Spiceware DBE v2.0
Security Target v1.4

Spiceware Co., Ltd.

https://spiceware.io

The Security Target related to the certified TOE.
This Security Target is written in Korean and translated from Korean into English.

Revision history

Version	Date	Content
1.0	2022.01.14	Draft
1.1	2022.03.22	Correction by observation report
1.2	2022.05.23	Correction by observation report
1.3	2022.07.28	TOE component version update
1.4	2022.08.24	Correction of Term definitions

Contents

List of Table

List of Figures

1. Security Target Introduction

This document is the Spiceware DBE V2.0 Security Target of Spiceware Co., Ltd. which targets the Common Criteria EAL1+ level.

1.1. Security Target Reference

This Security Target is identified as follows :

Classification	Description
Title	Spiceware DBE v2.0 Security Target
Version	v1.4
Author	Spiceware Co., Ltd.
Publication Date	August 24, 2022
Common Criteria Version	CC V3.1 r5
Evaluation Assurance Level	EAL1+ (ATE_FUN.1)

1.2. TOE Reference

The TOE that complies with this Security Target is identified as follows :

<table>
<tr><th>Classification</th><th colspan="3">Description</th></tr>
<tr><td>TOE</td><td colspan="3">Spiceware DBE v2.0</td></tr>
<tr><td>TOE Detail Version</td><td colspan="3">v2.0.5</td></tr>
<tr><td rowspan="3">TOE Components</td><td>spice.ssm</td><td>spice.ssm-2.0.1
(spice.ssm-2.0.1.tar.gz)</td><td rowspan="4">CD Distribution</td></tr>
<tr><td>spice.cc</td><td>spice.cc-2.0.3
(spice.cc-2.0.3.tar.gz)</td></tr>
<tr><td>spice.mgs</td><td>spice.mgs-2.0.1
(spice.mgs-2.0.1.tar.gz)</td></tr>
<tr><td>Guidance Document</td><td colspan="2">Spiceware DBE v2.0 Operational User Guidance v1.4
(Spiceware DBE v2.0-Operational User Guidance_v1.4.pdf)
Spiceware DBE v2.0 API Guide v1.0
(Spiceware DBE v2.0-API Guide_v1.0.pdf)</td></tr>
<tr><td>Developer</td><td colspan="3">Spiceware Co., Ltd.</td></tr>
</table>

1.3. TOE overview

Spiceware DBE v2.0 (hereinafter referred to as "TOE") performs the function of preventing the unauthorized disclosure of confidential information by encrypting the database (hereinafter referred to as "DB").

The encryption target of the TOE 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 (hereinafter referred to as "ST") 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.

The DBMS that controls the DB in the operational environment of the organization is different from the DBMS that is directly used by the TOE to control the TSF data (security policy, audit data, etc.).

1.3.1. TOE type and scope

The TOE is provided as software and shall provide the encryption/decryption function for the user data by each column. The TOE type defined in this ST can be grouped into the 'API type', depending on the TOE operation type.

The TOE consists of spice.ssm, spice.cc and spice.mgs. spice.ssm(API module) is installed in the Application Server and performs encryption/decryption of the user data according to the policy set by the authorized administrator. This document uses the same term as 'agent'. spice.cc is installed on the Management Server and supports functions such as identification and authentication of administrators and encryption policy setting as a security management interface.
spice.mgs is Installed on the Management Server, it carries out encrypted communication with spice.ssm. It transfers the encryption policy, etc. to spice.ssm, and collects the status information of spice.ssm and audit data generated by spice.ssm.

1.3.2. 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 the TOE access function to manage the access session of the authorized administrator. In addition, the TOE provides the trusted path/channel function that provides cryptographic communication between the TOE and authorized administrator.

The DEK (Data Encryption Key) used to encrypt/decrypt the user data is protected by encryption with the KEK (Key Encryption Key).

1.3.3. TOE operational environment

Figure 1-1 shows the operational environment of the API type provided by the TOE. 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. The API module 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 the API module, 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 the API module, which is installed in the application server, and sent to the application service user.

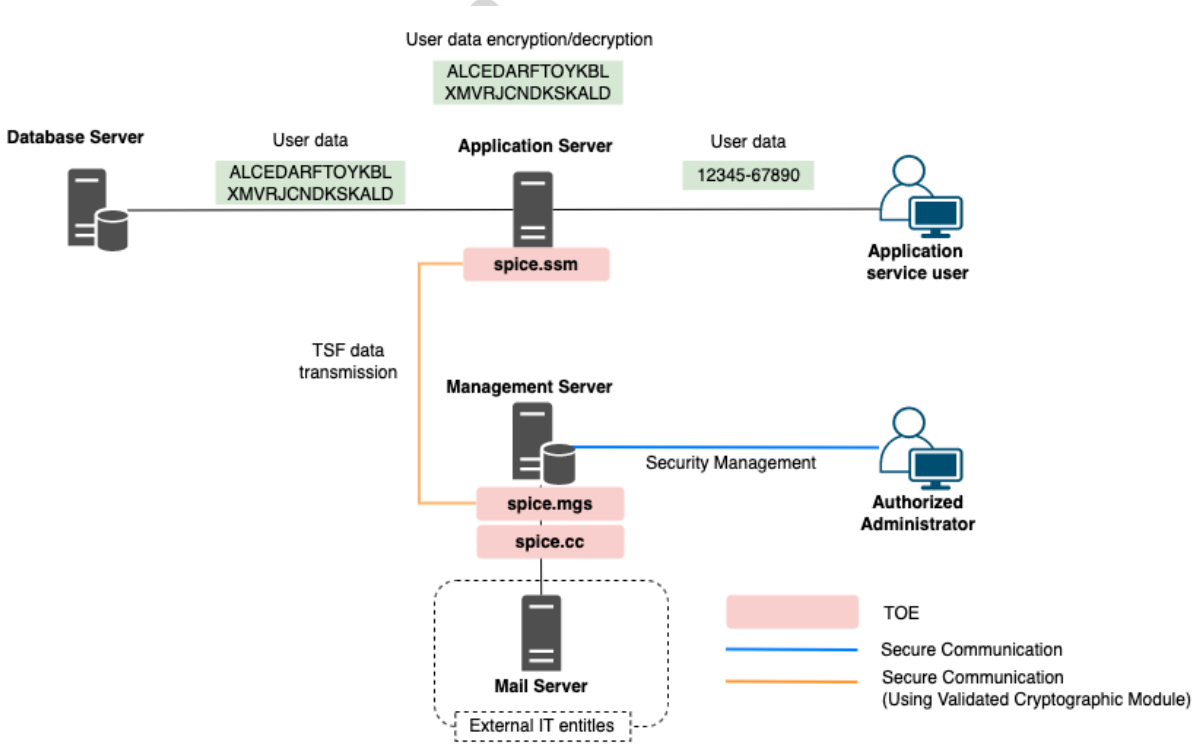


Figure 1-1. API-type operational environment (API module, management server separate type)

The authorized administrator can encrypt/decrypt the user data through the management server according to the scope of the encryption required by the organizational security policy. In addition, the authorized

administrator can perform security management through access to spice.cc. The policy set by the authorized administrator is sent to the API module (spice.ssm) through spice.mgs. The management server is installed physically separated from the Application Server where the API module is installed.

The communication among the TOE components(spice.mgs, spice.ssm) shall be based on the encrypted communication using the approved cryptographic algorithm of the validated cryptographic module.
When the administrator accesses the management server through a web browser, the security protocol(TLS v1.2) used.

the authorized administrator who performs security management on the TOE using the management server is the human user of the TOE. The application developed to provide application service in the application server is the user of the TOE as the external IT entity when the security function provided by the API module is used.

1.3.4. Non-TOE hardware, software Identification

The TOE consists of spice.ssm, spice.cc and spice.mgs. The TOE is provided as software. spice.ssm is installed in the Application Server, spice.cc, spice.mgs is installed in the Management Server. The minimum specifications for hardware and software required for the TOE installation and operation are as follows.

Table 1-1. Minimum specifications for H/W and S/W required for TOE installation and operation

Classification			Minimum Specification
Application Server	H/W	CPU	Intel Core i5 CPU @2.7 GHz or higher
		RAM	16 GB or higher
		HDD	Space required for TOE Installation is 30 GB or higher
		NIC	10/100/1000 1port or higher
	S/W	OS	Ubuntu 16.04 (64bit, Kernel 4.17)
		Mandatory S/W	Amazon corretto 8.342.07.3
Management Server	H/W	CPU	Intel Core i5 CPU @2.7 GHz or higher
		RAM	32 GB or higher
		HDD	Space required for TOE Installation is 30 GB or higher
		NIC	10/100/1000 1port or higher
	S/W	OS	Ubuntu 16.04 (64bit, Kernel 4.17)
		Mandatory S/W	Tomcat 9.0.65 Amazon corretto 8.342.07.3 MySQL 5.7.38 Elasticsearch 7.13.4

Non-TOE software that is not within the scope of the TOE but is necessary for TOE operation performs the following roles.

Table 1-2. Non-TOE software roles for TOE operation

Classification		Description
Application Server	Amazon corretto 8.342.07.3	JAVA runtime environment for the TOE operation
Management Server	Tomcat 9.0.65	Providing the security management interface
	Amazon corretto 8.342.07.3	JAVA runtime environment for the TOE operation
	MySQL 5.7.38	Storing configuration values and audit data of the TOE
	Elasticsearch 7.13.4	Storing audit data of the TOE

administrator PC

The minimum specifications for hardware and software required for authorized administrator's PC are as follows.

Table 1-3. Required for authorized administrator's PC

Classification			Minimum Specification
administrator PC	S/W	Web Browser	Chrome 97.0 (64bit)
		OTP generator	Authenticator 6.3.3 (by authenticator.cc)

External IT Entity

External IT entities required for the operation of the TOE are as follows.

Table 1-4. External IT Entity

Classification	Description
Mail Server	Mail Server for sending mail to the authorized administrators.

1.4. TOE Description

The TOE Description describes the physical and logical ranges of the TOE.

1.4.1. Physical scope of the TOE

The Physical scope of the TOE shown in Table 1-5 below. The TOE is provided as software. The TOE consists of spice.ssm, spice.cc and spice.mgs. Guidance Document is provided to the administrator for the secure management of the TOE.

The hardware, software and OS on which the TOE is installed are not included in the scope of the TOE.

Table 1-5. Physical scope of the TOE

Classification	Contents		Type	Distribution
TOE Components	spice.ssm	spice.ssm-2.0.1 (spice.ssm-2.0.1.tar.gz)	S/W	CD
	spice.cc	spice.cc-2.0.3 (spice.cc-2.0.3.tar.gz)	S/W	
	spice.mgs	spice.mgs-2.0.1 (spice.mgs-2.0.1.tar.gz)	S/W	
Guidance Document	Spiceware DBE v2.0 Operational User Guidance v1.4 (Spiceware DBE v2.0-Operational User Guidance_v1.4.pdf) Spiceware DBE v2.0 API Guide v1.0 (Spiceware DBE v2.0-API Guide_v1.0.pdf)			

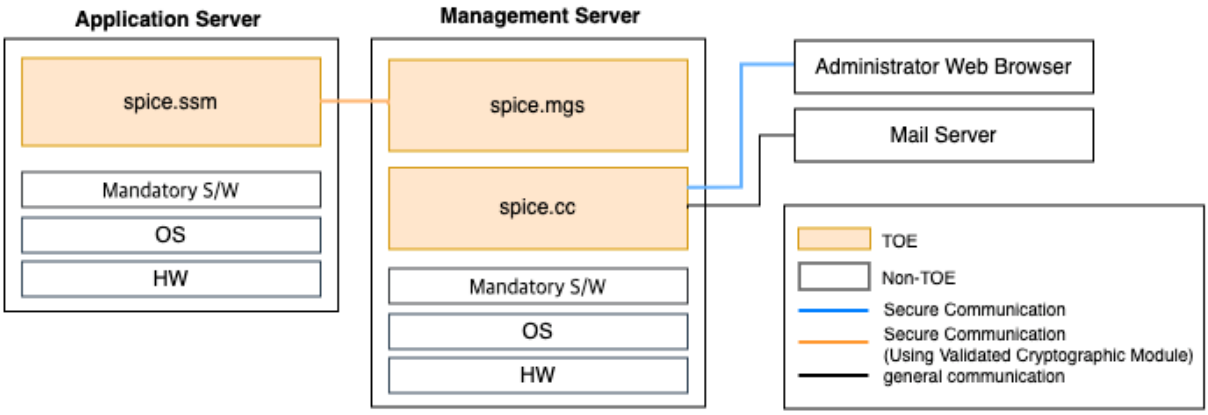


Figure 1-2. Physical scope of the TOE

The validated cryptographic module used at the TOE are as follows.

Table 1-6. Validated cryptographic module

Classification	Contents
Crypto Module Name	AhnLab Cryptographic Module V1.0

Verification Number	CM-152-2024.4
Developer	AhnLab, Inc.
Verification Date	April 19 2019

1.4.2. Logical scope of the TOE

The security functions included in the logical scope of the TOE are as follows.

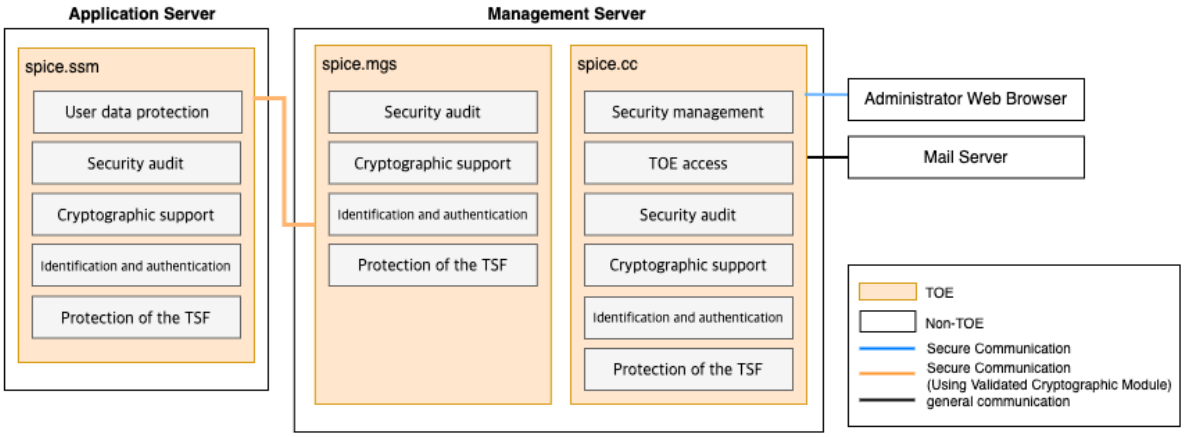


Figure 1-3. Logical scope of the TOE

1.4.2.1. spice.ssm

■ Security Audit

spice.ssm generates and manages the event date and time, event type, subject identification, outcome of the event, and event contents of the auditable events as audit data. spice.ssm sends audit data to spice.mgs.

■ Cryptographic Support

spice.ssm uses the approved cryptographic algorithm of the validated cryptographic module 'AhnLab Cryptographic Module V1.0' to encrypt/decrypt user data and protect data transmitted between TOE components.

spice.ssm performs cryptographic key generation, destruction and cryptographic operation to perform user data encryption/decryption. spice.ssm performs cryptographic key generation, destruction, distribution, and cryptographic operation to protect data transmitted to spice.mgs.

■ User data protection

spice.ssm encrypts/decrypts the user data for each DB column according to the encryption policy set by the authorized administrator. After encryption/decryption, the original user data is immediately deleted, and all

previous information contents are not available.

- Identification and Authentication

spice.ssm carries out mutual authentication through the internally implemented authentication protocol for secure communication with spice.mgs.

- Protection of the TSF

spice.ssm performs encrypted communication and verifies message integrity to protect the TSF data for communication with spice.mgs. spice.ssm performs self-tests the validated cryptographic module at initial startup, and performs self-tests at regular intervals during normal operation.

1.4.2.2. spice.mgs

- Security Audit

spice.mgs generates and manages the event date and time, event type, subject identification, outcome of the event, and event contents of the auditable events as audit data. spice.mgs collects the audit data generated by spice.ssm.

- Cryptographic Support

spice.mgs uses the approved cryptographic algorithm of the validated cryptographic module 'AhnLab Cryptographic Module V1.0' to protect the data transmitted to spice.ssm.
spice.mgs performs cryptographic key generation, destruction, distribution, and cryptographic operation to protect data transmitted to spice.ssm.

- Identification and Authentication

spice.mgs carries out mutual authentication through the internally implemented authentication protocol for secure communication with spice.ssm.

- Protection of the TSF

spice.mgs performs encrypted communication and verifies message integrity to protect the TSF data for communication with spice.mgs. spice.mgs performs self-tests the validated cryptographic module at initial startup, and performs self-tests at regular intervals during normal operation.

1.4.2.3. spice.cc

- Security Audit

spice.cc generates and manages the event date and time, event type, subject identification, outcome of the

event, and event contents of the auditable events as audit data. Only the authorized administrators can review the generated audit data through spice.cc, and it is detected as a potential security violation and an email is sent to the authorized administrator.

The authorized administrators can search and review about the audit data through spice.cc. Search results of audit data is sorted in descending order according to the date and time of generation. When the threshold of audit data storage (80%) exceeds, spice.cc overwrites the oldest audit data, and sends an email to the authorized administrator.

- Cryptographic Support

spice.cc uses the approved cryptographic algorithm of the validated cryptographic module 'AhnLab Cryptographic Module V1.0' to protect TSF data.

spice.cc performs cryptographic key generation, destruction and cryptographic operation to protect TSF data.

- Identification and Authentication

spice.cc provides identification and authentication functions to administrators who perform security management functions. The administrator's password is created and changed when the passwords combination rules are satisfied. When the administrator enters authentication data, it is masked. When identification and authentication failure, the TOE does not provide feedback on the cause of failure. When the maximum allowed number of authentication failures is reached, the administrator account status is changed to the account locked status.

spice.cc provides a function to block attempts to reuse authentication information for the administrators.

- Security Management

spice.cc can be accessed through the web browser (HTTPS protocol based on TLS v1.2), and only administrators who have successfully identified and authenticated through secure communication can perform security management functions of spice.cc.

spice.cc provides security management functions such as security policy management and administrator management to the authorized administrators. The TOE sets the administrator's ID and password during the installation process. Administrators perform security roles according to authority.

- Protection of the TSF

To check whether the TOE operates normally, spice.cc performs self-tests on main processes of the TOE and the validated cryptographic module at initial startup, and performs self-tests at regular intervals during normal operation. spice.cc performs integrity tests on TSF data and TSF executable files during initial startup, and periodically performs integrity tests during normal operation.

- TOE Access

spice.cc allows up to 1 concurrent session of the same administrator account or an administrator account with

the same authorities. The new administrator's access is blocked if the maximum concurrent sessions exceed. The session is forcibly terminated if the authorized administrator exceeds the allowed time for inactivity (600 seconds) after management access. The management access is blocked when accessing with an IP other than the access IP address set by the authorized administrator.

1.5. Conventions

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

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

Iteration

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

Assignment

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

Selection

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

Refinement

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

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.

"Application notes" is provided to clarify the intent of requirements, provide the information for the optional items in implementation, and define "Pass/Fail" criteria for a requirement. The application notes is provided with corresponding requirements if necessary.

1.6. Terms and definitions

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

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 DB to the database server.

Approved mode of operation

The mode of cryptographic module using approved cryptographic algorithm

Assets

Entities that the owner of the TOE presumably places value upon

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

Critical Security Parameters (CSP)

Information related to security that can erode the security of the encryption module if exposed or changed (e.g., verification data such as secret key/private key, password, or Personal Identification Number).

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

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

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

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

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.

Recommend/be recommended

The 'recommend' or 'be recommended' presented in Application notes is not mandatorily recommended, but required to be applied for secure operations of the TOE

Refinement

Addition of details to a component

Role

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

Security Function Policy (SFP)

A Set of rules that describes the specific security action performed by TSF (TOE security functionality) and describe them as SFR (security function requirement)

Secret Key

A cryptographic key which is used in an 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

Security Token

Hardware device that implements key generation and electronic signature generation inside the device to save/store confidential information safely.

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

Shall/must

The 'shall' or 'must' presented in Application notes indicates mandatory requirements applied to the TOE

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

Threat Agent

Entity that can adversely act on assets

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

Master

One of the administrators authorized to operate and manage a TOE safely, who has privileges such as query, modify, delete, encryption target system addition, administrator access IP addition/modify/delete, administrator account management, self-information management.

Viewer

One of the administrators authorized to operate and manage a TOE safely, who has privileges such as Query, administrator access IP addition/modify/delete, self-information management.

spice.ssm

spice.ssm(API module) is installed in the Application Server and performs encryption/decryption of the user data according to the policy set by the authorized administrator. This document uses the same term as 'agent'.

spice.cc

spice.cc is installed on the Management Server and supports functions such as identification and authentication of administrators and encryption policy setting as a security management interface.

spice.mgs

spice.mgs is Installed on the Management Server, it carries out encrypted communication with spice.ssm. It transfers the encryption policy, etc. to spice.ssm, and collects the status information of spice.ssm and audit data generated by spice.ssm.

1.7. ST organization

Chapter 1 introduces to the ST, providing ST references and the TOE overview.

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.

Chapter 6 describes the TOE summary specification.

2. Conformance claim

This describe how the ST conforms to the CC, PPs and packages.

2.1. CC conformance claim

This ST complies with the following CC.

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 claim

This Security Targe complied with the "Korean National Protection Profile for Database Encryption V1.1(2019.12.11)"

2.3. Package conformance claim

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

2.4. Conformance claim rationale

This ST declares "strict PP conformance" with 'the Korean National PP for Database Encryption V1.1'.

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_RE- INFORCEMENT

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 TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operation environment.

OE.AUDIT_DATA_PROTECT

The DBMS interacting with the TOE shall be managed safely and protected from unauthorized deletion or modification.

OE.TRUSTED_PATH

When an authorized administrator accesses the TOE using the web browser of the administrator's PC, a secure path must be ensured.

4. Extended components definition

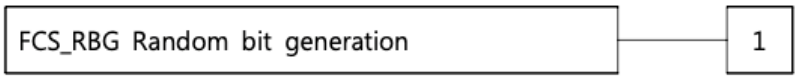
4.1. Cryptographic support (FCS)

4.1.1. Random Bit Generation

Family Behaviour

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

Component leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

4.1.1.1. FCS_RBG.1 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*].

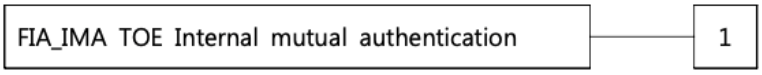
4.2. Identification & authentication (FIA)

4.2.1. TOE Internal mutual authentication

Family Behaviour

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

Component leveling



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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

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

a) Minimal: Success and failure of mutual authentication

b) Minimal: Modification of authentication protocol

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to	No other components.
Dependencies	No dependencies.

FIA_IMA.1 The TSF shall perform mutual authentication between [assignment: *different parts of TOE*] using the [assignment: *authentication protocol*] that meets the following [assignment: *list of standards*].

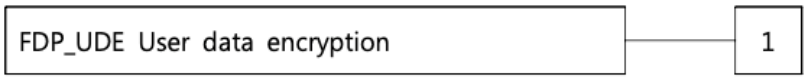
4.3. User data protection (FDP)

4.3.1. User data protection

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

4.4. Security Management (FMT)

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 (FPT)

4.5.1. Protection of stored TSF data

Family Behaviour

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

Component leveling

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

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

4.5.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to	No other components.
Dependencies	No dependencies.

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

4.6. TOE Access (FTA)

4.6.1. Session locking and termination

Family Behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking,

unlocking, and termination of interactive sessions.

Component leveling

In CC Part 2, the session locking and termination family consists of four components. In this PP, it consists of five components by extending one additional component as follows.
※ The relevant description for four components contained in CC Part 2 is omitted.

FTA_SSL.5 The management of TSF-initiated sessions, provides requirements that the TSF locks or terminates the session after a specified time interval of user inactivity.

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

Audit: FTA_SSL.5
The following actions are recommended to record if FAU_GEN Security audit data generation is included in the PP/ST:
a) 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 this ST.

5.1. Security Functional Requirements

The security functional requirements included in this ST are derived from CC Part 2 and Chapter 4 Extended Components Definition.

The following table summarizes the security functional requirements used in the ST.

Table 5-1. Security functional requirements

Security functional class	Security functional component		Remarks
Security audit (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.3	Protected audit trail storage	
	FAU_STG.4	Action in case of possible audit data loss	
Cryptographic support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)	Iteration
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)	Iteration
	FCS_CKM.2	Cryptographic key distribution	
	FCS_CKM.4	Cryptographic key destruction	
	FCS_COP.1(1)	Cryptographic operation (User data encryption)	Iteration
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)	Iteration
	FCS_RBG.1	Random bit generation	Extended
User data protection (FDP)	FDP_UDE.1	User data encryption	Extended
	FDP_RIP.1	Subset residual information protection	
Identification and authentication (FIA)	FIA_AFL.1	Authentication failure handling	
	FIA_IMA.1	TOE Internal mutual authentication	Extended
	FIA_SOS.1	Verification of secrets	
	FIA_UAU.2	Timing of authentication	
	FIA_UAU.4	Single-use authentication mechanisms	
	FIA_UAU.7	Protected authentication feedback	

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

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 [generate an alert log, sending an email to the authorized administrator] 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, *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, *no other components*].

Table 5-2. Audit event

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 Modify of authentication protocol	
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	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

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.1, integrity violation audit event and selftest failure event of validated cryptographic module among auditable events of FPT_TST.1, [None]] known to indicate a potential security violation

b) [None]

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 [the 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] of audit data based on [Table 5-3].

Table 5-3. Audit Review Selection Criteria

Audit data type	Selection criteria by type	Methods of selection and/or ordering
Processing history	■ Search period : Select (year, month) ■ Search conditions : Select (IP, UNIT), keywords	■ Search ■ Sort by date in descending order
Error history	■ Search period : Select (year, month)	■ Search ■ Sort by date in descending order
Audit log	■ Search period : Select (year, month, day) ■ Search conditions : Select (User, UserIP, Action, Result), keywords	■ Search ■ Sort by date in descending order
Alert log	■ Search period : Select (year, month, day) ■ Search conditions : Select (User, UserIP, Action, Result), keywords	■ Search ■ Sort by date in descending order

5.1.1.6. FAU_STG.3 Action in case of possible audit data loss

Hierarchical to No other components.

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [Notification to the authorized administrator, [None] if the audit trail exceeds [threshold(80%) of audit storage]].

5.1.1.7. 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 *overwrite the oldest stored audit records* and [send an email to 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 [cryptographic key generation algorithm of Table 5-4] and specified cryptographic key sizes [cryptographic key sizes of Table 5-4] that meet the following: [standard list of Table 5-4].

Table 5-4. Cryptographic key generation algorithm list (User data encryption)

Classification	Standards	Cryptographic key generation algorithm	Cryptographic key sizes
Generate cryptographic Key for User Data (DEK)	ISO/IEC 18031 NIST SP 800-90A R1	HASH_DRBG	256 bit

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 of Table 5-5] and specified cryptographic key sizes [cryptographic key sizes of Table 5-5] that meet the following: [standard list of Table 5-5].

Table 5-5. Cryptographic key generation algorithm list (TSF data encryption)

Classification	Standards	Cryptographic key generation algorithm	Cryptographic key sizes
Generate Cryptographic Key for	TTAS.KO-12.0334	PBKDF2(SHA-256)	256 bit

DEK (KEK generation)			
Generate Cryptographic Key for communication between the TOE components	ISO/IEC 1803 NIST SP 800-90A R1	HASH_DRBG	256 bit
Generate Cryptographic Key for TSF data	ISO/IEC 1803 NIST SP 800-90A R1	SHA-256	256 bit

5.1.2.3. FCS_CKM.2 Cryptographic key distribution(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_CKM.2.1: The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [cryptographic key destruction algorithm of Table 5-6] that meets the following: [standard list of Table 5-6].

Table 5-6. Cryptographic key destruction algorithm list

Classification	Standards	Cryptographic key destruction algorithm	Cryptographic key sizes
Distribute Cryptographic Key for communication between the TOE components	ISO/IEC 11770-3	DH	256 bit

5.1.2.4. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1: The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite with '0x00'] that meets the following: [None].

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

Table 5-7. Cryptographic operation list

Standards	Cryptographic algorithm	Cryptographic key sizes	Use
KS X 1213-1	ARIA	265 bit	User data encryption/decryption (Operation mode : CBC)

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

Table 5-8. Cryptographic operation list

Standards	Cryptographic algorithm	Cryptographic key sizes	Use
KS X 1213-1	ARIA	265 bit	DEK encryption/decryption

			(Operation mode : CBC)
KS X 1213-1	ARIA	256 bit	Encrypted communication between the TOE components - Encryption/decryption (Operation mode : CBC)
ISO/IEC 10118-3	SHA	256 bit	Encrypted communication between the TOE components - Integrity verification
KS X 1213-1	ARIA	256 bit	TSF data encryption/decryption (Operation mode : CBC)

5.1.2.7. 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 [ISO/IEC 18031, NIST SP 800-90A R1].

5.1.3. User data protection (FDP)

5.1.3.1. FDP_UDE.1 User data encryption

Hierarchical to No other components.

Dependencies FCS_COP.1 Cryptographic operation

FDP_UDE.1 The TSF shall provide a function that can encrypt/decrypt the user data to the TOE user according to the specified [encryption/decryption method by column, [None]].

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 (FIA)

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 attempts].

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

[

a) Master : Account locked for 5 minutes

b) Viewer : Account locked for 5 minutes or locked within 5 minutes until account unlocked by Master administrator

]

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.

Dependencies No dependencies.

FIA_IMA.1 The TSF shall perform mutual authentication using [the Internally Implemented Authentication Protocol] in accordance with [None] between [spice.mgs, spice.ssm].

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 [the acceptance criteria defined below].

[

a) Allowable characters : Available characters are as follows - Uppercase and lowercase letters (a-z, A-Z: 52 characters), numbers (0-9: 10 characters), and special characters (20 characters: ! @ # $ % ^ & * ( ) _ + - = ~ : ; . / |). Including these, there are a total of 82 characters.

b) Combination rules : Combination of four types of letters among English uppercase

and lowercase letters, special characters, and numbers

c) Min/Max Length: 9 to 20 characters

]

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 [password authentication method].

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 [the following list of feedback] to the user while the authentication is in progress.

[

a) Password : When entering the password, masking ("●") characters are displayed on the screen.

b) In case of identification and authentication failures, the feedback for the cause of failure is not provided.

]

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)

Table 5-9. Security management action and management type by component

Security functional component	Management function	Management type
FAU_ARP.1	Management of actions (addition, removal, modification) to be taken	Management of security functions
FAU_SAA.1	Maintenance of the rules (addition, removal and modification of the rules in the rule group)	Management of security functions
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records	Management of security roles
FAU_STG.3	Maintenance of the threshold	Management of TSF data threshold
	Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure	Management of security functions
FAU_STG.4	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	Management of security functions
FDP_UDE.1	Management of the user data encryption/decryption rules	Management of security attributes
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Management of TSF data threshold
	Management of actions to be taken in the event of an authentication failure	Management of security functions
FIA_IMA.1	Management of the authentication protocol for mutual authentication	Management of security functions
FIA_SOS.1	Management of the metric used to verify the secrets	Management of TSF data
FIA_UAU.2	management of the authentication data by an administrator management of the authentication data by the user associated with this data.	Management of TSF data
FIA_UID.2	the management of the user identities	Management of TSF data

FMT_MOF.1	Management of the group of roles that can interact with the functions in the TSF	Management of security roles
FMT_MTD.1	Management of the group of roles that can interact with the TSF data	Management of security roles
FMT_PWD.1	Management of ID and password configuration rules	Management of security functions
FMT_SMR.1	Management of the group of users that are part of a role.	Management of security roles
FPT_ITT.1	Management of the types of modification against which the TSF should protect Management of the mechanism used to provide the protection of the data in transit between different parts of the TSF	Management of security functions
FPT_TST.1	Management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions Management of the time interval if appropriate	Management of TSF data
FTA_MCS.2	Management of the maximum allowed number of concurrent user sessions by an administrator	Management of TSF data threshold
FTA_SSL.5	Specification of the time of user inactivity after which lock-out occurs for an individual user Specification of the default time of user inactivity after which lock-out occurs	Management of TSF data
FTA_TSE.1	Management of the session establishment conditions by the authorized administrator	Management of TSF data

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 [Security function list of Table 5-10] to [the authorized administrator].

Table 5-10. List of Security functions

Authority	Security Function	Management action			
		determine the behavior	disable	enable	modify the behaviour of
Master	Encryption target system Management	O	O	O	O
	User data encryption policy Management	O	O	O	O
	Agent Management	O	O	O	O
	administrator account Management	O	-	-	O
	administrator access IP Management	O	-	-	O
	Self-Information Management	O	-	-	O
Viewer	administrator access IP Management	O	-	-	O
	Self-Information Management	O	-	-	O

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

Table 5-11. List of TSF data

Authority	TSF data	manage		
		query	modify	delete
Master	Encryption target system information	O	O	-
	User data encryption policy	O	O	O
	Agent configuration information	O	O	O
	Audit data	O	-	-
	Administrator account information	O	O	O
	administrator access IP information	O	O	-
	Self-Information	O	O	-

Viewer	Encryption target system information	O	-	-
	User data encryption policy	O	-	-
	Agent configuration information	O	-	-
	Audit data	O	-	-
	administrator access IP information	O	O	-
	Self-Information	O	O	-

5.1.5.3. 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 [None] to [None].

1. [None]

2. [None]

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

1. [None]

2. [None]

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

5.1.5.4. 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: [list of management functions to be provided by the TSF].

[

a) Security function management : Management functions specified in FMT_MOF.1

b) TSF data management : Management functions specified in FMT_MTD.1

]

5.1.5.5. 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 administrator roles of Table 5-12].

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

Table 5-12. Authorized Administrator's Role

Authority	Role
Master	Query, modify, delete, encryption target system addition, administrator access IP addition/modify/delete, administrator account management, self-information management
Viewer	Query, administrator access IP addition/modify/delete, self-information management

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_PST.1 Basic protection of stored TSF data

Hierarchical to No other components.

Dependencies No dependencies.

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

5.1.6.3. 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*.

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

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity 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 { 1 } 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) [None]

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

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 [time interval of the administrator inactivity : 600sec].

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 Protection Profile are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following table summarizes assurance components.

Table 5-13. Security assurance requirements

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 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

5.2.1. Security Target evaluation

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

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

Evaluator action elements

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

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

5.2.4. Life-cycle support

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.

Table 5-14. Rationale for the dependency of the security functional requirements

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale(1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	Rationale(2)
7	FAU_STG.4	FAU_STG.1	Rationale(2)
8	FCS_CKM.1(1)	[FCS_CKM.2 또는 FCS_COP.1] FCS_CKM.4	10, 12 11
9	FCS_CKM.1(2)	[FCS_CKM.2 또는 FCS_COP.1] FCS_CKM.4	10, 13 11
10	FCS_CKM.2	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	9 11
11	FCS_CKM.4	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1]	8, 9
12	FCS_COP.1(1)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	8 11
13	FCS_COP.1(2)	[FDP_ITC.1 또는 FDP_ITC.2 또는 FCS_CKM.1] FCS_CKM.4	9 11
14	FCS_RBG.1	-	-
15	FDP_UDE.1	FCS_COP.1	12
16	FDP_RIP.1	-	-
17	FIA_AFL.1	FIA_UAU.1	20 Rationale(3)
18	FIA_IMA.1	-	-
19	FIA_SOS.1	-	-
20	FIA_UAU.2	FIA_UID.1	23 Rationale(4)
21	FIA_UAU.4	-	-

22	FIA_UAU.7	FIA_UAU.1	20 Rationale(3)
23	FIA_UID.2	-	-
24	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	27 28
25	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	27 28
26	FMT_PWD.1	FMT_SMF.1 FMT_SMR.1	27 28
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23 Rationale(4)
29	FPT_ITT.1	-	-
30	FPT_PST.1	-	-
31	FPT_TST.1	-	-
32	FTA_MCS.2	FIA_UID.1	23 Rationale(4)
33	FTA_SSL.5	FIA_UAU.1	20 Rationale(3)
34	FTA_TSE.1	-	-

Rationale(1) : FAU_GEN.1 have a dependency on FPT_STM.1. However, the TOE satisfies the dependency by using the reliable time stamp provided by the security objective OE.TIME_STAMP for the operating environment.

Rationale(2) : FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, the TOE ensures that audit data are protected from unauthorized deletion or modification by the security objective OE.AUDIT_DATA_PROTECT for the operating environment, thereby satisfying the dependency of FAU_STG.1.

Rationale (3): FIA_AFL.1, FIA_UAU.7, FTA_SSL.5 have a dependency on FIA_UAU.1, which satisfies the dependency using FIA_UAU.1 and hierarchical relationship FIA_UAU.2.

Rationale (4): FIA_UAU.2, FMT_SMR.1, FTA_MCS.2 have a dependency on FIA_UID.1, which satisfies the dependency using FIA_UID.1 and hierarchical relationship FIA_UID.2.

5.3.2. Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

The augmented SAR ATE_FUN.1 has dependency on ATE_COV.1. but, ATE_FUN.1 is augmented to require developer testing in order to check if the developer correctly performed and documented the tests in the test documentation, ATE_COV.1 is not included in this PP since it is not necessarily required to show the correspondence between the tests and the TSFIs.

6. TOE Summary Specification

This chapter describes SFRs implemented in the TOE.

6.1. Security Audit

The TOE generates and manages the event date and time, event type, subject identification, outcome of the event, and event contents of the auditable events as audit data. Only the authorized administrators can review the generated audit data through Management Server, and it is detected as a potential security violation and an email is sent to the authorized administrator.

The authorized administrators can search and review about the audit data through the management interface. Search results of audit data is sorted in descending order according to the date and time of generation. When the threshold of audit data storage (80%) exceeds, an email is sent to the authorized administrator.

6.1.1. Audit data generation

When an auditable event occurs during operation, spice.ssm, spice.mgs, spice.cc generates audit data, including the event date and time, event type, identity of the subject that caused the event, work history and results, and so forth. The audit data is generated when spice.ssm, spice.mgs, spice.cc is running, and spice.mgs collects the audit data generated by spice.ssm. The TOE saves the audit data in the storage provided by the TOE operational environment.

When generating audit data, the TOE uses the reliable time stamp provided by the TOE operational environment as the event occurrence time to ensure that the audit data is generated sequentially.

- SFR to be satisfied : FAU_GEN.1

6.1.2. Audit data review

The TOE allows the authorized administrator to review about all audit data from the audit storage. spice.cc, spice.mgs saves the audit data in the audit storage, the authorized administrator can search the audit data based on the event time, event type, and target IP through spice.cc. Search results of audit data is sorted in descending order based on the time of occurrence of the event.

- SFR to be satisfied : FAU_SAR.1, FAU_SAR.3

6.1.3. Security alarms

When an auditable event such as administrator authentication failure audit event, integrity violation audit event and self-test failure event of the validated cryptographic module occurs, spice.cc indicates it out as a potential security

violation. When a potential security violation event occurs, spice.cc generates audit data (alert log) for it and sends an email to the authorized administrator.

- SFR to be satisfied : FAU_ARP.1, FAU_GEN.1, FAU_SAA.1

6.1.4. Audit data loss prevention

In order to prevent audit data loss, spice.cc generates an alert log and sends an email to the authorized administrator when the usage rate of the audit storage exceeds the threshold (80%).

When the audit storage is full (usage rate exceeds 80%), spice.cc overwrites the oldest audit data, generates an alert log, and sends an email to the authorized administrator.

- SFR to be satisfied : FAU_STG.3, FAU_STG.4, FMT_MOF.1, FMT_MTD.1(2)

6.2. Cryptographic Support

To encrypt/decrypt user data and protect TSF data and data transmitted between the TOE components, the TOE generates, distributes and destroys cryptographic keys and performs cryptographic operates using the approved cryptographic algorithm of 'AhnLab Cryptographic Module V1.0'(the validated cryptographic module verified for safety and implementation conformities through KCMVP).

Table 6-1. TOE Cryptographic Support

Classification	Standards	Cryptographic algorithm	Cryptographic key sizes	Use
User data encryption	ISO/IEC 18031 NIST SP 800-90A R1	HASH_DRBG	256 bit (ARIA)	Cryptographic key generation (DEK)
	KS X 1213-1	ARIA	256 bit	Encryption/decryption (Operation mode : CBC)
DEK encryption	TTAS.KO-12.0334	PBKDF2(SHA-256)	256 bit (ARIA)	Cryptographic key generation (KEK)
	KS X 1213-1	ARIA	256 bit	Encryption/decryption (Operation mode : CBC)
Encrypted communication between the TOE components	ISO/IEC 18031 NIST SP 800-90A R1	HASH_DRBG	256 bit (ARIA)	Cryptographic key generation
	KS X 1213-1	ARIA	256 bit	Encryption/decryption (Operation mode : CBC)

	ISO/IEC 10118-3	SHA	256 bit	Integrity verification
	ISO/IEC 11770-3	DH	256 bit	Cryptographic key distribution
TSF data encryption	ISO/IEC 18031 NIST SP 800-90A R1	SHA	256 bit (ARIA)	Cryptographic key generation
	KS X 1213-1	ARIA	256 bit	Encryption/decryption (Operation mode : CBC)
	ISO/IEC 10118-3	SHA	256 bit	Integrity verification

6.2.1. Cryptographic key generation

spice.ssm generates DEK and KEK to encrypt the user data. spice.ssm, spice.mgs generates a cryptographic key for encrypted communication between spice.ssm, spice.mgs.

spice.cc generates a cryptographic key for encryption/decryption of the TOE setting values (TSF data).

The key generation algorithm and cryptographic keys follow "Table 6-1 TOE Cryptographic Support".

The TOE generates random numbers with the random number generator of the validated cryptographic module to generate the cryptographic key.

- SFR to be satisfied : FCS_CMK.1(1), FCS_CMK.1(2),

6.2.2. Cryptographic key distribution

In the case of the cryptographic keys to encrypt/decrypt the user data, the TOE generates and uses them in spice.ssm, and does not distribute the cryptographic keys to other TOE components.

spice.ssm, spice.mgs uses the DH algorithm for cryptographic key distribution during encrypted communication between spice.ssm, spice.mgs. The policy data and audit data transmitted between spice.ssm, spice.mgs. are encrypted using ARIA-256 algorithm.

- SFR to be satisfied : FCS_CMK.2

6.2.3. Cryptographic key destruction

The TOE destroys cryptographic keys to prevent the reuse of the cryptographic keys When the use of cryptographic keys loaded into the memory is completed. The cryptographic key destruction method is to overwrite the cryptographic key with '0x00'.

- SFR to be satisfied : FCS_CMK.4

6.2.4. Cryptographic operation

User data encryption, encryption communication between the TOE components, and TSF data encryption are encrypted using the validated cryptographic module. Cryptographic key generation and cryptographic algorithm follow "Table 6-1 TOE Cryptographic Support".

spice.ssm performs the user data encryption. According to the encryption policy created by the authorized administrator, user data is encrypted with the cryptographic algorithm (ARIA-256) in DEK. spice.ssm protects the DEK by encrypting it with the KEK using the ARIA-256 algorithm. KEK is generated using the secure key derivation function (PBKDF2).

spice.mgs and spice.cc perform TSF data encryption. The data transmitted between spice.ssm, spice.mgs is encrypted with the ARIA-256 algorithm.

- SFR to be satisfied : FCS_COP.1(1), FCS_COP.1(2)

6.3. User data Protection

spice.ssm encrypts/decrypts the user data by column based on the encryption policy set by the authorized administrator. It protects the user data by immediately deleting the original data after encryption/decryption of the user data is performed.

- SFR to be satisfied : FDP_UDE.1, FDP_RIP.1

6.4. Identification and authentication

The TOE provides identification and authentication functions to administrators who perform security management functions. The administrator's password is created and changed when the passwords combination rules are satisfied. When the administrator enters authentication data, it is masked. When identification and authentication failure, the TOE does not provide feedback on the cause of failure. When the maximum allowed number of authentication failures is reached, the administrator account status is deactivated.
The TOE provides a function to block attempts to reuse authentication information for the administrators.

6.4.1. Identification and authentication of the administrator

spice.cc provides security management functions after identification and authentication before all actions of the administrator.

spice.cc performs administrator identification and authentication through ID and password. The TOE sets the ID and password during the installation process. spice.cc forces the password to be changed when the newly added administrator accesses it for the first time and the administrator can change the password of his/her own account if desired. The administrator password is one-way encrypted (hash) and saved.

spice.cc provides the following verification mechanisms in generating the administrator password.

a) Allowable characters: Available characters are as follows - Uppercase and lowercase letters (a-z, A-Z: 52 characters), numbers (0-9: 10 characters), and special characters (20 characters: ! @ # $ % ^ & * ( ) _ + - = ~ : ; . / |). Including these, there are a total of 82 characters.

b) Combination rules: Combination of four types of letters among English uppercase and lowercase letters, special characters, and numbers

c) Min/Max Length: 9 to 20 characters

- SFR to be satisfied : FIA_UAU.2, FIA_UID.2, FIA_SOS.1, FMT_PWD.1

6.4.2. Protected Authentication Feedback

When the administrator password is input on the authentication request screen, spice.cc masks the password ("●●●") and outputs it on the screen. Since spice.cc does not provide feedback on the cause of failure in case of identification and authentication failure, it prevents unauthorized users from inferring the administrator's password.

- SFR to be satisfied : FIA_UAU.7

6.4.3. Authentication failure handling

When the number of authentication failures of an administrator reaches the maximum allowable number of authentication failures (5 times), spice.cc blocks authentication attempts by changing the administrator's account status to inactive (account locked). When authentication fails, the TOE creates audit data (alert log) and sends an email to the authorized administrator.

a) Master: Account locked for 5 minutes

b) Viewer: Account locked for 5 minutes or locked within 5 minutes until account unlocked by Master administrator

spice.cc greates one session when the authentication attempt is successful. spice.cc creates a new session ID including time stamp information for each session. If an unauthorized user reuses an authenticated session, spice.cc compares the session ID issued by itself with the session ID possessed by the unauthorized user and fails the identification and authentication procedures.

In addition, administrators use OTP for each management access to prevent the reuse of authentication sessions.

- SFR to be satisfied : FIA_AFL.1, FIA_UAU.4

6.5. Security management

The TOE can access the TOE through the web browser (HTTPS protocol based on TLS v1.2), and only administrators who have successfully identified and authenticated through secure communication can perform security management functions of the TOE.

The TOE provides security management functions such as security policy management and administrator management to the authorized administrators. The TOE sets the administrator's ID and password during the installation process. Administrators perform security roles according to authority.

6.5.1. Administrator role

If the administrator's identification and authentication are successful, spice.cc assigns the right appropriate to the security role. spice.cc provides the function of managing security functions only to the authorized administrator through identification and authentication procedures, and the authorized administrator is classified as follows according to the granted authority.

Table 6-2. Authorized Administrator's Role

Authority	Role
Master	Query, modify, delete, encryption target system addition, administrator access IP addition/modify/delete, administrator account management, self-information management
Viewer	Query, administrator access IP addition/modify/delete, self-information management

- SFR to be satisfied : FMT_SMR.1

6.5.2. Security Function Management

In spice.cc, only an authorized administrator who has succeeded in authentication can manage security functions according to the administrator's security role. For the security functions that can be performed according to the administrator security role, refer to "Table 5-10. List of Security Functions".

- SFR to be satisfied : FMT_MOF.1, FMT_SMF.1

6.5.3. Management of TSF Data

In spice.cc, only an authorized administrator who has succeeded in authentication can manage the TSF data according to the administrator's security role. For the TSF data that can be managed according to the administrator security role, refer to "Table 5-11. List of TSF data".

- SFR to be satisfied : FMT_MTD.1, FMT_SMF.1

6.6. Protection of the TSF

The TOE carries out mutual authentication through the internally implemented authentication protocol for secure communication between the TOE components.

The TOE performs encrypted communication to protect the TSF data transmitted between the TOE components.

In order to check whether the TOE operates normally, the TOE performs self-tests on main processes of the TOE during initial startup, and periodically performs self-tests during normal operation. The TOE performs integrity tests on TSF data and TSF executable files during initial startup, and periodically performs integrity tests during normal operation.

6.6.1. Internal TSF data transfer protection

For secure communication between spice.mgs and spice.ssm, spice.mgs, spice.ssm, performs mutual authentication, encrypted communication, and message integrity verification through the internally implemented authentication protocol.

spice.mgs, spice.ssm distributes the cryptographic key based on the internally implemented authentication protocol and uses this cryptographic key to ensure the confidentiality and integrity of the TSF data between spice.mgs and spice.ssm. The transmitted TSF data is encrypted/decrypted using the ARIA-256 cryptographic algorithm of the validated cryptographic module. To verify the integrity, the SHA-256 hash function of the validated cryptographic module is used.

Table 6-3. Internally Implemented Authentication Protocol and Encrypted Communication

단계	Sender	Receiver	설명
1	spice.ssm	spice.mgs	1) spice.ssm generates cryptographic key TK. 2) Mutual authentication message, DH public key are encrypted with cryptographic key TK and the message hash value is added. Send to spice.mgs.
2	spice.mgs	-	1) spice.mgs generates cryptographic key TK. 2) In the received message, Checks the mutual authentication message and verifies the integrity of the message.
3	spice.mgs	spice.ssm	1) Mutual authentication messages, DH public key are encrypted with cryptographic key TK and the message hash value is added. Send to spice.ssm
4	spice.ssm	-	1) In the received message, Checks the mutual authentication message and verifies the integrity of the message.

5	spice.ssm	spice.mgs	1) spice.ssm generates a session key. 2) The message is encrypted with the session key and the message hash value is added. Send to spice.mgs
6	spice.mgs	-	1) spice.mgs generates a session key. 2) In the received message, Verifies the integrity of the message.
7	spice.mgs	spice.ssm	1) The message is encrypted with the session key and the message hash value is added. Send to spice.ssm
8	spice.ssm	-	1) In the received message, Verifies the integrity of the message, response message is confirmed.

- SFR to be satisfied : FIA_IMA.1, FTP_ITT.1

6.6.2. protection of stored TSF data

The TOE encrypts, stores, and manages the TSF data to protect it from exposure and modification. The TOE encrypts the following TSF data using the validated cryptographic module.

- Administrator password (Master, Viewer): SHA-256
- DBMS account information: ARIA-256
- Audit log storage account information: ARIA-256
- User data cryptographic key (DEK): ARIA-256
- Keystore password: SHA-256

The user data encryption key (DEK) is encrypted using the key encryption key (KEK) generated by the PBKDF2 algorithm and stored in the keystore. The keystore can be saved using the keystore password.

- SFR to be satisfied : FPT_PST.1

6.6.3. Self tests

To check whether the TOE operates normally, spice.cc performs self-tests of spice.ssm, spice.cc, spice.mgs at initial startup, and performs self-tests at regular intervals during normal operation.
spice.ssm, spice.mgs, spice.cc performs self-tests of the validated cryptographic module at initial startup, and performs self-tests at regular intervals during normal operation. If it does not operate normally, the audit data (alert log) is generated and an email is sent to the authorized administrator.

spice.cc performs the function of verifying the integrity of TSF data and TSF executable files for the correct operation of TSF. The integrity verification detects TOE operation by unauthorized administrators.
spice.cc performs integrity tests on TSF data and TSF executable files during initial startup, and performs integrity tests

at regular intervals (60 minutes) during normal operation.
spice.cc generates hash values with the SHA-256 algorithm and performs the integrity test. If the hash values do not match, the audit data (alert log) is generated and an email is sent to the authorized administrator.

- SFR to be satisfied : FPT_TST.1

6.7. TOE Access

spice.cc allows up to 1 concurrent session of the same administrator account or an administrator account with the same authorities. The new administrator's access is blocked if the maximum concurrent sessions exceed.

spice.cc forcibly terminates the session of the account if the authorized administrator does not perform security functions for the predefined allowable period of administrator inactivity (600 seconds) after logging in. The administrator, whose session is terminated, must attempt re-authentication to access spice.cc.
spice.cc allows management access only from the set access IP address and rejects access attempted from an unauthorized access IP address.

- SFR to be satisfied : FTA_MCS.2, FTA_SSL.5, FTA_TSE.1