-2] Penta Key Transfer Protocol - Response Protocol

6.4.3. TSS_IA.3 Administrator password verification and management

Related SFR FIA_SOS.1 Verification of secrets
FMT_PWD.1(1)(2) Management of ID and password

D'Amo KMS verifies whether the acceptance criteria in the **[Table 5-9]** are satisfied when registering and changing the administrator password. If the password requested for registration and change does not meet the acceptance criteria, the administrator is forced to re-enter the password.

D'Amo KMS forces the default administrator to change the ID and password upon initial access after KMS installation, and forces the added administrator by the default administrator to change the password upon initial login. Both administrators can equally perform all security management functions.

6.5. Security management(TSS_MT)

6.5.1. TSS_MT.1 Management of security functions behaviour

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

Authorized administrators can perform management actions(enable, disable) for the following security functions after going through the identification and authentication process in D'Amo KMS.

- Apply Policy-Agent
- Agent key export
- Log out
- Mail configuration test

6.5.2. TSS_MT.2 Management of TSF data

Related SFR FMT_MTD.1 Management of TSF data
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

The authorized administrator can perform the following TSF data management functions through the TOE management screen.

Authorized administrators can manage(query, modify, delete, add) the following TSF data through the identification and authentication process in D'Amo KMS.

- Symmetric key
- Policy management
- Agent management
- Agent management – Access authority(period)
- Agent management – Access authority(IP, account, path)
- Audit/Access/System log
- Account(administrator)
- Administrator password
- KMS access allowed IP

- Administrator e-mail
- Mail account
- System

6.6. TSF protection(TSS_PT)

6.6.1. TSS_PT.1 integrity verification

Related SFR FPT_TST.1 TSF testing

TOE provides an integrity verification function to ensure the integrity of the mechanisms constituting the security functions and the safety of security management. When installing D'Amo Agent, D'Amo Agent generates hash values of the validated cryptographic module library and encryption/decryption library among the installation files using the SHA256 cryptographic algorithm and records them in the checksum.list file. And copies the checksumList.sig file, which is the signature value generated by digitally signing with each agent private key, to the installation path. D'Amo Agent performs integrity verification by verifying the signature of checksum.list with the agent public key at start-up or periodic intervals(1 hour) during operation. And The hash value of the validated cryptographic module library and encryption/decryption library in the checksum.list file in D'Amo Agent is generated using the SHA256 cryptographic algorithm, and verified by comparing with checksum.list.

When installing D'Amo KMS, the hash values of the validated cryptographic module library, DB account, key transmission daemon, and key management daemon among the installation files are generated using the SHA256 cryptographic algorithm and recorded in the checksum.list file. And the checksum.list file is protected by digital signature with the KMS site private key.

In the checksum.list file, there is a hash value generated using the sha-256 cryptographic algorithm of the validated cryptographic module library, DB account, key transmission daemon, and key management daemon. At start-up or periodically(5 minutes) during operation, the hash value of the integrity verification target list file in the contents of the checksum.list file is generated and verified by comparing with the hash value in the previously stored checksum.list.

D'Amo KMS generates HMAC-SHA256 hash values for each log using the log key when audit logs, system logs, and access logs of D'Amo KMS are recorded, and stores them together with the logs. When integrity verification is performed, the hash value created as the log key using HMAC-SHA256 for the stored log is compared with the stored value. D'Amo KMS performs integrity verification every 5 minutes on the hour.

6.6.2. TSS_PT.2 Self-test

Related SFR FPT_TST.1 TSF testing

D'Amo Agent performs self-test on the installed validated cryptographic module and encryption/decryption process at start-up or periodically(1 hour) during operation. The self-test of the validated cryptographic module calls the built-in self-test function to check the result. For the self-test of encryption/decryption process, a specific plaintext is encrypted using the sample key generated for self-test and then decrypted again. At this time, it is checked whether the obtained plaintext value is output the same as the plaintext entered before encryption, and if it is the same, the self-test is successful, and if not, the self-test is failed.

D'Amo KMS performs self-test on the installed validated cryptographic module and key

generation/destruction/distribution process at start-up or periodically (5 minutes) during operation. The self-test of the validated cryptographic module calls the built-in self-test function to check the result. In the key generation process, encryption and decryption are performed by generating random bit using the random bit generator of the validated cryptographic module. In this process, it is checked whether it is possible to acquire the user data encryption key, DB encryption key, and log key. Also, it is checked the status of the sgkms-apisvr daemon, which generation and destruction of keys, and the sgkms-keysvr daemon, which distributes keys. If all of these items are normal, the self-test succeeds, and if any one of them has a problem, the self-test fails.

6.6.3. TSS_PT.3 Protection of stored TSF data

Related SFR FPT_PST.1 Basic protection of stored TSF data

TSF data required for D'Amo KMS operation is stored in the operating environment, DBMS(Postgresql) or as a file. Important TSF data is encrypted and stored with a validated cryptographic module to protect it from unauthorized exposure and change.

Here, KEK1 is the KEK that encrypts the DB encryption key. KEK2 is a KEK that encrypts the KMS site private key password encryption key, DB account encryption key, and process configuration file encryption key.

TSF data	Protection mechanism
Administrator password	Store hash value generated with SHA256 (with SALT) in DBMS
User data encryption key	• Encrypted with DB encryption key (ARIA 256bit + CBC) and stored in DBMS • It is encrypted with the DB encryption key, loaded into memory, and decrypted the moment user data is encrypted.
Agent private key	• It is encrypted with the DB encryption key (ARIA 256bit + CBC) and stored in the DBMS. • It is encrypted with the DB encryption key and loaded into memory, and is decrypted in plain text when encrypted with the agent public key or decrypted with the agent private key.
Encryption policy	• It is encrypted with the DB encryption key (ARIA 256bit + CBC) and stored in the DBMS. • It is encrypted with the DB encryption key and loaded into memory, and is decrypted in plain text when user data is encrypted or viewed on the management screen.
Mail configuration value	• It is encrypted with the DB encryption key (ARIA 256bit + CBC) and stored in the DBMS. • It is encrypted with the DB encryption key and loaded into memory, and is decrypted in plain text when D'Amo KMS sends e-mail or inquires from the management screen.
Administrator account information	• It is encrypted with the DB encryption key (ARIA 256bit + CBC) and stored in the DBMS. • It is encrypted with the DB encryption key and loaded into the

TSF data	Protection mechanism
	memory, and is decrypted in plain text when the administrator account information is retrieved from the management screen.
Log key	• It is encrypted with the DB encryption key (ARIA 256bit + CBC) and stored in the DBMS. • It is encrypted with the DB encryption key and loaded into memory, and is decrypted as plain text at the time of generating the log integrity verification value.
DB encryption key	• It is encrypted with KEK1 (ARIA 256bit + CBC) and stored in DBMS. • It is encrypted with KEK1 and loaded into memory, and is decrypted as plain text at the moment of encryption/decryption of TSF data stored in DBMS.
KEK1	• It is encrypted with the KMS site public key (RSAES 2048bit - SHA256) and stored in the DBMS. • It is encrypted with the KMS site public key and loaded into the memory, and is decrypted in plain text at the moment the DB encryption key is encrypted and decrypted.
KMS site private key	• When KMS is installed, it is encrypted using the password entered in the process of generating the KMS site key pair using the PKCS#5 method, and then saved as a file.
KMS site private key password	• It is encrypted (ARIA 256bit + CBC) with the KMS site private key password encryption key and stored in a file. • It is encrypted with the KMS site private key password encryption key and loaded into memory, and is decrypted in plain text at the moment of encryption/decryption of the KMS site private key password.
KMS site private key password encryption key	• It is encrypted with KEK2 (ARIA 256bit + CBC) and stored in a file. • It is encrypted with KEK2 and loaded into memory, and is decrypted in plain text at the moment of encrypting and decrypting the KMS site private key password.
DB account	• It is encrypted (ARIA 256bit + CBC) with the DB account encryption key and saved as a file. • Encrypted with the DB account encryption key, loaded into memory, and decrypted as plain text the moment you connect to the DBMS
DB account encryption key	• It is encrypted with KEK2 (ARIA 256bit + CBC) and stored in DBMS. • It is encrypted with KEK2 and loaded into memory, and is decrypted in plain text at the moment of encrypting and

TSF data	Protection mechanism
	decrypting the DB account.
Process configuration file	• It is encrypted (ARIA 256bit + CBC) with the process configuration file encryption key and stored in the file. • It is encrypted with the process setting file encryption key and loaded into memory, and is decrypted in plain text at the moment of encryption/decryption of the process setting file.
Process configuration file encryption key	• It is encrypted with KEK2 (ARIA 256bit + CBC) and stored in a file. • It is encrypted with KEK2 and loaded into memory, and is decrypted in plain text at the moment of encrypting and decrypting the process setting file.
Audit log	• It is encoded with the Internally Implemented encoding technique and stored in a file. • The integrity verification value of the audit log is generated(HMAC-SHA256) and stored.

[Table 6-2] TSF data protection

6.6.4. TSS_PT.4 Testing of external entities

Related SFR FPT_TEE.1 Testing of external entities

D'Amo KMS executes availability tests of the mail server, DBMS(Postgresql) of D'Amo KMS, and web server(nginx) of D'Amo KMS, which are external entities, and performs specific countermeasures.

D'Amo KMS determines the availability of the mail server by sending a test mail to the mail server when requested by the administrator, and displays the result on the management screen.

D'Amo KMS executes a command to check the DBMS status of D'Amo KMS at initial start-up, determines whether the DBMS of D'Amo KMS is available, and displays the result on the screen. If the test fails, an alert mail is sent to the authorized administrator.

D'Amo KMS executes a command to check the status of the web server of D'Amo KMS at initial start-up, determines whether the web server of D'Amo KMS is available, and displays the result on the screen. If the test fails, an alert mail is sent to the authorized administrator.

6.7. TOE access(TSS_TA)

6.7.1. TSS_TA.1 Limiting the number of sessions and terminating sessions

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

D'Amo KMS limits the number of authorized administrator sessions that can be connected simultaneously to one. If an administrator is already logged in to D'Amo KMS and the same or another administrator attempts to log in, the existing connection is maintained and the new connection is blocked.

D'Amo KMS allows identification and authentication only for terminals with IP addresses that are allowed to access. And rejects identification and authentication attempts requested from terminals other than those with access permitted IP addresses registered in D'Amo KMS. Up to 2 access IPs can be registered.
D'Amo KMS forcibly terminates the administrator session and displays the login screen if the inactivity time is more than 10 minutes after successful administrator login.