EdgeDB v4.2
Security Target (ST) lite

v1.0

ITCEN PNS

The certified Security target is written in Korean. This document is a translation of the original from Korean into English.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Revision History		
Title	EdgeDB v4.2_Security Target(ST) lite	
Version	**Date**	**Description**
v1.0	2026.10.01	Created EdgeDB v4.2 Security Target (ST) v1.4 for Public

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

Table of Contents

1. SECURITY TARGET INTRODUCTION 8

1.1. ST REFERENCE 8
1.2. TOE REFERENCE 9
1.3. TOE OVERVIEW 10
1.3.1. TOE Usage and Key Security Features 10
1.3.2. TOE Type 12
1.3.3. Identification of non-TOE HW/SW 15
1.4. TOE DESCRIPTION 20
1.4.1. Physical Scope of the TOE 20
1.4.2. Logical Scope of the TOE 24
1.5. TERMS AND DEFINITIONS 32
1.6. CONVENTIONS 42

2. CONFORMANCE CLAIM 43

2.1. CC CONFORMANCE CLAIM 43
2.2. PP CONFORMANCE CLAIM 44
2.3. PACKAGE CONFORMANCE CLAIM 45

3. SECURITY PROBLEM DEFINITION 46

3.1. ASSETS 46
3.2. THREATS 46
3.2.1 UNAUTHORIZED ACCESS 46
3.2.2 INFORMATION LEAK 47
3.2.3 TOE FUNCTIONALITY COMPROMISE 47
3.3. ORGANIZATIONAL SECURITY POLICIES 47
3.4. ASSUMPTIONS 48

4. SECURITY OBJECTIVES 50

4.1. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 50
4.2. SECURITY OBJECTIVES RATIONALE 51
4.2.1. Security Objectives Rationale for the Operational Environment 51

5. EXTENDED COMPONENTS DEFINITION 55

5.1. IDENTIFICATION AND AUTHENTICATION (FIA) 55

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

5.1.1. TOE Internal mutual authentication 55
5.2. USER DATA PROTECTION (FDP) 56
5.2.1. User data encryption 56
5.3. SECURITY MANAGEMENT (FMT) 57
5.3.1. ID and password 57
5.4. PROTECTION OF THE TSF (FPT) 58
5.4.1. Protection of stored TSF data 58
6. SECURITY REQUIREMENTS 59
6.1. SECURITY FUNCTIONAL REQUIREMENTS 59
6.1.1. Security Audit (FAU) 61
6.1.2. Cryptographic Support (FCS) 65
6.1.3. User Data Protection (FDP) 74
6.1.4. Identification and Authentication (FIA) 75
6.1.5. Security Management (FMT) 77
6.1.6. Protection of the TSF (FPT) 80
6.1.7. TOE Access (FTA) 82
6.1.8. Trusted Path/Channels (FTP) 83
6.2. SECURITY ASSURANCE REQUIREMENTS 83
6.2.1. Security Target Evaluation 84
6.2.2. Development 90
6.2.3. Guidance 91
6.2.4. Life-cycle support 92
6.2.5. Tests 93
6.2.6. Vulnerability assessment 94
6.3. SECURITY REQUIREMENTS RATIONALE 95
6.3.1. Security Functional Requirements Rationale 95
6.3.2. Security Assurance Requirements Rationale 104
6.3.3. Dependencies of Security Functional Requirements 104
6.3.4. Dependencies of Assurance Requirements 107
7. TOE SUMMARY SPECIFICATION 107
7.1. SECURITY AUDIT 109
7.1.1. Audit data generation 109
7.1.2. Audit Review 112
7.1.3. Potential Violation Analysis and Response 113

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

7.1.4. Protection of Audit Data and Response to Possible Audit Data Loss 114
7.2. CRYPTOGRAPHIC SUPPORT 115
7.2.1. Cryptographic Key Generation 115
7.2.2. Cryptographic key derivation 117
7.2.3. Cryptographic key distribution 117
7.2.4. Cryptographic Key Destruction 120
7.2.5. Cryptographic Operation 122
7.2.6. Random Bit Generation 124
7.3. USER DATA PROTECTION 125
7.4. IDENTIFICATION AND AUTHENTICATION 126
7.4.1. Identification and Authentication of the Administrator 126
7.4.2. mutual authentication 129
7.5. SECURITY MANAGEMENT 129
7.5.1. Security Roles 129
7.5.2. Management of security functions behavior 130
7.5.3. Management of TSF data 130
7.5.4. Management of ID and Password 132
7.6. PROTECTION OF THE TSF 133
7.6.1. Basic internal TSF data transfer protection 134
7.6.2. Basic Protection of Stored TSF Data 134
7.6.3. Self-Test 138
7.6.4. Failure with preservation of secure state 144
7.7. TOE ACCESS 144
7.7.1. Limitation on Multiple Concurrent Sessions 145
7.7.2. Session Management and Configuration 145
7.8. TRUSTED PATH/CHANNELS 145
7.8.1. Inter-TSF trusted channel 145

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

List of Figures

[FIGURE 2-1] TOE OPERATIONAL ENVIRONMENT (PLUG-IN METHOD) 13
[FIGURE 2-2] TOE OPERATIONAL ENVIRONMENT (API METHOD) 14
[FIGURE 2-3] OPERATIONAL ENVIRONMENT CONFIGURATION OF THE API METHOD 16
[FIGURE 2-4] OPERATIONAL ENVIRONMENT CONFIGURATION OF THE PLUG-IN METHOD 17
[FIGURE 2-5] PHYSICAL SCOPE OF THE TOE (PLUG-IN METHOD) 22
[FIGURE 2-6] PHYSICAL SCOPE OF THE TOE (API METHOD) 23
[FIGURE 2-7] LOGICAL SCOPE OF THE TOE 24

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

List of Tables

[Table 2-1] ST Reference 8
[Table 2-2] TOE Reference 9
[Table 2-3] TLS v1.2 Cipher Suites allowed by the WAS for access to the administrator page 15
[Table 2-4] Operational Environment Configuration of the API Method 16
[Table 2-5] Operational Environment Configuration of the Plug-in Method 17
[Table 2-6] Minimum Hardware and Software Requirements for TOE Installation and Operation 18
[Table 2-7] Role of the 3rd Party Software Used in the TOE 19
[Table 2-8] External IT Entity 19
[Table 2-9] Physical Scope of the TOE 21
[Table 2-10] Validated Cryptographic Module 21
[Table 2-1] Conformance to CC 44
[Table 2-2] Rationale for PP Conformance Claim 45
[Table 4-1] Correspondence between the Security Problem Definition and the Security Objectives for the Operational Environment 52
[Table 6-1] Security Functional Requirements (SFR) 61
[Table 6-2] Auditable events 63
[Table 6-3] Audit Data Types and Selection Criteria 64
[Table 6-4] Cryptographic algorithms used by the TOE to generate user data encryption keys 66
[Table 6-5] Cryptographic algorithms used by the TOE to generate TSF data encryption keys 66
[Table 6-6] Cryptographic key distribution method 68
[Table 6-7] Key derivation algorithms used by the TOE to generate cryptographic keys 68
[Table 6-8] Cryptographic Key Destruction Method 71
[Table 6-9] Cryptographic Operation of User Data 72
[Table 6-10] Cryptographic Operation of TSF Data 72
[Table 6-11] Mutual Authentication Method between TOE Components 76
[Table 6-12] Security Functions Subject to Management 78
[Table 6-13] TSF Data Subject to Management 79
[Table 6-14] Security Assurance Requirements 84
[Table 6-15] Correspondence between Security Problem Definition and Security Functional Requirements 98
[Table 6-16] Rationale for the Dependencies 106
[Table 7-1] List of TOE Security Functions 109
[Table 7-2] Auditable Events of the TOE 110

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

[Table 7-3] Audit Event Record Data 112
[Table 7-4] Additional Audit Record Content for Specific Audit Events 112
[Table 7-5] Selective Review Criteria for Audit Data 113
[Table 7-6] Examples of Potential Violation Audit Events and Response Actions 114
[Table 7-7] Validated Cryptographic Module 115
[Table 7-8] User Data Cryptographic Key Generation 116
[Table 7-9] TSF Data Cryptographic Key Generation 117
[Table 7-10] Auth Key Pair Distribution 119
[Table 7-11] Audit Key and User data Key Distribution 119
[Table 7-12] Cryptographic Key Destruction 122
[Table 7-13] User Data Cryptographic Operations 123
[Table 7-14] TSF Data Cryptographic Operations 124
[Table 7-15] Use of the Random Bit Generator for Providing Other Security Functions 125
[Table 7-16] Secret Information Verification on the EdgeDB Key Server 128
[Table 7-17] Mutual Authentication between TOE Components 129
[Table 7-18] Managed Security Functions 130
[Table 7-19] TSF Data Subject to Management 132
[Table 7-20] Administrator Password Generation Rules 133
[Table 7-21] Protection Methods for Stored TSF Data 138
[Table 7-22] Self-Test Items by TOE 141
[Table 7-23] TSF Data Integrity Verification Items by TOE 143
[Table 7-24] TSF Integrity Verification Items by TOE 144
[Table 7-25] List of Cipher Suites Selected for TLS v1.2 Communication with the Mail Server 146

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1. Security Target Introduction

This document is the Security Target (ST) of EdgeDB v4.2 (hereinafter referred to as the "TOE"), a database (hereinafter referred to as 'DB') encryption product of ITCEN PNS Co., Ltd. It defines the TOE security functions and assurance requirements, describes the TOE's security objectives and IT requirements, and provides the rationale for them.

This ST is composed of the following sections.

- Section 1: Provides basic information on the TOE of the ST and identifies the TOE through the TOE reference, TOE overview, and TOE description.
- Section 2: States the TOE's conformance to the Common Criteria and its conformance to Protection Profiles and Packages, and provides the rationale for them.
- Section 3: Describes the Security Problem Definition, including the assets the TOE must handle, threats, organizational security policies, and assumptions.
- Section 4: Describes the security objectives for the operational environment of the TOE and their rationale.
- Section 5: Describes the definition of extended components.
- Section 6: Describes the security requirements and assurance requirements for the TOE and provides the rationale for them.
- Section 7: Describes the TOE Summary Specification for the security functional requirements defined in Section 6.

1.1. ST Reference

Classification	Description
Title	EdgeDB v4.2 Security Target (ST)
ST Version	1.4
Developer	ITCEN PNS Co., Ltd.
Publication Date	2026.09.30
Common Criteria Version	CC:2022 R1
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	Database, Encryption.

[Table 1-1] ST Reference

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1.2. TOE Reference

The TOE that conforms to this ST is identified as follows.

Classification		Description	
TOE Identification		EdgeDB v4.2	
TOE Version		v4.2.0.3	
TOE Component	EdgeDB Key Agent	EdgeDB Key Agent v4.2.0.3 - EdgeDB_Key_Agent_4.2.0.3_Linux-x86_64.run	Software (CD Dist.)
	EdgeDB Log Agent	EdgeDB Log Agent v4.2.0.3 - EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	
	EdgeDB Key Server	EdgeDB Key Server v4.2.0.3 - EdgeDB_Key_Server_4.2.0.3_Linux-x86_64.run	
	EdgeDB Log Server	EdgeDB Log Server v4.2.0.3 - EdgeDB_Log_Server_4.2.0.3_Linux-x86_64.run	
Guidance		EdgeDB v4.2 Preparative Procedure (PRE) v1.4 - EdgeDB v4.2_Preparative Procedure(PRE)_v1.4.pdf	PDF (CD Dist.)
		EdgeDB v4.2 Operational User Guidance (OPE) v1.2 - EdgeDB v4.2_Operational User Guidance(OPE)_v1.2.pdf	
		EdgeDB v4.2 Developer User's Guidance (DUG) v1.2 - EdgeDB v4.2_Developer User's Guidance(DUG)_v1.2.pdf	
Developer		ITCEN PNS Co., Ltd.	

[Table 1-2] TOE Reference

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1.3. TOE Overview

EdgeDB v4.2 (hereinafter referred to as the TOE) is a DB encryption product provided in the form of software, which encrypts data stored in the DB to prevent unauthorized disclosure of important data to be protected, such as personal information and sensitive information. The TOE consists of EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, and EdgeDB Log Agent.

1.3.1. TOE Usage and Key Security Features

The encryption target of the TOE is user data within the DB managed by the organization's database management system (hereinafter referred to as the 'DBMS'). User data is defined as the data before and after it is encrypted and stored in the DB, and typically includes the organization's important data that should be protected against threats, such as personal information and sensitive information managed by the organization. Depending on the security policy of the organization operating the TOE, part or all of the user data can be the encryption target. The TOE performs encryption/decryption of user data per column in accordance with the security policy established by the authorized chief administrator. By encrypting user data, the TOE serves to protect the organization's important data from unauthorized disclosure.

The TOE's encryption method is divided into the plug-in method and the API method, depending on where user data is encrypted and decrypted. In the plug-in method, user data is encrypted and decrypted by a cryptographic procedure call in the query used by the application program in the DBMS, and the Oracle DBMS on a Linux server is supported. In the API method, user data is encrypted and decrypted by an API call of the application program's application service on the Application Server. The API method requires modification of the application program source code, and the plug-in method requires modification of the application program queries. After encryption and decryption are complete, residual information is safely deleted and protected from unauthorized disclosure.

The TOE provides a security audit function that records major events as audit data when security functions and management functions are operated, and TSF protection functions such as protection of data stored in the repository controlled by the TSF and TSF self-tests. In addition, the TOE provides identification and authentication functions such as authentication failure handling and mutual authentication among TOE components; cryptographic support functions such as cryptographic key management, distribution, and cryptographic operation for functions such as authentication token issuance; security management functions for security function management

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

and configuration; and a TOE access function for managing the access sessions of the authorized administrator.

The administrator who manages the TOE can perform security management using the administrator interface provided by the TOE and can view TOE audit records, etc. For secure communication between the TOE administrator interface and the connecting administrator, the TOE provides trusted path and channel functions through the TLS 1.2 protocol configuration of the WAS, which is part of the operational environment, and provides an integrity check function for major TOE files at TOE start-up and periodically.

The major functions evaluated for each component of the TOE are as follows.

- EdgeDB Key Server
  - Integrated management server for EdgeDB Key Agent, administrators, cryptographic keys, DB encryption policies, etc.
  - Provision of the administrator interface for TOE security management
  - Prevention of duplicate login by the chief administrator through real-time maintenance of authentication sessions
  - Provision of a function to view audit data stored in the local DB
  - Security audit functions such as audit record generation, security alarms, and (selectable) audit review

- EdgeDB Log Server
  - Server that stores the encryption/decryption execution logs, operation logs, and audit log data received from EdgeDB Log Agent in the local DB
  - Provision of security audit functions such as response to (anticipated) saturation of the audit trail storage

- EdgeDB Key Agent
  - Module that receives encryption/decryption-related policies from EdgeDB Key Server in order to provide a DB encryption service that can encrypt and decrypt user data using different cryptographic keys, cryptographic algorithms, etc. for each column
  - EdgeDB Key Agent installed on the DB Server provides a plug-in method library for performing encryption and decryption of user data
  - EdgeDB Key Agent installed on the Application Server provides an API method library

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

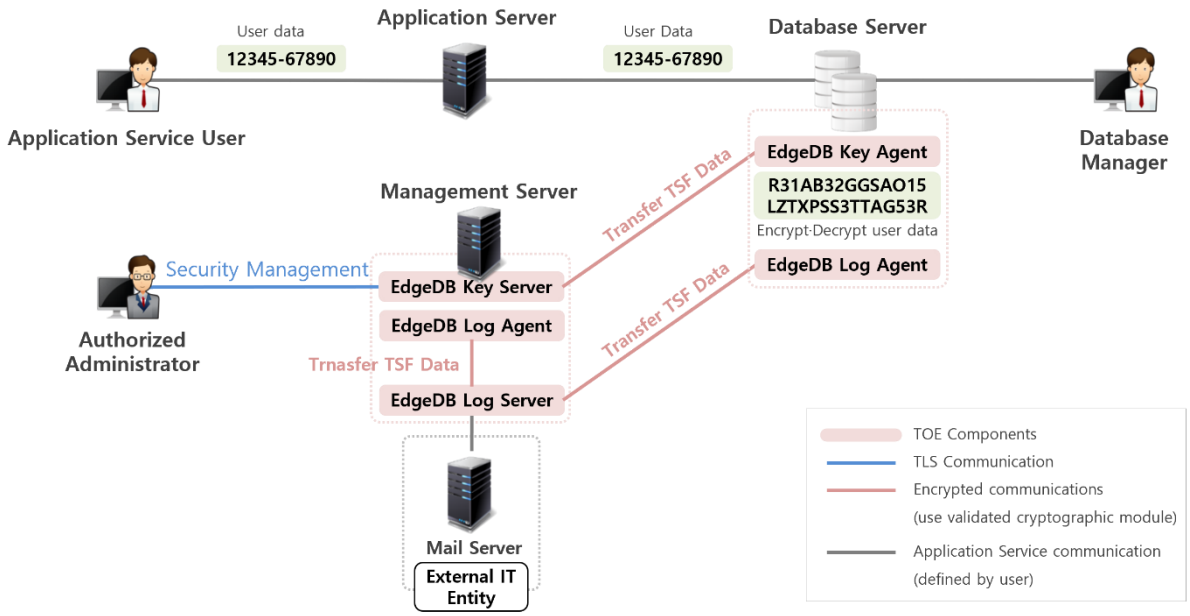
supporting JAVA- and C-based platforms for performing encryption and decryption of user data

- EdgeDB Log Agent
  - Module that delivers the encryption/decryption execution logs, operation logs, and audit log data generated by EdgeDB Key Server, EdgeDB Key Agent, EdgeDB Log Server, and EdgeDB Log Agent to EdgeDB Log Server

1.3.2. TOE Type

Depending on the TOE operation method, the TOE is divided into two types: the 'Plug-in method', which performs column-level encryption and decryption of user data using queries based on UDF (User Define Function) definitions within the database, and the 'API method', which performs column-level encryption and decryption of user data by calling the cryptographic API at the source level. Either the 'Plug-in method' or the 'API method' can be applied as desired. The 'API method' is recommended if the program source in which encryption and decryption are to be applied can be modified; otherwise, the 'Plug-in method', which can be used by modifying only the queries to be sent to the database, is recommended. Both methods are composed of four components: EdgeDB Key Agent, EdgeDB Log Agent, EdgeDB Key Server, and EdgeDB Log Server.

The environment in which the TOE operates is shown in [Figure 2-1] and [Figure 2-2].



Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

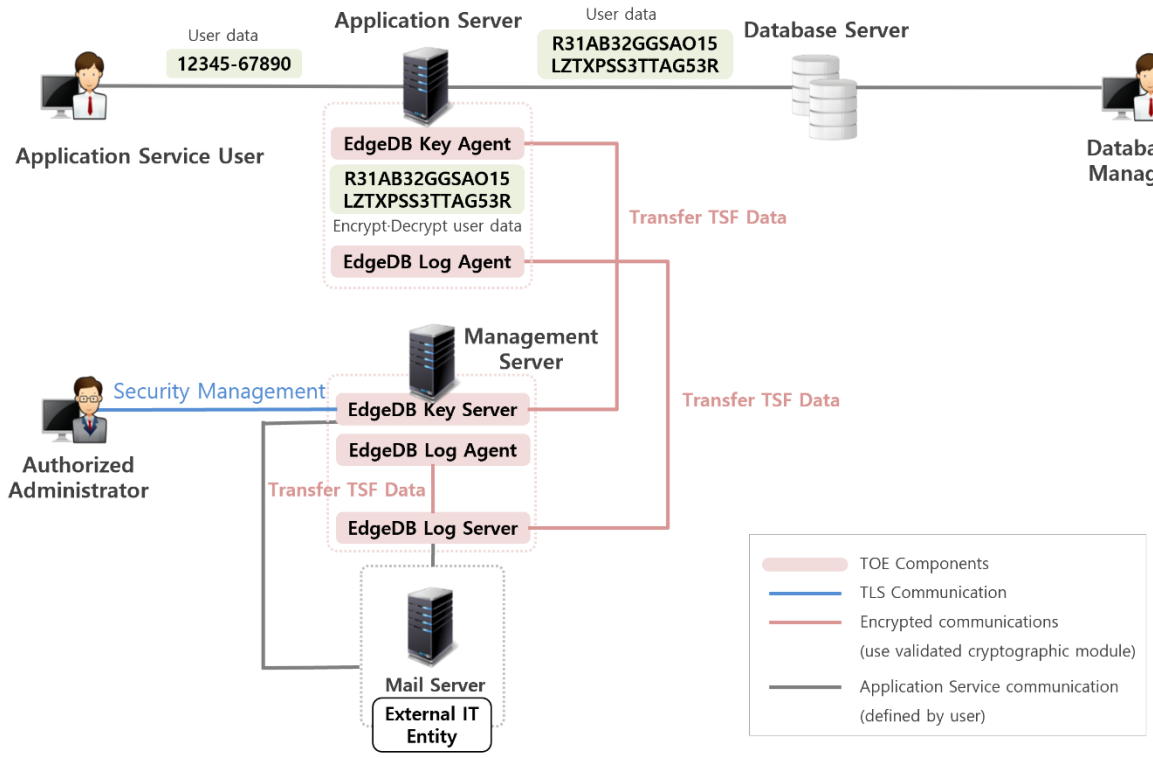
[Figure 1-1] TOE Operational Environment (Plug-in method)

In the plug-in method, EdgeDB Key Agent is installed on the Database Server where the protected DB exists, and the management server is separated. EdgeDB Key Server and EdgeDB Log Server are installed on the management server, and EdgeDB Log Agent is installed on both the Database Server and the management server where TOE components exist. The DBMS supported by the plug-in method is Oracle Database 19c (19.3.0.0.0) Enterprise Edition for Linux x86-64 in a Linux environment. In addition, a Mail Server is required in the TOE operational environment to send alarm emails when security violations occur or are detected during TOE operation.

When the authorized chief administrator sets the TOE security policy through a web browser on the administrator PC, EdgeDB Key Server delivers the corresponding DB encryption policy to EdgeDB Key Agent. In accordance with the DB encryption policy, user data received from the Application Server is encrypted before being stored in the DB through the library provided by EdgeDB Key Agent, and encrypted user data transmitted from the Database Server to the Application Server is decrypted before being transmitted to the Application Server. EdgeDB Log Agent installed on the Database Server and the management server delivers the logs generated by each TOE component to EdgeDB Log Server, and EdgeDB Log Server stores the logs collected through EdgeDB Log Agent in the DB.

Communication between the administrator PC and EdgeDB Key Server is protected using the TLS v1.2 protocol configured in the WAS, and all communications between TOE components that transmit TSF data are encrypted using the validation-target cryptographic algorithms of the validated cryptographic module.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential



[Figure 1-2] TOE Operational Environment (API method)

In the API method, EdgeDB Key Agent is installed on the Application Server, and the management server and the Database Server are separated. EdgeDB Key Server and EdgeDB Log Server are installed on the management server, and EdgeDB Log Agent is installed on both the Application Server and the management server where TOE components exist. In addition, a Mail Server is required in the TOE operational environment to send alarm emails when security violations occur or are detected during TOE operation.

When the authorized chief administrator sets the TOE security policy through a web browser on the administrator PC, EdgeDB Key Server delivers the corresponding DB encryption policy to EdgeDB Key Agent. In accordance with the DB encryption policy, user data received from the Application user is encrypted before being transmitted to the Database Server through the library provided by EdgeDB Key Agent, and encrypted user data received from the Database Server is decrypted before being transmitted to the Application user. EdgeDB Log Agent installed on the Application Server and the management server delivers the logs generated by each TOE component to EdgeDB Log Server, and EdgeDB Log Server stores the logs collected through EdgeDB Log Agent in the DB.

Communication between the administrator PC and EdgeDB Key Server is protected using the TLS

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

v1.2 protocol configured in the WAS. The following is the list of TLS v1.2 Cipher Suites allowed by the WAS.

Cipher Suites List
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256

[Table 1-3] TLS v1.2 Cipher Suites allowed by the WAS for access to the administrator page

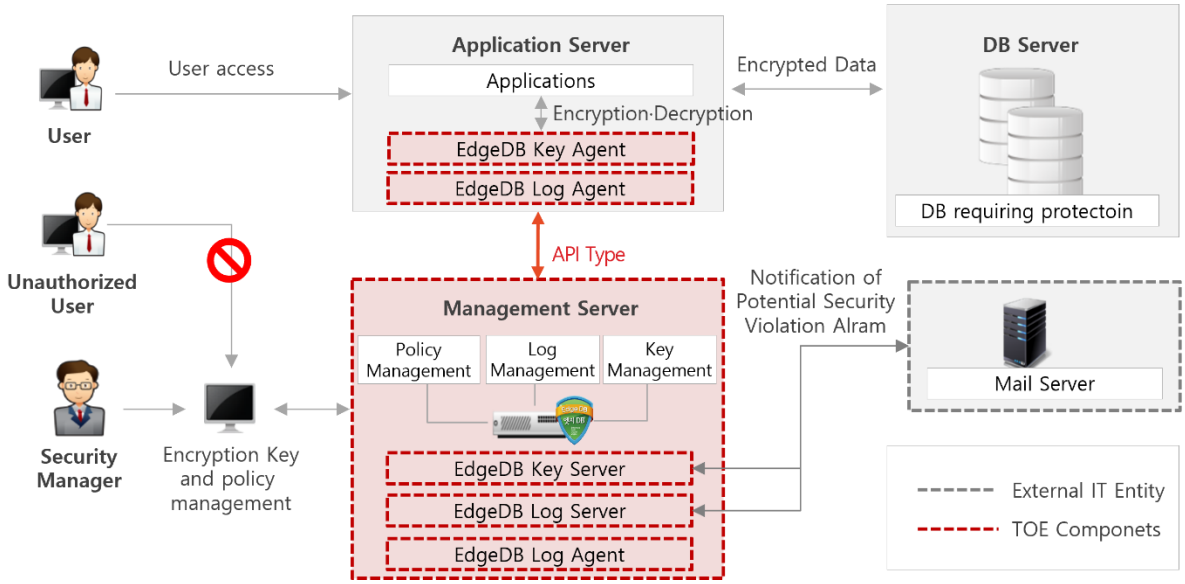
All communications between TOE components that transmit TSF data are encrypted using the validation-target cryptographic algorithms of the validated cryptographic module.

1.3.3. Identification of non-TOE HW/SW

Operating the TOE requires additional hardware and software, which are not subject to evaluation. The 3rd party software Apache-tomcat 9.0.122 and MariaDB 11.4.9 x86_64, which are specified as requirements for EdgeDB Key Server / EdgeDB Log Server, are provided separately on a CD. To operate the TOE, each TOE component and the additional software must be installed on the correct hardware, which differs depending on the operational environment and operation method.

The following describes the TOE components and 3rd party software to be installed on each piece of hardware when the operational environment is configured using the API method.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential



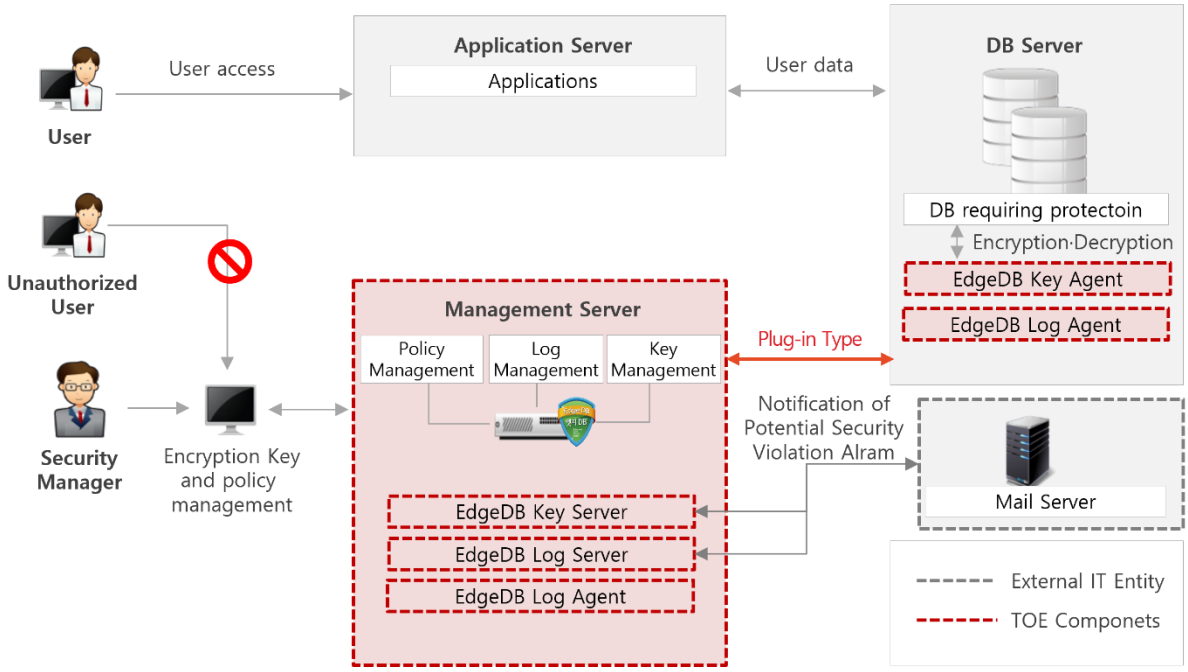
[Figure 1-3] Operational Environment Configuration of the API Method

To operate the TOE using the API method, the correct TOE components must be installed on each piece of hardware as shown in [Figure 2-3], and for the Application Server, the TOE components to be installed differ depending on the operational environment of the Application Server. The details of the TOE components to be installed for each operational environment and piece of hardware are as follows.

Classification	TOE Components	3rd Party Software
Management Server	EdgeDB_Key_Server_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Server_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	jre 8u261 linux x64 MariaDB 11.4.9 x86_64 Apache-tomcat 9.0.122 JavaMail 1.4.7
Application Server (Linux Environment)	EdgeDB_Key_Agent_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	jre 8u261 linux x64

[Table 1-4] Operational Environment Configuration of the API Method

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential



[Figure 1-4] Operational Environment Configuration of the Plug-in Method

To operate the TOE using the Plug-in method, the correct TOE components must be installed on each piece of hardware as shown in [Figure 2-4], and for the Database Server, the TOE components to be installed differ depending on the operational environment of the Database Server. The details of the TOE components to be installed for each operational environment and piece of hardware are as follows.

Classification	TOE Components	3rd Party Software
Management Server	EdgeDB_Key_Server_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Server_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	jre 8u261 linux x64 MariaDB 11.4.9 x86_64 Apache-tomcat 9.0.122 JavaMail 1.4.7
Database Server (Linux Environment)	EdgeDB_Key_Agent_4.2.0.3_Linux-x86_64.run EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	jre 8u261 linux x64 Oracle Database 19c (19.3.0.0.0) Enterprise Edition for Linux x86-64

[Table 1-5] Operational Environment Configuration of the Plug-in Method

The minimum hardware and software requirements for installing and operating the TOE are as follows.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved I Confidential

Classification			Minimum Requirements
Application Server	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB required to install the TOE
		NIC	At least one 10/100/1000 Base-T Port
	SW	OS	Ubuntu 24.04.3 LTS (release 24.04) (Kernel Linux version 6.14.0-37-generic, x86_64)
		JRE	jre 8u261 linux x64
Database Server	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB required to install the TOE
		NIC	At least one 10/100/1000 Base-T Port
	SW	OS	Ubuntu 24.04.3 LTS (release 24.04) (Kernel Linux version 6.14.0-37-generic, x86_64)
		DBMS	Oracle Database 19c (19.3.0.0.0) Enterprise Edition for Linux x86-64
		JRE	jre 8u261 linux x64
Management Server	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB required to install the TOE
		NIC	At least one 10/100/1000 Base-T Port
	SW	OS	Ubuntu 24.04.3 LTS (release 24.04) (Kernel Linux version 6.14.0-37-generic, x86_64)
		DBMS	MariaDB 11.4.9 x86_64
		JRE	jre 8u261 linux x64
		WAS	Apache-tomcat 9.0.122
Administrator PC for Windows	SW	ETC	Chrome 143.0.7499.193 64bit

[Table 1-6] Minimum Hardware and Software Requirements for TOE Installation and Operation

Among the operational requirements of the TOE described above, the 3rd party software used serves the following purposes.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

3rd Party Software	Role
jre 8u261 linux x64	Java Runtime Environment required for each TOE component to operate in a Linux operational environment
Oracle Database 19c (19.3.0.0.0) Enterprise Edition for Linux x86-64	DBMS for which the TOE provides service using the plug-in method in a Linux environment
MariaDB 11.4.9 x86_64	Database for storing TSF data such as cryptographic keys on the management server
Apache-tomcat 9.0.122	Web-based dynamic application server that provides management services by establishing a secure SSL channel for the administrator interface of EdgeDB Key Server. Uses the cipher suites in [Table 2-3] to establish the secure SSL channel.
Chrome 143.0.7499.193 64bit	Web browser used to access the administrator interface
JavaMail 1.4.7	Java mail library used by EdgeDB Key Server and EdgeDB Log Server to send security alert emails to the mail server

[Table 1-7] Role of the 3rd Party Software Used in the TOE

A separate external IT entity is required to operate the TOE. The external IT entities required by the TOE other than the evaluation target are as follows.

Classification	Description
Mail Server	Server for sending email to the authorized administrator when a potential security violation is detected

[Table 1-8] External IT Entity

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1.4. TOE Description

This section describes the scope and boundary of the TOE.

1.4.1. Physical Scope of the TOE

The physical scope and boundary of the TOE consist of EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, EdgeDB Log Agent, and the guidance documents: EdgeDB v4.2 Preparative Procedure (PRE), EdgeDB v4.2 Operational User Guidance (OPE), and EdgeDB v4.2 Developer User's Guidance (DUG).

The TOE consists of software and guidance documents, as shown in [Table 2-9].

Classification		Name	TOE Scope	File Format	Distribution Format
TOE Components	EdgeDB Key Agent	EdgeDB Key Agent v4.2.0.3 - EdgeDB_Key_Agent_4.2.0.3_Linux-x86_64.run	O	S/W	CD
	EdgeDB Log Agent	EdgeDB Log Agent v4.2.0.3 - EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run	O	S/W	
	EdgeDB Key Server	EdgeDB Key Server v4.2.0.3 - EdgeDB_Key_Server_4.2.0.3_Linux-x86_64.run	O	S/W	
	EdgeDB Log Server	EdgeDB Log Server v4.2.0.3 - EdgeDB_Log_Server_4.2.0.3_Linux-x86_64.run	O	S/W	
Guidance		EdgeDB v4.2 Preparative Procedure (PRE) v1.4 - EdgeDB v4.2_Preparative Procedure(PRE)_v1.4.pdf	O	PDF	
		EdgeDB v4.2 Operational User Guidance (OPE) v1.2 - EdgeDB v4.2_Operational User Guidance(OPE)_v1.2.pdf			
		EdgeDB v4.2 Developer User's Guidance (DUG) v1.2			

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

	- EdgeDB v4.2_Developer User's Guidance(DUG)_v1.2.pdf			
3rd party Software	MariaDB 11.4.9 x86_64 - mariadb-11.4.9-linux-systemd-x86_64.tar.gz Apache-tomcat 9.0.122 - apache-tomcat-9.0.122.tar.gz	X	S/W	Separate CD
	JavaMail 1.4.7 - mail-1.4.7.jar	O	S/W	Distributed as part of the TOE component
Validated cryptographic module	EdgeCrypto v4.2 - libEdgeCrypto.so	O	S/W	Distributed as part of the TOE component

[Table 1-9] Physical Scope of the TOE

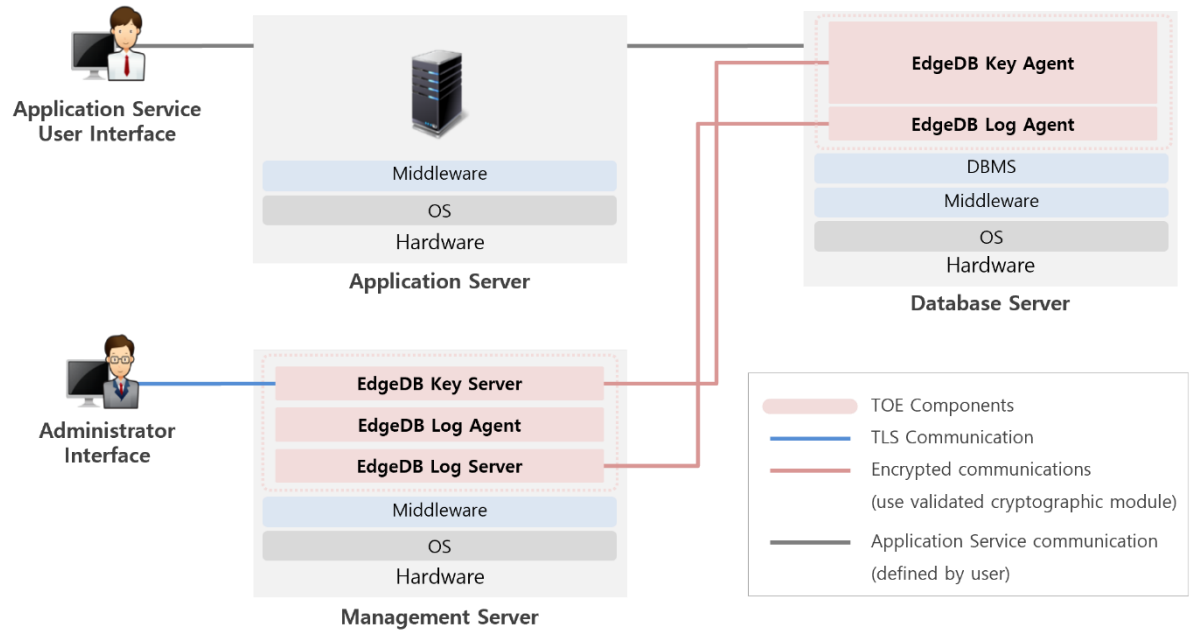
Validated cryptographic module used by the evaluated TOE

Cryptographic module name	Validated cryptographic module information	TOE used
EdgeCrypto v4.2	Verification No.: CM-299-2031.7 Verified Date: 2026.07.13	EdgeDB Key Server EdgeDB Key Agent EdgeDB Log Server EdgeDB Log Agent

[Table 1-10] Validated Cryptographic Module

The physical scope of the TOE is shown in [Figure 2-5] and [Figure 2-6].

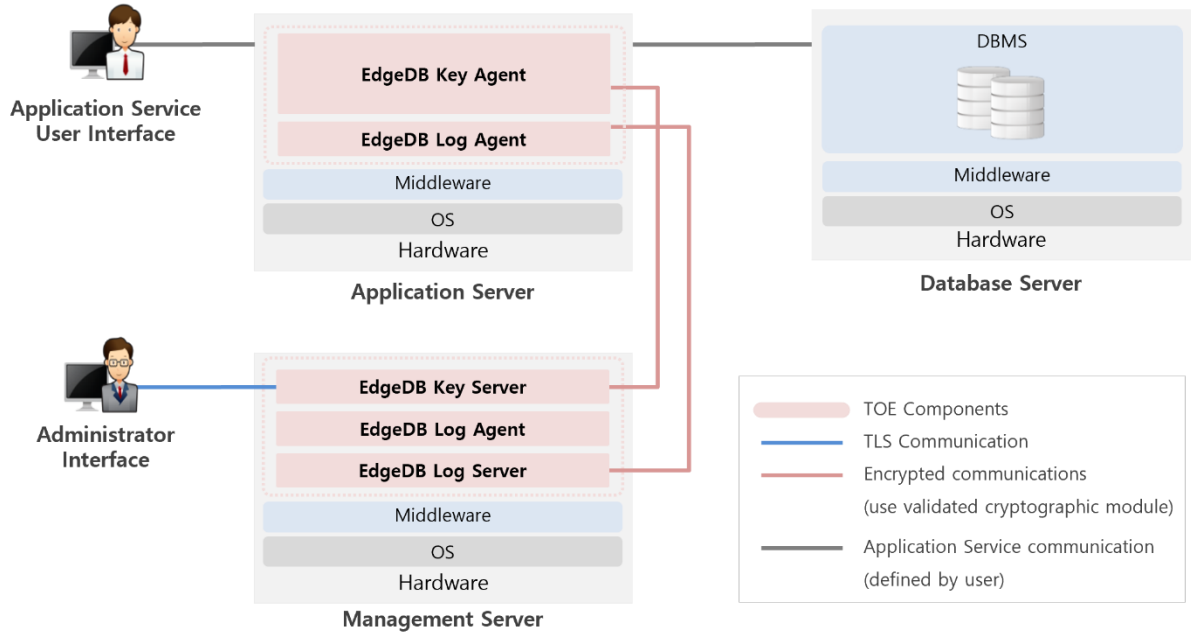
Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential



[Figure 1-5] Physical Scope of the TOE (Plug-in method)

In the plug-in method, EdgeDB Key Agent is installed on the Database Server where the protected DB exists. EdgeDB Key Server and EdgeDB Log Server are installed on the same physical management server, and EdgeDB Log Agent is installed on all servers on which TOE components are installed. Because the TOE encrypts and decrypts user data by SQL Query on the Database Server, the developer must modify the queries sent from the Application Server to the Database Server so that the plug-in function is executed.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential



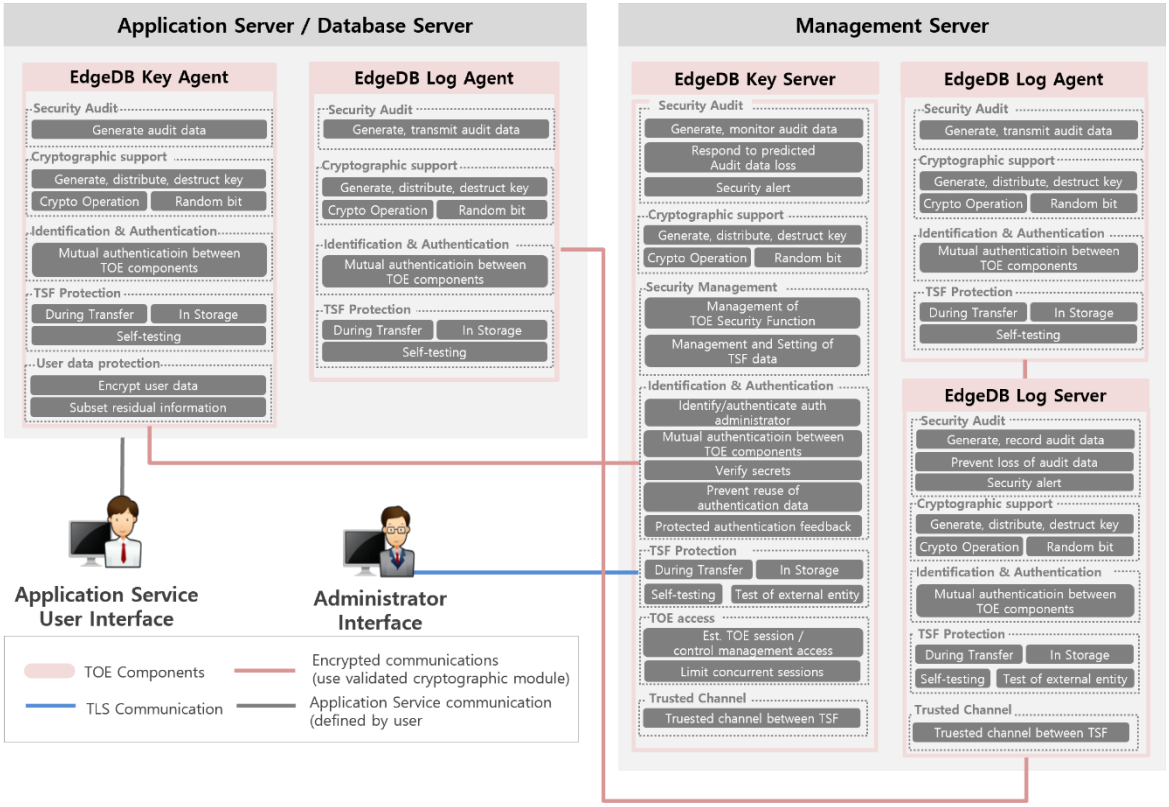
[Figure 1-6] Physical Scope of the TOE (API method)

In the API method, EdgeDB Key Agent is installed on the Application Server. EdgeDB Key Server and EdgeDB Log Server are installed on the same physical management server, and EdgeDB Log Agent is installed on all servers on which TOE components are installed. Because the TOE performs encryption before user data is transmitted from the Application Server to the Database Server, and performs decryption after user data is received from the Database Server and before it is transmitted to the user, the developer must develop the Application Server source code so that encryption and decryption are performed on the user data subject to encryption.

The hardware platform and OS (operating system) on which the TOE is installed, and 3rd party software such as the DBMS required to operate the TOE, are excluded from the scope of the TOE.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1.4.2. Logical Scope of the TOE



[Figure 1-7] Logical Scope of the TOE

1.4.2.1. EdgeDB Key Server

① Security Audit (FAU)

EdgeDB Key Server generates audit data recording the date and time of occurrence, IP of occurrence, event type, subject of the event, and event details when an auditable event, such as a defined security violation event, occurs.

Because EdgeDB Key Server is installed on the same server as EdgeDB Log Server, it can access the database in which audit data is stored, and the authorized administrator can search and view all security audit data through the administrator page provided by EdgeDB Key Server. The retrieved data can be sorted in ascending or descending order by date and time of occurrence or storage, and when specific security audit data requires review, specific conditions can be applied to perform selective audit data filtering and review.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

EdgeDB Key Server provides an audit data generation function.

When a potential violation audit event occurs in each TOE (such as authentication failure of an administrator, process check failure of EdgeDB Log Server and EdgeDB Key Agent, integrity violation, or self-test failure of the validated cryptographic module), EdgeDB Key Server sends a real-time alert email about the event to the registered email address of the authorized administrator designated by the chief administrator.

② Cryptographic Support (FCS)

EdgeDB Key Server performs the following cryptographic support required to carry out mutual authentication with TOE components, protection of transmitted TSF data, protection of stored TSF data, encryption of user data, and integrity verification of the TSF and TSF data.

- Cryptographic key generation: Generates Master Key, Local Key, Audit Key, Auth Key Pair, Session Key, and User data Key with the cryptographic algorithms and key lengths in [Table 6-4] and [Table 6-5].
- Cryptographic key distribution: Distributes Audit Key, Auth Key, and User data Key online or offline by the methods in [Table 6-6].
- Cryptographic operation: Performs encryption operations on TSF data using the cryptographic algorithms in [Table 6-10].
- Cryptographic key destruction: The TOE zeroizes cryptographic keys and Critical Security Parameters (CSPs) as in [Table 6-8] (overwriting with zeros twice).

Random number generation, and the HMAC-SHA256 algorithm used in the PBKDF2 algorithm, as well as all cryptographic algorithms of the TOE, use the validation-target algorithms of the validated cryptographic module. (Excluding the TLS v1.2 algorithms)

③ Identification and Authentication (FIA)

To allow access to the security management functions provided by EdgeDB Key Server, an identification and authentication process for identity verification is performed before any action of the authorized administrator and before allowing any action related to security functions. All administrator passwords must satisfy the combination rule of uppercase English letters, lowercase English letters, numbers, and special characters; passwords identical to the user account (ID), consecutive repeated input of the same characters or

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

numbers, and sequential input of consecutive keyboard characters or numbers are prohibited. All passwords entered when creating, changing, and authenticating a password are masked with ("*").

When authentication fails, no feedback on the reason for the failure is provided, and if authentication fails consecutively for the permitted number of authentication failures (fixed at 5), the identification and authentication function is deactivated for 5 minutes.
EdgeDB Key Server prevents reuse of authentication sessions by issuing a sessionId that guarantees the uniqueness of the authentication session of the authorized administrator.

When EdgeDB Key Agent requests authentication, EdgeDB Key Server performs mutual authentication through mutual signature generation and verification using the Auth Key Pair.

④ Security Management (FMT)
EdgeDB Key Server provides security management functions that allow security policies, important data, etc. to be configured and managed through the administrator page, and a function that allows every authorized administrator to change the ID and password, or the password, at first access.

Administrators are divided into the chief administrator, who is the first administrator created, and general administrators additionally created by the chief administrator; general administrators can perform only monitoring functions.

⑤ Protection of the TSF (FPT)
To confirm that the external entities required for operation are operating normally, EdgeDB Key Server checks whether the mail server and the local DB are operating normally according to conditions defined in the TOE, and notifies the administrator when a problem occurs.

EdgeDB Key Server protects stored TSF data such as administrator passwords, cryptographic keys, Critical Security Parameters, TOE configuration values, and file-type audit data using ARIA-256-CBC encryption, self-implemented encoding techniques, SHA-256 hash, etc., and cryptographic keys and Critical Security Parameters loaded into memory are self-encoded and stored in memory.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

EdgeDB Key Server protects TSF data transmitted to EdgeDB Key Agent from disclosure and modification using the ARIA-256-CBC and SHA-256 cryptographic algorithms.

EdgeDB Key Server performs self-tests at server start-up and periodically during regular server operation to check whether the major processes of each TOE component are running correctly, and performs the self-test of the validated cryptographic module. It also performs integrity checks on some TSF and TSF data at start-up, on demand by the administrator, or periodically during operation, and notifies the authorized administrator in case of an integrity violation.

⑥ TOE Access (FTA)

The security management interface of EdgeDB Key Server controls TOE access so that login is possible only from registered IPs. Through the security management interface provided by EdgeDB Key Server, permitted access IPs can be added and changed one at a time. By limiting the number of sessions that can connect to the interface simultaneously, concurrent access with the same account and the same authority is blocked. When a duplicate connection with the same account is attempted, the existing session is terminated and the new connection is established, and audit data is generated for this.

Only one account is permitted the authority of the chief administrator. The number of general administrators who can connect concurrently is limited (default: 5, configurable from 5 to 100). The security management interface automatically terminates the session after 10 minutes of inactivity following login.

⑦ Trusted Path/Channels (FTP)

To securely send emails containing important information to the authorized administrator, EdgeDB Key Server performs encrypted communication using TLS v1.2 and a cryptographic algorithm that satisfies a complexity of 112 bits or more.

1.4.2.2. EdgeDB Log Server

① Security Audit (FAU)

EdgeDB Log Server generates audit data recording the date and time of occurrence, IP of occurrence, event type, subject of the event, and event details when an auditable event,

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

such as a defined security violation event, occurs.

When EdgeDB Log Agent sends audit data from a server on which TOE components are installed, EdgeDB Log Server stores it in the local DB on the management server on which EdgeDB Log Server is installed.

When notification is configured for the usage of the DB audit data storage, a threshold between 60% and 90% can be specified, and an email notifying that the threshold has been exceeded can be sent to the authorized administrator. When the audit trail storage is saturated, audit data is no longer stored in the DB, and a warning email notifying that audit data can no longer be stored is sent to the authorized administrator designated by the chief administrator.

② Cryptographic Support (FCS)

EdgeDB Log Server performs the following cryptographic support required to carry out mutual authentication with TOE components, protection of transmitted TSF data, and integrity verification of the TSF and TSF data.

- Cryptographic key generation: Generates Master Key and Session Key with the cryptographic algorithms and key lengths in [Table 6-4] and [Table 6-5].
- Cryptographic key distribution: Distributes Audit Key online by the method in [Table 6-6].
- Cryptographic operation: Performs encryption operations on TSF data using the cryptographic algorithms in [Table 6-10].
- Cryptographic key destruction: The TOE zeroizes cryptographic keys and Critical Security Parameters (CSPs) as in [Table 6-8] (overwriting with zeros twice).

③ Identification and Authentication (FIA)

When EdgeDB Log Agent requests authentication, EdgeDB Log Server performs mutual authentication through mutual signature generation and verification using the Auth Key Pair.

④ Protection of the TSF (FPT)

EdgeDB Log Server protects stored TSF data such as cryptographic keys, critical security parameters, TOE configuration values, and file-type audit data using ARIA-256-CBC encryption and self-implemented encoding techniques, and cryptographic keys and critical

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

security parameters loaded into memory are stored in memory using self-encoding.

EdgeDB Log Server protects TSF data transmitted to EdgeDB Log Agent from disclosure and modification using the ARIA-256-CBC and SHA-256 cryptographic algorithms.

EdgeDB Log Server performs self-tests at server start-up and periodically during normal server operation to check whether the main security function processes are runnig correctly, performs the self-test of the validated cryptographic module, and performs integrity checks on some TSF and TSF data at start-up or periodically during operation; upon an integrity violation, it notifies the authorized administrator.

⑤ Trusted Path/Channels (FTP)
EdgeDB Log Server performs encrypted communication using TLS v1.2 and a cryptographic algorithm that satisfies a cryptographic strength of 112 bits or more in order to securely send mail containing critical information to the authorized administrator.

1.4.2.3. EdgeDB Key Agent

① Security Audit (FAU)
When an auditable event such as a defined security violation occurs, EdgeDB Key Agent generates audit data recording the date and time of occurrence, IP of occurrence, event type, subject of the event, and event details. The library modules in plug-in form or API form provided by EdgeDB Key Agent also generate audit data, and the information recorded at generation is the same.

② Cryptographic Support (FCS)
EdgeDB Key Agent performs the following cryptographic support required to perform mutual authentication with TOE components, protect transmitted TSF data, and verify the integrity of the TSF and TSF data.

- Cryptographic key generation: Generates the Master Key, Session Key, and Local Key with the cryptographic algorithms and key lengths in [Table 6-4] and [Table 6-5].
- Cryptographic key distribution: Receives the Audit Key, User data Key, and Auth Key, either online or offline, by the methods in [Table 6-6].
- Cryptographic operation: Performs encryption operations on user data using the

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

cryptographic algorithms in [Table 6-9] and encryption operations on TSF data using the cryptographic algorithms in [Table 6-10].

- Cryptographic key destruction: The TOE zeroizes cryptographic keys and Critical Security Parameters (CSPs) as in [Table 6-8] (overwriting with zeros twice).

③ User Data Protection (FDP)

EdgeDB Key Agent can encrypt/decrypt user data, or perform one-way encryption, empty-value encryption, and double encryption, using a different DB encryption policy for each column. After encryption/decryption is performed, the plaintext of the user data remaining in memory is securely deleted from memory using the zeroization function, thereby protecting the user data from unauthorized disclosure.

④ Identification and Authentication (FIA)

EdgeDB Key Agent requests mutual authentication from EdgeDB Key Server and performs mutual authentication through mutual signature generation and verification using the Auth Key Pair.

⑤ Protection of the TSF (FPT)

EdgeDB Key Agent protects stored TSF data such as cryptographic keys, critical security parameters, TOE configuration values, and file-type audit data using ARIA-256-CBC encryption and self-implemented encoding techniques, and cryptographic keys and critical security parameters loaded into memory are stored in memory using self-encoding.

EdgeDB Key Agent protects TSF data transmitted to EdgeDB Key Server from disclosure and modification using the ARIA-256-CBC and SHA-256 cryptographic algorithms.

EdgeDB Key Agent performs self-tests at start-up and periodically during normal operation to check whether the main security function processes are running correctly, performs the self-test of the validated cryptographic module, and performs integrity checks on some TSF and TSF data at start-up and periodically during operation; upon an integrity violation, it notifies the authorized administrator.

1.4.2.4. EdgeDB Log Agent

① Security Audit (FAU)

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

When an auditable event such as a defined security violation occurs, EdgeDB Log Agent generates audit data recording the date and time of occurrence, IP of occurrence, event type, subject of the event, and event details. Because EdgeDB Log Agent is installed on every physical server on which other TOE components are installed, it can access the audit data files generated by other TOE components on the same physical server where EdgeDB Log Agent is installed. It transmits the generated audit data to EdgeDB Log Server.

② Cryptographic Support (FCS)

EdgeDB Log Agent performs the following cryptographic support required to perform mutual authentication with TOE components, protect transmitted TSF data, and verify the integrity of the TSF and TSF data.

- Cryptographic key generation: Generates the Master Key, Session Key, and Local Key with the cryptographic algorithms and key lengths in [Table 6-4] and [Table 6-5].
- Cryptographic key distribution: Receives the Audit Key and Auth Key, either online or offline, by the methods in [Table 6-6].
- Cryptographic operation: Performs encryption operations on TSF data using the cryptographic algorithms in [Table 6-10].
- Cryptographic key destruction: The TOE zeroizes cryptographic keys and Critical Security Parameters (CSPs) as in [Table 6-8] (overwriting with zeros twice).

③ Identification and Authentication (FIA)

EdgeDB Log Agent requests mutual authentication from EdgeDB Log Server and performs mutual authentication through mutual signature generation and verification using the Auth Key Pair.

④ Protection of the TSF (FPT)

EdgeDB Log Agent protects stored TSF data such as cryptographic keys, critical security parameters, TOE configuration values, and file-type audit data using ARIA-256-CBC encryption and self-implemented encoding techniques, and cryptographic keys and critical security parameters loaded into memory are stored in memory using self-encoding.

EdgeDB Log Agent protects TSF data transmitted to EdgeDB Log Server from disclosure and modification using the ARIA-256-CBC and SHA-256 cryptographic algorithms.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

EdgeDB Log Agent performs self-tests at server start-up and periodically during normal server operation to check whether the main security function processes are running correctly, performs the self-test of the validated cryptographic module, and performs integrity checks on some TSF and TSF data at start-up and periodically during operation; upon an integrity violation, it notifies the authorized administrator.

1.5. Terms and Definitions

Among the terms used in this ST, those that are the same as terms used in the CC are in accordance with the CC. Other terms used in this ST are as follows.

Private Key
A cryptographic key that is used with an asymmetric cryptographic algorithm and is uniquely associated with a single entity (the subject using the private key); it must not be disclosed.

Object
A passive entity in the TOE that contains or receives information and on which subjects perform operations.

Personal Information
Information on a living individual that can identify that individual by name, resident registration number, etc. (including information that cannot identify a specific individual by itself but can be easily combined with other information to identify the individual)

Approved cryptographic algorithm
A cryptographic algorithm selected by the cryptographic module validation authority, considering safety, reliability, and interoperability, for block cipher, secure hash, message authentication code, random bit generation, key agreement, public key cipher, and digital signature cryptographic algorithms.

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

Public Key
A cryptographic key that is used with an asymmetric cryptographic algorithm and is uniquely

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

associated with a single 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.

Management access
The act of an administrator attempting to access the TOE using HTTPS, SSH, TLS, IPSec, etc. for the purpose of managing the TOE.

Random bit generator (RBG)
A device or algorithm that outputs a binary string that is statistically independent and unbiased. An RBG used for cryptographic applications generally generates a bit string of 0s and 1s, and this string can be combined into random bit blocks. RBGs are classified into deterministic and non-deterministic types. A deterministic RBG consists of an algorithm that generates bit strings from an initial value called a seed key, and a non-deterministic RBG produces output that depends on an unpredictable physical source.

Symmetric cryptographic technique
An encryption technique that uses the same secret key in both encryption and decryption modes; also called a secret key cryptographic technique.

Database (DB)
A set of data organized according to a certain structure in order to receive, store, and provide data in response to the demands of multiple users so as to support multiple application duties at the same time. The database related to column-level encryption required by this PP refers to a relational database.

Database Manager
A person who, or the task of, managing data stored in a database accurately and in an integrated manner.

Data Encryption Key (DEK)
A key that encrypts and decrypts data.

Local Key

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

A cryptographic key that encrypts and decrypts TSF data existing on the Management Server on which EdgeDB Key Server and EdgeDB Log Server are installed and on the servers on which EdgeDB Key Agent and EdgeDB Log Agent are installed, among the TOE components.

Master Key
A key that encrypts and decrypts the keys used to encrypt and decrypt TSF data and the user data encryption keys.

Master Password
A password directly entered by the administrator to generate the Master Key through the PBKDF2-HMAC-SHA-256 algorithm.

Audit Key
HMAC-SHA256 key for generating integrity values of the TSF and TSF data.

Sensitive Information
Information that, when leaked or damaged, has a negative impact on the owner of the information, makes continued operation of the system impossible, and causes a situation in which a significant amount of resources must be re-created.

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

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

Security attribute
Characteristics of subjects, users (including external IT products), objects, information, sessions, and/or resources that are used to define the SFR,
whose values are used to enforce the SFR.

Security Token
A hardware device implemented so that key generation, digital signature generation, etc. are processed inside the device in order to securely store and keep secret information.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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

Decryption
The act of restoring ciphertext to the original plaintext using a decryption key.

Secret Key
A cryptographic key that is used with a secret key cryptographic algorithm and is uniquely associated with one or several entities; it must not be disclosed.

User
Refer to "External Entity".

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

User data Key
A key for encrypting user data.

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

Session Key
A key used for encrypted communication between TOE components.

Identity
A representation uniquely identifying an authorized user, which can be the full or abbreviated name of that user or a pseudonym.

Encryption
The act of converting plaintext into ciphertext using an encryption key.

Element
Indivisible statement of a security need.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Role

Predefined set of rules establishing the allowed interactions between a user and the TOE.

Operation (on a component of the CC)

Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement, and selection.

Operation (on a subject)

Specific type of action performed by a subject on an object.

External Entity

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

Threat Agent

An unauthorized external entity that poses a threat to assets, such as illegal access, modification, or deletion.

Authorized Administrator

An authorized user who operates and manages the TOE securely (subdivided into Chief Administrator and General Administrator).

Authorized User

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

Authentication Data

Information used to verify the claimed identity of a user.

Auth Priv Key

The private key of the key pair used to perform mutual authentication.

Auth Pub Key

The public key of the key pair used to perform mutual authentication.

Auth Key Pair

The Auth Priv Key and Auth Pub Key used to perform mutual authentication.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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

Assets
Entities that the owner of the TOE presumably places value upon.

Refinement
Addition of details to a component.

Organizational Security Policies
Currently imposed and/or expected to be imposed in the future on the operational environment by an actual or hypothetical organization,
a set of security rules, procedures, practices, and guidelines.

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

Subject
Active entity in the TOE that performs operations on objects.

Augmentation
Addition of one or more requirements to a package.

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

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

Class
Set of CC families that share a common focus.

Target of Evaluation (TOE)

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Set of software, firmware, and/or hardware possibly accompanied by guidance.

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

Family
Set of components that share a similar goal but differ in emphasis or rigor.

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

Critical Security Parameters (CSP)
Security-related information that can compromise the security of the cryptographic module if disclosed or modified (e.g., secret keys/private keys, and authentication data such as passwords or personal identification numbers).

Application Server
The Application Server defined in this ST refers to the server on which an application, developed to provide a specific application service by the organization operating the TOE, is installed and operated. At the request of the application program, the application reads user data from the DB residing on the Database Server, or sends user data to be stored in the DB to the Database Server.

Database Server
The Database Server defined in this ST refers to the server on which the DBMS managing the protected DB is installed in the organization operating the TOE.

DBMS (Database Management System)
A software system configured to build and apply a database. The DBMS related to column-level encryption required by this PP refers to a database management system based on the relational database model.

SSL (Secure Sockets Layer)
A protocol proposed by Netscape to provide security such as confidentiality and integrity over a computer network;

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

it is a security protocol.

TLS (Transport Layer Security)
A cryptographic authenticated communication protocol between a server and a client based on SSL, 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.

Request IP
IP address of the client that requested an administrator function from EdgeDB Key Server.

Log Classification
The audit data generated by each TOE is classified by encryption, decryption, audit, and operation for selective review.

Log Level
The audit data generated by each TOE is classified as INFO, ERROR, and WARNING for selective review.

Occurrence Module
The audit data generated by each TOE is classified by each TOE component (KS (EdgeDB Key Server), LS (EdgeDB Log Server), KA (EdgeDB Key Agent), LA (EdgeDB Log Agent), LB (Library)) for selective review.

Process
A program that drives each TOE and is classified by the name of the application program that uses the JRE or the cryptographic library.

Execution Object
A function that generates audit data, classified into system, administrator, environment setting, agent, etc.

Subject of Execution

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

The execution target that generated the audit data; the administrator's ID is the target.

Classification for Execution
The actions of the execution target that generated the audit data are classified into inquiry, creation, modification, deletion, etc.

Result Code
Result code of the audit data.

Result Message
Result message of the audit data.

DB table space usage
The ratio (%) of the actual used size (data + index) of the audit log DB (edgedblog) to the total capacity of the disk on which the DB data directory is located.

DB table space usage threshold
The reference value at which storage is judged to be saturated when the DB table space usage exceeds 95%.

Zeroization
The procedure of overwriting with 0 twice for the length of the data so as not to leave residual data in the storage space of memory or files.

Storage space usage Threshold
The reference value for sending a security warning email regarding the usage of the DB table space in which audit data is stored.

Chief Administrator
An authorized administrator who has the authority to add, modify, and delete the TOE's security functions and TSF data management.

General Administrator
An authorized administrator who has only the authority to view the TOE's security functions and TSF data management.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

DBMS Account Information

Account information for accessing the DBMS.

Hash_df (Hash Derivation Function)

A derivation function defined in [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2] that converts an input bit string of arbitrary length into a fixed bit string of the requested length by repeatedly applying an approved hash function. It is used to combine and compress the entropy input collected during the instantiate and reseed processes of HASH DRBG to derive the seed and the internal state values (V, C).

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1.6. Conventions

This ST uses the same conventions as the CC for the selection, assignment, refinement, and iteration operations. The CC allows the iteration, assignment, selection, and refinement operations to be performed in security functional requirements. Each operation is used in this ST.

Iteration

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

Assignment

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

Selection

Used to select one or more of the options provided by the Common Criteria in stating a requirement. The result of a selection operation is expressed in *underlined and italicized text*.

Refinement

Used to add details to a requirement, thereby further restricting it. The result of refinement is shown in **bold text.**

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

2. Conformance Claim

The Conformance Claim describes the Common Criteria, Protection Profile, and package to which this Security Target conforms, and how this ST conforms to the Protection Profile. The language of the CC publications is Korean.

2.1. CC Conformance Claim

CC		Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CC:2022 R1 (CCMB-2022-11-001, 2022.11.) - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CC:2022 R1 (CCMB-2022-11-002, 2022.11.) - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CC:2022 R1 (CCMB-2022-11-003, 2022.11.) - Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC:2022 R1 (CCMB-2022-11-004, 2022.11.) - Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022 R1 (CCMB-2022-11-005, 2022.11.) Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2025-001 Version 1.2, 2025-10-15
Conformance claim	**Part 2 Security functional**	Extended: FDP_UDE.1, FIA_IMA.1, FMT_PWD.1, FPT_PST.1

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	components	
	Part 3 Security assurance components	*Conformant*
	Package	Augmented: EAL1 augmented (ATE_FUN.1)

[Table 2-1] Conformance to CC

2.2. PP Conformance Claim

This ST strictly conforms to the 'Korean National Protection Profile for Database Encryption V3.1 (KECS-PP-1350-2025).'

Classification	Conformance Claim (PP)	Security Target (ST)	Rationale
Type of TOE	Database Encryption	Database Encryption	Same as PP
Security Function Requirement (SFR)	FAU_ARP.1	FAU_ARP.1	Same as PP
	FAU_GEN.1	FAU_GEN.1	Same as PP
	FAU_SAA.1	FAU_SAA.1	Same as PP
	FAU_SAR.1	FAU_SAR.1	Same as PP
	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_STG.1	FAU_STG.1	Same as PP
	FAU_STG.4	FAU_STG.4	Same as PP
	FAU_STG.5	FAU_STG.5	Same as PP
	FCS_CKM.1(1)	FCS_CKM.1(1)	Same as PP
	FCS_CKM.1(2)	FCS_CKM.1(2)	Same as PP
	FCS_CKM.2	FCS_CKM.2	Same as PP
	FCS_CKM.5	FCS_CKM.5	Same as PP
	FCS_CKM.6	FCS_CKM.6	Same as PP
	FCS_COP.1(1)	FCS_COP.1(1)	Same as PP
	FCS_COP.1(2)	FCS_COP.1(2)	Same as PP
	FCS_RBG.1	FCS_RBG.1	Same as PP
	FCS_RBG.3	FCS_RBG.3(1)	Same as PP
	FCS_RBG.3	FCS_RBG.3(2)	Same as PP
	FCS_RBG.3	FCS_RBG.3(3)	Same as PP
	FCS_RBG.4	FCS_RBG.4	Same as PP

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	FCS_RBG.5	FCS_RBG.5	Same as PP
	FDP_UDE.1	FDP_UDE.1(Extended)	Same as PP
	FDP_RIP.1	FDP_RIP.1	Same as PP
	FIA_AFL.1	FIA_AFL.1	Same as PP
	FIA_IMA.1	FIA_IMA.1(Extended)	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_UAU.1	FIA_UAU.2	FIA_UAU.2, which is hierarchical to FIA_UAU.1, is used in accordance with the PP
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP
	FIA_UID.1	FIA_UID.2	FIA_UID.2, which is hierarchical to FIA_UID.1, is used in accordance with the PP
	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1	FMT_PWD.1(Extended)	Same as PP
	FMT_SMF.1	FMT_SMF.1	Same as PP
	FMT_SMR.1	FMT_SMR.1	Same as PP
	FPT_FLS.1	FPT_FLS.1	Same as PP
	FPT_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1	FPT_PST.1(Extended)	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.3	FTA_SSL.3	Same as PP
	FTA_TSE.1(1)	FTA_TSE.1(1)	Same as PP
	FTP_ITC.1	FTP_ITC.1	Same as PP

[Table 2-2] Rationale for PP Conformance Claim

2.3. Package Conformance Claim

The assurance requirement package to which this ST conforms is EAL1, with some additional assurance requirements defined.

- Assurance Package: EAL1 augmented (ATE_FUN.1)

pyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

3. Security Problem Definition

The Security Problem Definition defines the threats, organizational security policies, and assumptions that the TOE and the TOE operational environment are intended to address.

3.1. Assets

The basic assets protected by Database Encryption are as follows.

- Database managed by the DBMS in the organization's operational environment
- Important data related to the TOE itself and TOE operation (e.g., TSF data)

3.2. Threats

Threat agents are IT entities and human users that cause harm to assets through unauthorized access or abnormal methods, and can generate various threats as follows. At this time, threat agents to the TOE have a basic level of expertise, resources, and motivation.

3.2.1 Unauthorized access

T.SESSION_HIJACK

Threat agents can access user screens that are left unattended and logged in, or take advantage of user sessions that are not properly terminated while logged out to steal user authorization.

T.RETRY_AUTH_ATTEMPT

Using information gained by continuously attempting authentication, threat agents can successfully authenticate and then impersonate an authorized user to access the TOE.

T.IMPERSONATION

Threat agents can access the TOE by impersonating an authorized user, TOE components, etc.

T.REPLAY

Threat agents can find out and copy the authentication information, and replay it to access the TOE.

T.WEAK_PASSWORD

Threat agents can access the TOE by obtaining poorly managed passwords, such as those using default values, and then impersonating an authorized administrator. If low-level password rules are

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

applied, threat agents can access the TOE by impersonating an authorized administrator.

3.2.2 Information leak

T.UNAUTHORIZED_INFO_LEAK

Threat agents can leak important user information stored in the database in an unauthorized manner.

T.STORED_DATA_LEAKAGE

Threat agents can leak important data (e.g., cryptographic keys, TOE settings, etc.) stored inside the TOE or in external entities (e.g., DBMS) that interact with the TOE in an unauthorized manner.

T.TRANSMISSION_DATA_DAMAGE

Threat agents can leak or modify transmission data between TOE components and with external IT entities in an unauthorized manner.

T.WEAK_CRYPTO_PROTOCOLS

Threat agents can analyze traffic that uses weak cryptographic communication protocols or low cryptographic strength to infer cryptographic key information or find out the content of communication ciphertext.

3.2.3 TOE functionality compromise

T.TSF_COMPROMISE

Threat agents can compromise the TSF through unauthorized access, etc. to cause malfunction of the TOE functions or disable the TOE functions.

3.3. Organizational Security Policies

P.AUDIT

To track accountability for security-related actions, security-related events shall be recorded and maintained, and the recorded data shall be reviewed. In addition, the space on the disk available for storing audit data shall be regularly checked to prevent the loss of audit data, and the stored audit data must be protected from unauthorized modification or deletion.

P.SECURE_OPERATION

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Management means shall be provided so that the administrator can securely set up the TOE to comply with the organizational security policy and operate it correctly according to the TOE operation manual.

P.CRYPTO_STRENGTH

Organizations shall apply encryption measures for storage and transmission of important data, such as passwords for user authentication, and use secure cryptographic algorithms.

3.4. Assumptions

A.PHYSICAL_CONTROL

The place where the TOE is installed and operated shall be equipped with access control and protection facilities so that only authorized administrators can access it.

A.TRUSTED_ADMIN

The authorized administrator of the TOE is non-malicious, has been appropriately trained for the TOE management functions, and accurately fulfills their duties in accordance with administrator guidelines.

A.SECURE_DEVELOPMENT

Developers who use the TOE to link the encryption function to the application or DBMS shall comply with the requirements of the manual provided with the TOE to ensure that the security functions of the TOE are safely applied.

A.OPERATION_SYSTEM_REINFORCEMENT

The reliability and security of the operating system shall be ensured by reinforcing the latest vulnerabilities in the operating system on which the TOE is installed and operated.

A.SAFE_CHANNEL

Communication between the web browser of the administrator PC and the web server, which is the operational environment of the TOE server, shall be secured.

A.TIME_STAMP

The TOE operational environment shall provide reliable time stamps to the TOE.

A.AUDIT_PROTECTION

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Audit records stored in the DBMS installed on the same operating system as the TOE shall be protected by the DBMS from deletion or modification by unauthorized users.

A.MANUAL_RECOVERY

Upon completion of manual recovery, the tampered information of the TOE agent or client shall be recovered.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

4. Security Objectives

4.1. Security Objectives for the Operational Environment

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

OE.LOG_BACKUP

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

OE.PHYSICAL_CONTROL

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

OE.TRUSTED_ADMIN

The authorized administrator of the TOE shall be non-malicious, has been appropriately trained for the TOE management functions, and accurately fulfills their duties in accordance with administrator guidelines.

OE.SECURE_DEVELOPMENT

Developers who use TOE to link the encryption function to the application or DBMS must comply with the requirements of the manual provided with the TOE to ensure that the security function of the TOE is safely applied

OE.OPERATION_SYSTEM_REINFORCEMENT

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

OE.SAFE_CHANNEL

To ensure secure communication between the authorized administrator of the TOE and the WAS, which is the operational environment of the management server, the communication shall be managed through a safe channel. To configure the safe channel, the TLS v1.2 protocol provided by the WAS shall be used in accordance with the Preparative Procedures supplied with the TOE.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

OE.TIME_STAMP

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

OE.AUDIT_PROTECTION

The DBMS interacting with the TOE shall protect the audit records in which audit trails are stored from unauthorized deletion or modification.

OE.MANUAL_RECOVERY

The TOE shall be capable of manual recovery according to the procedures described in the administrator operational guidance, and upon completion of manual recovery, the tampered information of the TOE agent or client shall be recovered.

4.2. Security Objectives Rationale

4.2.1. Security Objectives Rationale for the Operational Environment

	OE.LOG_BACKUP	OE.PHYSICAL_CONTROL	OE.TRUSTED_ADMIN	OE.SECURE_DEVELOPMENT	OE.OPERATION_SYSTEM_REINFORCEMENT	OE.SAFE_CHANNEL	OE.TIME_STAMP	OE.AUDIT_PROTECTION	OE.MANUAL_RECOVERY
P.AUDIT	O							O	
P.SECURE_OPERATION			O						O
A.PHYSICAL_CONTROL		O							
A.TRUSTED_ADMIN	O		O						
A.SECURE_DEVELOPMENT				O					
A.OPERATION_SYSTEM_REINFORCEMENT					O				

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

A.SAFE_CHANNEL						O			
A.TIME_STAMP							O		
A.AUDIT_PROTECTION								O	
A.MANUAL_RECOVERY									O

[Table -1] Correspondence between the Security Problem Definition and the Security Objectives for the Operational Environment

P.AUDIT (OE.LOG_BACKUP, OE.AUDIT_PROTECTION)

P.AUDIT is performed by **OE.LOG_BACKUP** and **OE.AUDIT_PROTECTION**.

OE.LOG_BACKUP ensures that regular audit data storage space is checked by the administrator as well as the TOE function, and regular log backups or log transmission to an external log server are performed to prevent log records from being lost.

OE.AUDIT_PROTECTION protects the stored audit records from deletion or modification by unauthorized users by using the identification and authentication functions of the DBMS.

P.SECURE_OPERATION (OE.TRUSTED_ADMIN, OE.MANUAL_RECOVERY)

P.SECURE_OPERATION is performed by **OE.TRUSTED_ADMIN** and **OE.MANUAL_RECOVERY.**

OE.TRUSTED_ADMIN ensures that the administrator operates the TOE accurately in accordance with the organizational security policy and the operation manual.

OE.MANUAL_RECOVERY enables the administrator to recover the tampered information of the TOE agent or client according to the procedures described in the operational guidance.

A.PHYSICAL_PROTECTION (OE.PHYSICAL_PROTECTION)

A.PHYSICAL_PROTECTION is supported by **OE.PHYSICAL_PROTECTION.**

OE.PHYSICAL_PROTECTION places the management server in a place with protective facilities, and controls access so that only authorized administrators can access them.

A.TRUSTED_ADMIN (OE.TRUSTED_ADMIN, OE.LOG_BACKUP)

A.TRUSTED_ADMIN is supported by **OE.TRUSTED_ADMIN** and **OE.LOG_BACKUP.**

OE.TRUSTED_ADMIN has no malicious intent, is properly trained in TOE management functions, and ensure that they perform their duties accurately according to administrator guidelines.

OE.LOG_BACKUP ensures that the authorized administrator periodically checks a spare space of

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.

A.SECURE_DEVELOPMENT (OE.SECURE_DEVELOPMENT)
A.SECURE_DEVELOPMENT is supported by **OE.SECURE_DEVELOPMENT**.
OE.SECURE_DEVELOPMENT ensures that developers who use the TOE to link encryption functions to applications or DBMS comply with the requirements of the documentation provided with the TOE so that the security functions of the TOE are safely applied.

A.OPERATION_SYSTEM_REINFORCEMENT (OE.OPERATION_SYSTEM_REINFORCEMENT)
A.OPERATION_SYSTEM_REINFORCEMENT is supported by **OE.OPERATION_SYSTEM_REINFORCEMENT**.
OE.OPERATION_SYSTEM_REINFORCEMENT ensures the reliability and security of the operating system by reinforcing the latest vulnerabilities of the operating system in which the TOE is installed and operated.

A.SAFE_CHANNEL (OE.SAFE_CHANNEL)
A.SAFE_CHANNEL is supported by **OE.SAFE_CHANNEL**.
OE.SAFE_CHANNEL ensures that a secure communication path is provided for the communication between the web browser of the administrator PC and the web server, which is the operational environment of the TOE server.

A.TIME_STAMP (OE.TIME_STAMP)
A.TIME_STAMP is supported by **OE.TIME_STAMP**.
OE.TIME_STAMP ensures that reliable time stamps are provided by the operational environment of the TOE.

A.AUDIT_PROTECTION (OE.AUDIT_PROTECTION)
A.AUDIT_PROTECTION is supported by **OE.AUDIT_PROTECTION**.
OE.AUDIT_PROTECTION ensures that unauthorized deletion or modification of audit data is prevented by the DBMS installed on the operating system of the TOE.

A.MANUAL_RECOVERY (OE.MANUAL_RECOVERY)
A.MANUAL_RECOVERY is supported by **OE.MANUAL_RECOVERY**.
OE.MANUAL_RECOVERY ensures that, when the TOE agent or client has been tampered with, the

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

tampered information can be recovered through manual recovery.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

5. Extended Components Definition

This ST defines and uses the following components in addition to the components of CC Part 2. The extended components of this ST are as follows.

Identification and Authentication (FIA)

- FIA_IMA.1 TOE Internal mutual authentication

User Data Protection (FDP)

- FDP_UDE.1 User data encryption

Security Management (FMT)

- FMT_PWD.1 Management of ID and password

Protection of the TSF (FPT)

- FPT_PST.1 Basic protection of stored TSF data

5.1. Identification and Authentication (FIA)

5.1.1. 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 and description

FIA_IMA TOE Internal mutual authentication	1

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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

the PP, PP-Module, functional package or ST:
a) Minimal: Success and failure of mutual authentication

5.1.1.1. FIA_IMA.1 TOE Internal mutual authentication

Component relationships
Hierarchical to No other components.
Dependencies No dependencies.

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

5.2. User Data Protection (FDP)

5.2.1. User data encryption

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

Component leveling and description

FDP_UDE User data encryption	1

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 should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:
a) Minimal: Success and failure of user data encryption/decryption

5.2.1.1. FDP_UDE.1 User data encryption

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Hierarchical to No other components.
Dependencies FCS_COP.1 Cryptographic operation
FDP_UDE.1.1 TSF shall provide TOE users with the ability to encrypt/decrypt user data according to [assignment: *the list of encryption/decryption methods*] specified.

5.3. Security Management (FMT)

5.3.1. 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 and description

FMT_PWD ID and password	1

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 should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:
a) Minimal: All changes of the password.

5.3.1.1 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*]

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

2. [assignment: *other management such as management of special characters to be excluded from the 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 [*setting the password during installation, changing the ID and password when the authorized administrator accesses for the first time, and changing the password when the authorized administrator accesses for the first time*].

5.4. Protection of the TSF (FPT)

5.4.1. 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 and description

FPT_PST Protection of stored TSF data	1

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

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

5.4.1.1. FPT_PST.1 Basic protection of stored TSF data

Component relationships

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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 unauthorized [selection: *disclosure, modification*].

6. Security Requirements

The security requirements describe the security functional requirements and assurance requirements that the TOE must satisfy.

6.1. Security Functional Requirements

The security functional requirements defined in this Security Target were selected and used from the relevant security functional components of Common Criteria Part 2 and Chapter 5 Extended Components Definition.

Security Functional Class	Security Functional Component	
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.1	Audit data storage location
	FAU_STG.4	Action in case of possible audit data loss
	FAU_STG.5	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.5	Cryptographic key derivation
	FCS_CKM.6	Timing and event of cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	FCS_RBG.1	Random bit generation (RBG)
	FCS_RBG.3(1)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.3(2)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.3(3)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.4	Random bit generation (Internal seeding - Multiple sources)
	FCS_RBG.5	Random bit generation (Combining entropy sources)
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	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User authentication before any action
Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	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_FLS.1	Failure with preservation of secure state
	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.3	TSF-initiated termination
	FTA_TSE.1(1)	TOE session establishment
Trusted	FTP_ITC.1	Inter-TSF trusted channel

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

Path/Channels (FTP)		

[Table 6-1] Security Functional Requirements (SFR)

6.1.1. Security Audit (FAU)

6.1.1.1. 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 [
a) Send email to the administrator designated by the chief administrator
b) Deny access to the administrator menu (when the cumulative number of authentication failures exceeds the limit (5 times))
] upon detection of a potential security violation.

6.1.1.2. 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 audit records 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
c) [None]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, ["Additional audit record contents" in [Table 6-2]]

Security functional	Auditable event	Additional audit record

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

component		contents
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.4	Actions taken due to exceeding a threshold	
FAU_STG.5	Actions taken due to audit storage failure	
FCS_CKM.1	Success and failure of cryptographic key generation	
FCS_CKM.2	Success and failure of the activity (only applicable to key distribution related to user data encryption/decryption)	
FCS_CKM.6	Success and failure of the activity (only applicable to key destruction related to user data encryption/decryption)	
FCS_COP.1	Success and failure of cryptographic operation, type of cryptographic operation	
FDP_UDE.1	Success and failure of user data encryption/decryption	
FIA_AFL.1	Performance of response actions upon reaching the user authentication attempt threshold and the result (success, failure)	
FIA_IMA.1	Success of mutual authentication	
FIA_UAU.2	Timing of authentication	
FIA_UAU.4	Authentication failure due to detection of an attempt to reuse authentication data	
FMT_MOF.1	All modifications in the behavior 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	
FPT_TST.1	Execution of the TSF self-test and the test results, performance and result (success, failure) of integrity verification of TOE components	TSF data or executable code modified in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions Response actions upon detection of duplicate login	

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	with the same account Performance and result (success, failure) of blocking duplicate connections	
FTA_SSL.3	Performance and result (success, failure) of session termination of the user	
FTA_TSE.1	Blocking of the IP address of the administrative terminal connection	
FTP_ITC.1	All attempts to use the trusted channel function	

[Table 6-2] Auditable events

6.1.1.3. 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 [consecutive authentication failure events defined in FIA_AFL.1, integrity violation audit events among the auditable events of FPT_TST.1 and self-test failure events of the validated cryptographic module, verification failure events of major security function processes, audit log storage failure] known to indicate a potential security violation
b) [None]

6.1.1.4. FAU_SAR.1 Audit review

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

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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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

6.1.1.5. 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 ability to apply [selection and sorting in ascending/descending order based on date and time of occurrence/storage] of audit data based on [date and time of occurrence AND occurrence IP AND request IP AND log classification AND log level AND occurrence module AND success or failure AND result code AND number of posts].

Selection criteria (AND)	Permitted functions
Date and time of occurrence	Selective search and sorting in ascending/descending order based on date and time of occurrence/storage
Occurrence IP	
Request IP	
Log Classification	
Log Level	
Occurrence Module	
Success or failure	
Result Code	
Number of posts	

[Table 6-3] Audit Data Types and Selection Criteria

6.1.1.6. FAU_STG.1 Audit data storage location

Hierarchical to No other components.
Dependencies FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.1.1 The TSF shall be able to store generated audit data on the *[the local DBMS*

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

interworking with the TOE].

6.1.1.7. FAU_STG.4 Action in case of possible audit data loss

Hierarchical to	No other components.
Dependencies	FAU_STG.2 Protected audit data storage

FAU_STG.4.1 The TSF shall take [Notification to the authorized administrator, [None]] if the audit data storage exceeds [the inspection threshold set by the authorized administrator (60 ~ 90%, default 70%)].

6.1.1.8. FAU_STG.5 Prevention of audit data loss

Hierarchical to	FAU_STG.4 Action in case of possible audit data loss
Dependencies	FAU_STG.2 Protected audit data storage

FAU_STG.5.1 The TSF shall [*ignore audited events*, [notify the authorized administrator of the audit storage failure by email]] if the audit data storage is full.

6.1.2. Cryptographic Support (FCS)

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

Hierarchical to	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Random number generation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate **data encryption keys (DEK)** in accordance with a specified cryptographic key generation algorithm [Cryptographic algorithm of [Table 6-4]] and specified cryptographic key sizes [Cryptographic key size of [Table 6-4]] that meet the following: [Standard list of [Table 6-4]].

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Standard list	Cryptographic algorithm	Cryptographic key size
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits

[Table 6-4] Cryptographic algorithms used by the TOE to generate user data encryption keys

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Random number generation]
FCS_CKM.6 Timing and event of cryptographic key destruction

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

Standard list	Cryptographic algorithm	Cryptographic key size
TTAK.KO-12.0334-Part1, TTAK.KO-12.0334-Part2	PBKDF(HMAC-SHA256)	256 bits
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits
ISO/IEC 11770-3	ECDH(ECC-P256)	256 bits
ISO/IEC 14888-2	RSA-PSS	2048 bits

[Table 6-5] Cryptographic algorithms used by the TOE to generate TSF data encryption keys

6.1.2.3. FCS_CKM.2 Cryptographic key distribution

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, or
FCS_CKM.5 Cryptographic key derivation]

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Cryptographic key distribution method of [Table 6-6]] that meets the following: [Standard list of [Table 6-6]].

Standard list	Delivering TOE	Receiving TOE	Cryptographic key	Distribution method
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Pub Key (Server)	During the installation procedure Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Priv Key (Agent)	During the installation procedure Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Pub Key (Server)	During the installation procedure Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Priv Key (Agent)	During the installation procedure Distributed offline, then key injected through the TOE interface
ISO/IEC 11770-3, KS X 1213, ISO/IEC 10118-3	EdgeDB Key Server	EdgeDB Key Agent	Audit Key	Hash using the SHA256 cryptographic algorithm, include the hash value, encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver
ISO/IEC 11770-3, KS X 1213,	EdgeDB Log Server	EdgeDB Log Agent	Audit Key	Hash using the SHA256 cryptographic algorithm, include the hash value,

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

ISO/IEC 10118-3				encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver
ISO/IEC 11770-3, KS X 1213, ISO/IEC 10118-3	EdgeDB Key Server	EdgeDB Key Agent	User data Key	Hash using the SHA256 cryptographic algorithm, include the hash value, encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver

[Table 6-6] Cryptographic key distribution method

6.1.2.4. FCS_CKM.5 Cryptographic key derivation

Hierarchical to No other components.

Dependencies [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [Key Encryption Key (KEK)] from [user-entered password, Salt, iteration count] in accordance with a specified key derivation algorithm [Key derivation algorithm of [Table 6-7]] and specified cryptographic key sizes [Cryptographic key size of [Table 6-7]] that meet the following: [Standard list of [Table 6-7]].

Standard list	Key derivation algorithm	Cryptographic key size
TTAK.KO-12.0334-Part1 ~ TTAK.KO-12.0334-Part4	PBKDF(HMAC-SHA256)	256 bits

[Table 6-7] Key derivation algorithms used by the TOE to generate cryptographic keys

6.1.2.5. FCS_CKM.6 Timing and event of 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, or

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.6.1 The TSF shall destroy [cryptographic keys of [Table 6-8]] when *[deletion timing of [Table 6-8]]*.

FCS_CKM.6.2 The TSF shall destroy the cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [Deletion method of [Table 6-8]] that meets the following: [None].

Cryptographic key	TOE	Location	Deletion method	Deletion timing
User data Key	EdgeDB Key Agent	Memory	Zeroization	Immediately after encryption/decryption of user data
Master Key	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
Local Key	EdgeDB Key Server	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	key file	Zeroize the file area, then delete	Upon deletion of the TOE
Audit Key	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
Session Key	EdgeDB Key Server	Memory	Zeroization	Upon session termination
	EdgeDB Log Server	Memory	Zeroization	Upon session termination
	EdgeDB Key Agent	Memory	Zeroization	Upon session termination
	EdgeDB Log Agent	Memory	Zeroization	Upon session termination
Auth Key Pair	EdgeDB Key Server	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Server	Memory	Zeroization	After signature value generation
	EdgeDB Log Server	Memory	Zeroization	After signature value generation
	EdgeDB Key Agent	key file (private key)	Zeroize the file area, then delete	After key injection
	EdgeDB Key Agent	key file (server public key)	Zeroize the file area, then delete	After key injection
	EdgeDB Key Agent	Configuration file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Agent	Memory	Zeroization	After signature value generation
	EdgeDB Log Agent	key file (private key)	Zeroize the file area, then delete	After key injection
	EdgeDB Log Agent	key file (server public key)	Zeroize the file area, then delete	After key injection

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	EdgeDB Log Agent	Configuration file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Log Agent	Memory	Zeroization	After signature value generation
ECDH Private Key	EdgeDB Key Server	Memory	Zeroization	Upon Session Key generation
	EdgeDB Log Server	Memory	Zeroization	Upon Session Key generation
	EdgeDB Key Agent	Memory	Zeroization	Upon Session Key generation
	EdgeDB Log Agent	Memory	Zeroization	Upon Session Key generation

[Table 6-8] Cryptographic Key Destruction Method

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1: The TSF shall perform [Operations list of [Table 6-9]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 6-9]] and cryptographic key sizes [Key size of [Table 6-9]] that meet the following: [Standard list of [Table 6-9]].

Standard list	Cryptographic algorithms	Cryptographic key size	Operation mode	Padding	Operation list
KS X 1213	ARIA	128 bits	CBC	PKCS#5	Encryption· Decryption
KS X 1213	ARIA	256 bits	CBC	PKCS#5	Encryption· Decryption

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	Encryption·Decryption
ISO/IEC 10118-3	SHA256	None	None	None	Hash
ISO/IEC 10118-3	SHA384	None	None	None	Hash
ISO/IEC 10118-3	SHA512	None	None	None	Hash

[Table 6-9] Cryptographic Operation of User Data

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

Hierarchical to No other components.

Dependencies [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Operations list of [Table 6-10]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 6-10]] and cryptographic key sizes [Key size of [Table 6-10]] that meet the following: [Standard list of [Table 6-10]].

Standard list	Cryptographic algorithms	Cryptographic key size	Operation mode	Padding	Operation list
KS X 1213	ARIA	256 bits	CBC	PKCS#5	Encryption·Decryption
ISO/IEC 10118-3	SHA256	None	None	None	Hash
ISO/IEC 9797-2	HMAC-SHA256	256 bits	None	None	Integrity verification of the TSF and TSF data
ISO/IEC 14888-2	RSA-PSS	2048 bits	None	None	Signature generation and verification

[Table 6-10] Cryptographic Operation of TSF Data

6.1.2.8. FCS_RBG.1 Random bit generation (RBG)

Hierarchical to No other components.

Dependencies [FCS_RBG.2 Random bit generation (External seeding) or

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FCS_RBG.3 Random bit generation (Internal seeding – Single source)]
FPT_FLS.1 Failure with preservation of secure state
FPT_TST.1 TSF testing

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [HASH DRBG] in accordance with [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2] after initialization.

FCS_RBG.1.2 The TSF shall use the *TSF entropy source [gettimeofday, clock_gettime, /dev/urandom]* for initialization and seeding.

FCS_RBG.1.3 The TSF shall update the DRBG state by *reseeding* in accordance with [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2] using the *TSF entropy source [gettimeofday, clock_gettime, /dev/urandom]* in the following situations:
o On the condition *[after 2^27-1 random numbers have been collected]*

6.1.2.9. FCS_RBG.3(1) Random bit generation (Internal seeding – Single source)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using the *TSF software-based entropy source* [gettimeofday] with at least [13] bits of min-entropy.

6.1.2.10. FCS_RBG.3(2) Random bit generation (Internal seeding – Single source)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using the *TSF software-based entropy source* [clock_gettime] with at least [20] bits of min-entropy.

6.1.2.11. FCS_RBG.3(3) Random bit generation (Internal seeding – Single source)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using the *TSF software-based entropy source* [/dev/urandom] with at least [280] bits of min-entropy.

6.1.2.12. FCS_RBG.4 Random bit generation (Internal seeding – Multiple sources)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)
FCS_RBG.5 Random bit generation (Combining entropy sources)

FCS_RBG.4.1 The TSF shall be able to seed the DRBG using *[3] TSF software-based entropy source(s)*.

6.1.2.13. FCS_RBG.5 Random bit generation (Combining entropy sources)

Hierarchical to No other components.
Dependencies FCS_RBG.1 Random bit generation (RBG)
[FCS_RBG.2 Random bit generation (External seeding) or
FCS_RBG.3 Random bit generation (Internal seeding – Single source) or
FCS_RBG.4 Random bit generation (Internal seeding – Multiple sources)]

FCS_RBG.5.1 The TSF shall perform [concatenation followed by application of the derivation function (Hash_df)] on the *output from the TSF entropy source(s)* generating at least [256] min-entropy, in order to generate the entropy input for the derivation function defined in [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2], resulting in a minimum of [256] bits of min-entropy.

6.1.3. User Data Protection (FDP)

6.1.3.1. FDP_UDE.1 User data encryption

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

FDP_UDE.1.1 The TSF shall provide a function that can encrypt/decrypt the user data to the TOE user according to the specified [encryption/decryption method by column, [one-way encryption, empty encryption, double encryption]].

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

6.1.3.2. 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].

6.1.4. Identification and Authentication (FIA)

6.1.4.1. 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 [deactivate the identification and authentication function (5 minutes: fixed)].

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

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

FIA_IMA.1.1 The TSF shall perform mutual authentication between [TOE components of [Table 6-11]] using the Authentication protocol of [Table 6-11]] that meets the following [[Standard list of [Table 6-11]].

Standard list	TOE Components	Authentication protocol
None	EdgeDB Key Agent, EdgeDB Key Server	self mutual authentication protocol
None	EdgeDB Log Agent, EdgeDB Log Server	self mutual authentication protocol

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

[Table 6-11] Mutual Authentication Method between TOE Components

6.1.4.3. 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 assigned criteria defined below].

Classification	Description
Compliance requirements	Ensure a length of 9 or more characters
	Include at least one each of digits, uppercase letters (English), lowercase letters (English), and special characters
Prohibited items	Setting a password identical to the user account (ID) is prohibited
	Consecutive repeated input of the same character or digit is prohibited
	Sequential input of consecutive characters or digits on the keyboard is prohibited
	Reuse of the immediately previous password is prohibited

6.1.4.4. 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 user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.5. FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components.
Dependencies No dependencies.

FIA_UAU.4.1 TSF shall prevent reuse of authentication data related to [password authentication method].

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

6.1.4.6. 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 [masking of the entered password so that it cannot be seen on the screen (example: "****"), and feedback that does not reveal the reason for failure when identification and authentication fail] to the user while the authentication is in progress.

6.1.4.7. 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 user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5. Security Management (FMT)

6.1.5.1. 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 functions subject to management" of [Table 6-12]] to ["Administrator" of [Table 6-12]].

Administrator	Function list
Chief Administrator	Modify, delete, and query EdgeDB Key Agent
Chief Administrator	Query, add, modify, and delete DB encryption policy
Chief Administrator	Request to perform integrity checks of the TOE configuration values and the TOE itself

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

[Table 6-12] Security Functions Subject to Management

6.1.5.2. 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 subject to management" of [Table 6-13]] to ["Administrator" of [Table 6-13]].

Administrator	TSF data list
Chief Administrator	Grant privileges to user accounts
Chief Administrator	Add, delete, and modify user IDs
Chief Administrator	Add, delete, and modify passwords of users (Chief Administrator, General Administrator)
Chief Administrator	Set the audit trail threshold for notifying the administrator when audit record loss is predicted
Chief Administrator	Register, delete, modify, and query IP addresses of management terminals (security management access)
Chief Administrator	Query agents – agent version, security policy applied to the agent, agent operating status (enabled/disabled), agent integrity verification result (success/failure)
Chief Administrator	Manage agent security policy
Chief Administrator	Set authentication information for accessing external IT entities (SMTP)
Chief Administrator	Change the default password used to access TOE internal components or external IT entities
Chief Administrator	Set the execution interval of TOE server integrity verification
Chief Administrator	Query identification information of the TOE and TOE components (Key Server, Key Agent, Log Server, Log Agent)
Chief	Set the number of concurrent sessions for monitoring administrators

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Administrator	
Chief Administrator	Query audit records
Chief Administrator	Query the maximum number of allowable failed authentication attempts
Chief Administrator	Query, add, and delete cryptographic keys
General Administrator	Modify own password
General Administrator	Query the audit trail threshold for notifying the administrator when audit record loss is predicted
General Administrator	Query IP addresses of management terminals (security management access)
General Administrator	Query agents – agent version, security policy applied to the agent, agent operating status (enabled/disabled), agent integrity verification result (success/failure)
General Administrator	Query agent security policy
General Administrator	Query authentication information for accessing external IT entities (SMTP)
General Administrator	Query the execution interval of TOE server integrity verification
General Administrator	Query identification information of the TOE and TOE components (Key Server, Key Agent, Log Server, Log Agent)
General Administrator	Query the number of concurrent sessions for monitoring administrators
General Administrator	Query audit records
General Administrator	Query the maximum number of allowable failed authentication attempts
General Administrator	Query cryptographic keys

[Table 6-13] TSF Data Subject to Management

6.1.5.3. FMT_PWD.1 Management of ID and password (Extended)

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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] as follows:
1. [None]
2. [None]

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

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

6.1.5.4. 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: [
a) Management functions specified in FMT_MOF.1
b) Management functions specified in FMT_MTD.1
]

6.1.5.5. FMT_SMR.1 Security roles

Hierarchical to No other components.
Dependencies FIA_UID.1 Timing of identification
FMT_SMR.1.1 TSF shall maintain the roles [Chief Administrator, General Administrator].
FMT_SMR.1.2 TSF shall be able to associate users and their roles **defined in FMT_SMR.1.1.**

6.1.6. Protection of the TSF (FPT)

6.1.6.1. FPT_FLS.1 Failure with preservation of secure state

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Hierarchical to No other components.
Dependencies No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
[
a) Random number generator failure
]

6.1.6.2. 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 TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

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

Hierarchical to No other components.
Dependencies No dependencies.

FPT_PST.1.1 The TSF shall protect [IP address information, Port information, Agent ID, network interface, master password, administrator password, DBMS account information, SMTP password, security alert recipient email for the administrator, threshold and threshold inspection cycle for storing audit data in the local DB, maximum number of failed authentication attempts, maximum number of concurrent general administrator sessions, self-test, forgery/falsification and process-check audit cycle and audit time, communication cycle of the Key Agent, validity period of the administrator password and master password, access control policy, DB encryption policy, audit data stored as files, cryptographic keys] stored in containers controlled by the TSF from unauthorized *disclosure*.

6.1.6.4. FPT_TST.1 TSF testing

Hierarchical to No other components.
Dependencies No dependencies.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FPT_TST.1.1 The TSF shall run a suite of the following self-tests [*during initial start-up, periodically during normal operation*] to demonstrate the correct operation of *[the TSF]: [self-test items per TOE of [Table 7-22]]*.

FPT_TST.1.2 The TSF shall provide authorized **administrators** the capability to verify the integrity of *[TSF data integrity verification items per TOE of [Table 7-23]]*.

FPT_TST.1.3 The TSF shall provide authorized **administrators** the capability to verify the integrity of *[TSF integrity verification items per TOE of [Table 7-24]]*.

6.1.7. TOE Access (FTA)

6.1.7.1. 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 belong to the same user according to the rules: [the maximum number of concurrent sessions is limited to 1 for users with the same privilege and for the same user, [the maximum number of concurrent sessions for general administrators is limited to 5~100.]]

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

6.1.7.2. FTA_SSL.3 TSF-initiated termination

Hierarchical to No other components.
Dependencies FMT_SMR.1 Security roles

FTA_SSL.3.1 The TSF shall terminate an interactive session after [10 minutes].

6.1.7.3. FTA_TSE.1(1) TOE session establishment

Hierarchical to No other components.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

Dependencies No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **the administrator's management access session** establishment based on [access IP, *None*].

6.1.8. Trusted Path/Channels (FTP)

6.1.8.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to No other components.
Dependencies No dependencies.

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [the function of the chief administrator to send email to authorized administrators].

6.2. Security Assurance Requirements

The security assurance requirements of this Security Target consist of the assurance components of Common Criteria Part 3, and the evaluation assurance level is EAL1+. The following table summarizes the assurance components.

Security Assurance Class	Security Assurance Component	
Security Target Evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance Claim
	ASE_SPD.1	Security Problem Definition
	ASE_OBJ.1	Security Objectives for the Operational Environment
	ASE_ECD.1	Extended Components Definition
	ASE_REQ.1	Direct rationale security requirements

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 6-14] Security Assurance Requirements

6.2.1. Security Target Evaluation

6.2.1.1. ASE_INT.1 ST introduction

Dependencies No dependencies.

Developer action elements

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

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

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

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

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

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

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

ASE_INT.1.7C For a multi-assurance ST, the TOE overview shall describe the TSF organization in terms of the sub-TSFs defined in the PP-Configuration to which the ST claims conformance to.

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

ASE_INT.1.9C The TOE description shall describe the logical scope of the TOE.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.

6.2.1.2. ASE_CCL.1 Conformance claims

Dependencies ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Direct rationale 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 identify the edition 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 a PP-Configuration, or all PPs and security requirement packages to which the ST claims conformancepackages 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 shall describe any conformance of the ST to a PP as PP-Conformant.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

claimed.

ASE_CCL.1.9C 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 PP-Configuration, PPs and any functional packages for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PP-Configuration, PPs, and any functional package for which conformance is being claimed.

ASE_CCL.1.11C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PP-Configuration, PPs, and any functional packages for which conformance is being claimed.

ASE_CCL.1.12C The conformance claim for PP(s) or a PP-Configuration shall be exact, strict, or demonstrable, or a list of conformance types.

ASE_CCL.1.13C If the conformance claim identifies a set of Evaluation methods and Evaluation activities derived from CEM work units that shall be used to evaluate the TOE then this set shall include all those that are included in any package, PP, or PP-Module in a PP-Configuration to which the ST claims conformance, and no others.

Evaluator action elements

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

6.2.1.3. ASE_SPD.1 Security problem definition

Dependencies No dependencies.

Developer action elements

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

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

6.2.1.4. ASE_OBJ.1 Security objectives for the operational environment

Dependencies ASE_SPD.1 Security problem definition

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives for the operational environment.

ASE_OBJ.1.2D The developer shall provide a security objectives rationale for the operational environment.

Content and presentation elements

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

ASE_OBJ.1.2C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.1.3C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements

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

6.2.1.5. ASE_ECD.1 Extended components definition

Dependencies No dependencies.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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 may 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.

6.2.1.6. ASE_REQ.1 Direct rationale security requirements

Dependencies ASE_ECD.1 Extended components definition
ASE_SPD.1 Security problem definition
ASE_OBJ.1 Security objectives for the operational environment

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.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

ASE_REQ.1.2C For a single-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE. The sets of SARs shall be consistent with the PPs or PP-Configuration to which the ST claims conformance.

ASE_REQ.1.3C For a multi-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE and the sets of SARs that apply to each sub-TSF. The sets of SARs shall be consistent with the multi-assurance PP-Configuration to which the ST claims conformance.

ASE_REQ.1.4C 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.1.5C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.6C All operations shall be performed correctly.

ASE_REQ.1.7C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.8C The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) counter all threats for the TOE.

ASE_REQ.1.9C The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operationsl environment) enforce all OSPs.

ASE_REQ.1.10C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.1.11C The statement of security requirements shall be internally consistent.

ASE_REQ.1.12C If the ST defines sets of SARs that expand the sets of SARs of the PPs or PP-Configuration it claims conformance to, the security requirements rationale shall include an assurance rationale that justifies the consistency of the extension and provides a rationale for the disposition of any Evaluation methods and Evaluation activities identified in the conformance statement that are affected by the extension of the sets of SARs.

Evaluator action elements

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

6.2.1.7. ASE_TSS.1 TOE summary specification

Dependencies ASE_INT.1 ST introduction

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

ASE_REQ.1 Direct rationale 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.

6.2.2. Development

6.2.2.1. 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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.

6.2.3. Guidance documents

6.2.3.1. 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 shell 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 controls 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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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

6.2.3.2. 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.

6.2.4. Life-cycle support

6.2.4.1. ALC_CMC.1 Labelling 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 unique reference for the TOE.

Content and presentation elements

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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Evaluator action elements

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

6.2.4.2. 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.

6.2.5. Tests

6.2.5.1. 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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.

6.2.5.2. 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.

6.2.6. Vulnerability assessment

6.2.6.1. 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

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

The security functional requirements rationale demonstrates the following.

▷Each threat and organizational security policy is addressed by at least one security functional requirement.

▷Each security functional requirement traces to at least one threat or organizational security policy.

Security Functional Requirements	T. SESSION_HIJACK	T. RETRY_AUTH_ATTEMPT	T. IMPERSONATION	T. REPLAY	T. WEAK_PASSWORD	T. UNAUTHORIZED_INFO_LEAK	T. STORED_DATA_LEAKAGE	T. TRANSMISSION_DATA_DAMAGE	T. WEAK_CRYPTO_PROTOCOLS	T. TSF_COMPROMISE	P. AUDIT	P. SECURE_OPERATION	P. CRYPTO_STRENGTH
FAU_ARP.1										O			
FAU_GEN.1											O		
FAU_SAA.										O			

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

1												
FAU_SAR.1										O		
FAU_SAR.3										O		
FAU_STG.1										O		
FAU_STG.4										O		
FAU_STG.5										O		
FCS_CKM.1(1)						O						O
FCS_CKM.1(2)							O	O	O			O
FCS_CKM.2						O	O	O	O			O
FCS_CKM.5						O	O	O	O			O
FCS_CKM.6						O	O	O	O			O
FCS_COP.1(1)						O						O
FCS_COP.1(2)							O	O	O			O
FCS_RBG.1						O	O	O	O			O
FCS_RBG.3(1)						O	O	O	O			O
FCS_RBG.3(2)						O	O	O	O			O

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

FCS_RBG.3(3)						O	O	O	O				O
FCS_RBG.4						O	O	O	O				O
FCS_RBG.5						O	O	O	O				O
FDP_UDE.1						O							
FDP_RIP.1						O							
FIA_AFL.1		O	O							O			
FIA_IMA.1			O										
FIA_SOS.1					O								
FIA_UAU.2			O							O			
FIA_UAU.4			O	O						O			
FIA_UAU.7			O		O					O			
FIA_UID.2			O							O			
FMT_MOF.1										O		O	
FMT_MTD.1										O		O	
FMT_PWD.1					O					O		O	
FMT_SMF.1										O		O	
FMT_SMR.1										O		O	

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

FPT_FLS.1						O	O	O	O				O
FPT_ITT.1								O					
FPT_PST.1							O						
FPT_TST.1						O	O	O	O	O			O
FTA_MCS.2	O												
FTA_SSL.3	O												
FTA_TSE.1(1)	O												
FTP_ITC.1								O					

[Table 6-15] Correspondence between Security Problem Definition and Security Functional Requirements

T.SESSION_HIJACK	FTA_MCS.2, FTA_SSL.3, FTA_TSE.1(1)

FTA_MCS.2 responds to T.SESSION_HIJACK by restricting concurrent access to the TOE with the same user account or the same privileges.

FTA_SSL.3 responds to T.SESSION_HIJACK by ensuring session locking or session termination for interactive sessions after a period of inactivity of authorized users.

FTA_TSE.1(1) responds to T.SESSION_HIJACK by ensuring that it determines whether to establish an authorized user access session based on IP, etc.

T.RETRY_AUTH_ATTEMPT	FIA_AFL.1

FIA_AFL.1 responds to T.RETRY_AUTH_ATTEMPT by defining the number of failed authentication attempts by authorized administrators and general users and ensuring the ability to take responsive action when the defined number is reached.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved I Confidential

T.IMPERSONATION	FIA_AFL.1, FIA_IMA.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

FIA_AFL.1 responds to T.IMPERSONATION by defining the number of failed authentication attempts by authorized administrators and ensuring the ability to take responsive action when the defined number is reached.

FIA_IMA.1 responds to T.IMPERSONATION by ensuring that mutual authentication is performed between TOE components.

FIA_UAU.2 and FIA_UAU.4 respond to T.IMPERSONATION by ensuring that administrators and general users attempting to access the TOE are successfully authenticated.

FIA_UAU.7 responds to T.IMPERSONATION by ensuring that only masked values are output to or hidden from the user while authentication is in progress, and that no feedback on the reason for failure is provided upon authentication failure.

FIA_UID.2 responds to T.IMPERSONATION by ensuring that administrators and general users attempting to access the TOE are successfully identified.

T.REPLAY	FIA_UAU.4

FIA_UAU.4 responds to T.REPLAY by ensuring the ability to prevent the reuse of authentication data.

T.WEAK_PASSWORD	FIA_SOS.1, FIA_UAU.7, FMT_PWD.1

FIA_UAU.7 responds to T.WEAK_PASSWORD by ensuring that only masked values are output to or hidden from the user while authentication is in progress.

FIA_SOS.1 responds to T.WEAK_PASSWORD by verifying that the password complexity rules are satisfied.

FMT_PWD.1 responds to T.WEAK_PASSWORD by ensuring the ability to force a change of the default password when the authorized administrator first connects

T.UNAUTHORIZED_INFO_LEAK	FCS_CKM.1(1), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(1), FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3),

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	FCS_RBG.4, FCS_RBG.5, FDP_UDE.1, FDP_RIP.1, FPT_FLS.1, FPT_TST.1

FCS_CKM.1(1), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 respond to T.UNAUTHORIZED_INFO_LEAK by ensuring that a cryptographic key is created and distributed according to a secure cryptographic algorithm and key length when encrypting and decrypting important user information stored in the database.

FCS_CKM.6 responds to T.UNAUTHORIZED_INFO_LEAK by ensuring that cryptographic keys are destroyed according to the specified cryptographic key destruction method after encrypting and decrypting important user information stored in the database.

FCS_COP.1(1) responds to T.UNAUTHORIZED_INFO_LEAK by ensuring that cryptographic operations are performed according to the specified secure algorithm and cryptographic key length when encrypting and decrypting important user information stored in the database.

FDP_RIP.1 responds to T.UNAUTHORIZED_INFO_LEAK by ensuring that all original user data is deleted after the encrypting and decrypting important user information stored in the database

FDP_UDE.1 responds to T.UNAUTHORIZED_INFO_LEAK by ensuring that encryption and decryption occur when an authorized user stores important information in the database.

T.STORED_DATA_LEAKAGE	FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, FPT_PST.1, FPT_TST.1

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 respond to T.STORED_DATA_LEAKAGE by ensuring that a cryptographic key is created and distributed according to a secure cryptographic algorithm and key length when encrypting stored data.

FCS_CKM.6 responds to T.STORED_DATA_LEAKAGE by ensuring that the cryptographic keys and their related information are destroyed according to the specified cryptographic key destruction method upon completion of storage data encryption.

FCS_COP.1(2) responds to T.STORED_DATA_LEAKAGE by ensuring that cryptographic operations are

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

performed according to the specified secure algorithm and specified cryptographic key length when encrypting stored data.

FPT_PST.1 responds to T.STORED_DATA_LEAKAGE by ensuring that the stored TSF data is protected from being leaked by means of encryption, access control, etc.

T.TRANSMISSION_DATA_DAMAGE	FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, FPT_ITT.1, FPT_TST.1, FTP_ITC.1

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1 and FPT_TST.1 respond to T.TRANSMISSION_DATA_DAMAGE by ensuring that a cryptographic key is created and distributed according to a secure cryptographic algorithm and key length during cryptographic communication.

FCS_CKM.6 responds to T.TRANSMISSION_DATA_DAMAGE by ensuring that cryptographic keys and their related information are destroyed according to the specified cryptographic key destruction method at the end of cryptographic communication.

FCS_COP.1 responds to T.TRANSMISSION_DATA_DAMAGE by ensuring that cryptographic operations are performed according to the specified secure algorithm and specified cryptographic key length during cryptographic communication.

FPT_ITT.1 responds to T.TRANSMISSION_DATA_DAMAGE by ensuring the confidentiality and integrity of transmission data between TOE components.

FTP_ITC.1 responds to T.TRANSMISSION_DATA_DAMAGE by ensuring the confidentiality and integrity of transmission data between the TOE and external IT entities.

T.WEAK_CRYPTO_PROTOCOLS	FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, FPT_TST.1

FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 respond to T.WEAK_CRYPTO_PROTOCOLS by ensuring that the cryptographic key is created and distributed according to the standard

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

cryptographic algorithm and key length with a security strength of 112 bits or more when encrypting transmission data.

FCS_CKM.6 responds to T.WEAK_CRYPTO_PROTOCOLS by ensuring that the cryptographic key is destroyed according to the specified destruction method.

FCS_COP.1(2) responds to T.WEAK_CRYPTO_PROTOCOLS by ensuring that cryptographic operations are performed according to the standard cryptographic algorithm and cryptographic key length with a security strength of 112 bits or more when encrypting transmission data.

T.TSF_COMPROMISE	FAU_ARP.1, FAU_SAA.1, FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2, FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1, FPT_TST.1

FAU_ARP.1 responds to T.TSF_COMPROMISE by ensuring the ability to take response actions when detecting security violations such as TOE integrity compromise, etc.

FAU_SAA.1 responds to T.TSF_COMPROMISE by ensuring the ability to review audited events to point out security violations, such as TOE integrity compromise.

FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, and FIA_UID.2 respond to T.TSF_COMPROMISE by allowing access to the TOE only after successful user identification and authentication, ensuring the blocking of bypass access by threat agents.

FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, and FMT_SMR.1 respond to T.TSF_COMPROMISE by dividing authorized user roles into administrator and end user when accessing and configuring management functions, and by providing security policies and functions based on those roles to ensure blocking of unauthorized access by threat agents.

FPT_TST.1 responds to T.TSF_COMPROMISE by ensuring that the TOE agents or clients can recover modified information

P.AUDIT	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FAU_STG.5

FAU_GEN.1 satisfies P.AUDIT by ensuring that audit records are generated for auditable events such as the startup/termination of the audit function and the success/failure of the identification and authentication of the administrator.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FAU_SAR.1 satisfies P.AUDIT by providing the authorized administrator with the ability to retrieve audit records and ensuring that the audit records are presented in a manner suitable for the administrator to interpret the information.

FAU_SAR.3 satisfies P.AUDIT by providing a selective audit review function based on logical relationship criteria for audit data.

FAU_STG.1 satisfies P.AUDIT by providing the ability to store audit data in local storage or transmit it to an external IT entity for storage in real time using a trusted channel for the TOE server.

FAU_STG.4 satisfies P.AUDIT by ensuring that appropriate response actions are taken if the audit trail on the TOE server exceeds the storage limit.

FAU_STG.5 satisfies P.AUDIT by ensuring the ability to take appropriate response actions when the audit trail of the TOE server is full.

P.SECURE_OPERATION	FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1

FMT_MOF.1 satisfies P.SECURE_OPERATION by ensuring that only authorized users have the ability to manage security functions.

FMT_MTD.1 satisfies P.SECURE_OPERATION by ensuring that only authorized users have the ability to manage the TSF data.

FMT_PWD.1 satisfies P.SECURE_OPERATION by ensuring that only authorized administrators have the ability to manage the combination rules and length of IDs and passwords, and by providing functions such as changing passwords when authorized administrators first access.

FMT_SMF.1 satisfies P.SECURE_OPERATION by requiring management functions such as security functions to be performed by the TSF, the TSF data, etc. to be specified.

FMT_SMR.1 satisfies P.SECURE_OPERATION by ensuring that authorized roles related to security management are specified.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

P.CRYPTO_STRENGTH	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1(1), FCS_COP.1(2), FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, FPT_TST.1

FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 satisfy P.CRYPTO_STRENGTH by ensuring that the cryptographic keys required for standard cryptographic algorithms with a security strength of 112 bits or more are securely generated and distributed during data encryption.

FCS_COP.1(1) and FCS_COP.1(2) satisfies P.CRYPTO_STRENGTH by ensuring that cryptographic operations are performed according to standard cryptographic algorithms with a security strength of 112 bits or more and the cryptographic key length during data encryption.

6.3.2. Security Assurance Requirements Rationale

The evaluation assurance level of this Security Target is selected as EAL1+(ATE_FUN.1).
EAL1 can be applied in cases where a certain degree of trust in correct operation is required, but the threat to security is not serious. If EAL1 is developed according to the development methodology commonly applied by the developer, no additional effort is required from the developer to prepare the evaluation submissions. In other words, there is no need to invest more money or time to prepare for the evaluation. EAL1 provides a basic level of assurance by analyzing the security functional requirements included in the limited security target using function and interface specifications and documentation to understand security behavior. This analysis is supported by independent testing of the TSF and searching for potential vulnerabilities in the public domain(functional testing and penetration testing).
EAL1 does not require evidence of testing conducted by the developer based on functional specifications, but ATE_FUN.1 was added in this PP to allow the developer to independently test whether the TSF has been implemented correctly and whether defects have occurred, etc. and document the results.

6.3.3. Dependencies of Security Functional Requirements

The following table shows the dependencies of the security functional requirements.

No.	Security Functional Requirements	Dependencies	Reference No.

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

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.1	FAU_GEN.1	2
		FTP_ITC.1	Rationale (2)
7	FAU_STG.4	FAU_STG.2	Rationale (3)
8	FAU_STG.5	FAU_STG.2	Rationale (3)
9	FCS_CKM.1(1)	[FCS_CKM.2 OR FCS_CKM.5 OR FCS_COP.1]	11, 12, 14
		[FCS_RBG.1 OR FCS_RNG.1]	16
		FCS_CKM.6	13
10	FCS_CKM.1(2)	[FCS_CKM.2 OR FCS_CKM.5 OR FCS_COP.1]	11, 12, 15
		[FCS_RBG.1 OR FCS_RNG.1]	16
		FCS_CKM.6	13
11	FCS_CKM.2	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5]	9, 10, 12
12	FCS_CKM.5	[FCS_CKM.2 OR FCS_COP.1]	11, 14, 15
		FCS_CKM.6	13
13	FCS_CKM.6	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5]	9, 10, 12
14	FCS_COP.1(1)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5]	9, 12
		FCS_CKM.6	13
15	FCS_COP.1(2)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5]	10, 12
		FCS_CKM.6	13
16	FCS_RBG.1	[FCS_RBG.2 OR FCS_RBG.3]	17, 18, 19
		FPT_FLS.1	36
		FPT_TST.1	39
17	FCS_RBG.3(1)	FCS_RBG.1	16
18	FCS_RBG.3(2)	FCS_RBG.1	16
19	FCS_RBG.3(3)	FCS_RBG.1	16
20	FCS_RBG.4	FCS_RBG.1	16

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

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

[Table 6-16] Rationale for the Dependencies

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1, but OE.TIME_STAMP ensures that a reliable time stamp is provided in the operational environment of the TOE, so the dependency is satisfied.

Rationale (2): FAU_STG.1 has a dependency on FTP_ITC.1, but the TOE does not transmit the

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential

generated audit data to an external IT entity and instead stores it in the local DBMS linked with the TOE, so the dependency does not need to be satisfied.
Rationale (3): FAU_STG.4 and FAU_STG.5 have a dependency on FAU_STG.2, but OE.AUDIT_PROTECTION ensures that audit data is protected from unauthorized deletion or modification by the DBMS installed on the operating system of the TOE, so the dependency is satisfied.

6.3.4. Dependencies of 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.

7. TOE Summary Specification

This chapter describes the security functions of the TOE in detail and explains how the TOE satisfies the security requirements. The following are all the security functions provided by the TOE that are described in the TOE Summary Specification.

Security Functional Class	Security Functional Component	
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.1	Audit data storage location
	FAU_STG.4	Action in case of possible audit data loss
	FAU_STG.5	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (User data encryption)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	FCS_CKM.5	Cryptographic key derivation
	FCS_CKM.6	Timing and event of cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1	Random bit generation (RBG)
	FCS_RBG.3(1)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.3(2)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.3(3)	Random bit generation (Internal seeding - Single source)
	FCS_RBG.4	Random bit generation (Internal seeding - Multiple sources)
	FCS_RBG.5	Random bit generation (Combining entropy sources)
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	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User authentication before any action
Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	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_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1	Basic protection of stored TSF data (Extended)
	FPT_TST.1	TSF self-test
TOE Access	FTA_MCS.2	Per user attribute limitation on multiple concurrent

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

(FTA)		sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1(1)	TOE session establishment
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel

[Table 7-1] List of TOE Security Functions

7.1. Security Audit

This section describes the security audit functions provided by the TOE and how those functions satisfy the declared security functional requirements.

7.1.1. Audit data generation

The TOE components (EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, and EdgeDB Log Agent) generate audit data in the form of temporary files; the data is collected by the EdgeDB Log Agent installed on the same physical server, transmitted to the EdgeDB Log Server, and stored in the local DBMS linked with the TOE. Temporary audit data files whose transmission has been completed are deleted by the EdgeDB Log Agent after one day. (FAU_GEN.1)

Security functional component	Auditable event	Additional audit record contents
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.4	Actions taken due to exceeding a threshold	
FAU_STG.5	Actions taken due to audit storage failure	
FCS_CKM.1	Success and failure of cryptographic key generation	
FCS_CKM.2	Success and failure of the activity (only applicable to key distribution related to user data encryption/decryption)	
FCS_CKM.6	Success and failure of the activity (only applicable to key destruction related to user data encryption/decryption)	

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FCS_COP.1	Success and failure of cryptographic operation, type of cryptographic operation	
FDP_UDE.1	Success and failure of user data encryption/decryption	
FIA_AFL.1	Performance of response actions upon reaching the user authentication attempt threshold and the result (success, failure)	
FIA_IMA.1	Success/failure of mutual authentication, change of the authentication protocol	
FIA_UAU.2	Timing of authentication	
FIA_UAU.4	Authentication failure due to detection of an attempt to reuse authentication data	
FMT_MOF.1	All modifications in the behavior 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 management functions	
FMT_SMR.1	Changes to the user group with divided roles	
FPT_TST.1	Execution of the TSF self-test and the test results, performance and result (success, failure) of integrity verification of TOE components	TSF data or executable code modified in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions Response actions upon detection of duplicate login with the same account Performance and result (success, failure) of blocking duplicate connections	
FTA_SSL.3	Performance and result (success, failure) of session termination of the user	
FTA_TSE.1	Blocking of the IP address of the administrative terminal connection	
FTP_ITC.1	All attempts to use the trusted channel function	

[Table 7-2] Auditable Events of the TOE

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

All TOE components generate audit data for the auditable events in [Table 7-2], including the audit record content shown in [Table 7-3]. (FAU_GEN.1)

audit record contents	Description
Date and time of occurrence	Time at which the auditable event occurred
Storage date/time	Time at which the audit data was stored in the local DB
Occurrence IP	IP of the server on which the TOE component where the auditable event occurred is running
Request IP	IP of the subject that caused the auditable event in the TOE component (Not recorded if the subject that caused the auditable event is the same as the TOE component where the auditable event occurred)
Log Classification	Encryption: events related to encryption operations on user data Decryption: events related to decryption operations on user data Audit: all auditable events other than user data encryption/decryption and operation Operation: events related to the operational status of TOE components
Log Level	INFO: general events ERROR: events in which a problem occurred WARNING: events in which a problem may occur
Occurrence Module	Key-Server: events that occurred in the EdgeDB Key Server Key-Agent: events that occurred in the EdgeDB Key Agent Log-Server: events that occurred in the EdgeDB Log Server Log-Agent: events that occurred in the EdgeDB Log Agent Library: events that occurred in the Library provided by the EdgeDB Key Agent
Process	Process in which the auditable event occurred
Success or failure	Whether the operation was normal
Execution administrator ID	ID of the administrator who caused the auditable event (Recorded only when the auditable event was caused by an authorized administrator)
Execution Object	Function in which the auditable event occurred
Subject of Execution	Subject that performed the execution object
Classification for	Classification of the detailed function of the execution object

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Execution	(Recorded only when the auditable event was caused by an authorized administrator)
Result Code	Result code of the auditable event (6 digits) (I: INFO, E: ERROR, 0: library) + classification code (5 digits)
Result Message	Message about the auditable event

[Table 7-3] Audit Event Record Data

For the auditable events in [Table 7-2], audit data is generated that includes the additional audit record content in [Table 7-4] in addition to the audit record content in [Table 7-3]. (FAU_GEN.1)

Auditable event	Additional audit record content
All modifications to the values of TSF data	Modified values of TSF data
Execution and result (success, failure) of the TOE server self-test	Failed security function
Performance and result (success, failure) of integrity verification of TOE components	Component that failed the integrity check

[Table 7-4] Additional Audit Record Content for Specific Audit Events

※ **Related security functional requirements**
- FAU_GEN.1

7.1.2. Audit Review

Audit data stored in the local DB audit repository can be viewed by an authorized administrator on the administrator page.

The EdgeDB Log Agent, which resides on the same physical server as the TOE component that generated the audit data files, collects the audit data files generated by all TOE components every 10 seconds and transmits the entire audit data to the EdgeDB Log Server in units of 20 audit data items, and the EdgeDB Log Server stores the data in the local DB on the Management Server. When an authorized administrator requests a query of the audit data stored in the local DB through the security management interface provided by the EdgeDB Key Server, the EdgeDB Key Server queries the audit data stored in the local DB and provides review and selective review of the audit data collected from all TOE components through the security management interface. Selective review of the collected audit data is performed using the selection criteria in [Table 7-5]. (FAU_SAR.1,

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

FAU_SAR.3)

Selection criteria (AND)	Permitted functions
Date and time of occurrence	Selective search and sorting in ascending/descending order based on date and time of occurrence/storage
Occurrence IP	
Request IP	
Log Classification	
Log Level	
Occurrence Module	
Success or failure	
Result Code	
Number of posts	

[Table 7-5] Selective Review Criteria for Audit Data

※ Related security functional requirements
- FAU_SAR.1, FAU_SAR.3

7.1.3. Potential Violation Analysis and Response

The audit data generated by all TOE components as described in FAU_GEN.1 is forwarded by the EdgeDB Log Agent to the EdgeDB Log Server, and the EdgeDB Log Server stores it in the local DB. Every 30 seconds, the EdgeDB Key Server queries the local DB for the occurrence of the potential violation audit events defined in FAU_SAA.1, namely consecutive authentication failures of the chief administrator and general administrators, self-test failures of the validated cryptographic module and of the TOE itself, integrity verification failures of cryptographic keys and of the TOE itself, and audit log storage failures; the Log Server queries immediately upon receiving an integrity violation audit event among the auditable events of FPT_TST.1. (FAU_SAA.1)

When a potential violation audit event is found, the EdgeDB Key Server and EdgeDB Log Server perform the response action corresponding to that audit event in [Table 7-6]. (FAU_ARP.1)

SFR	Potential violation audit event	Response action
FIA_AFL.1	Audit event of exceeding the allowed number of authentication failures (5)	Administrator menu access is blocked Notification by email, through the EdgeDB Key Server, to the authorized administrator designated

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

		by the chief administrator
FPT_TST.1	Integrity violation audit event	Notification by email, through the EdgeDB Log Server, to the authorized administrator designated by the chief administrator
FPT_TST.1	Validated cryptographic module's self-test failure event	Notification by email, through the EdgeDB Key Server and EdgeDB Log Server, to the authorized administrator designated by the chief administrator
FPT_TST.1	Major security function process's verification failure event	Notification by email, through the EdgeDB Key Server, to the authorized administrator designated by the chief administrator
FAU_STG.4	Usage of the local DB storing audit data exceeds the threshold	Notification by email, through the EdgeDB Key Server, to the authorized administrator designated by the chief administrator
FAU_STG.5	Audit log storage failure	Notification by email, through the EdgeDB Log Server, to the authorized administrator designated by the chief administrator

[Table 7-6] Examples of Potential Violation Audit Events and Response Actions

※ **Related security functional requirements**
- FAU_ARP.1, FAU_SAA.1,

7.1.4. Protection of Audit Data and Response to Possible Audit Data Loss

The audit data generated by the EdgeDB Key Server, EdgeDB Key Agent, and EdgeDB Log Agent is stored as files in the temporary audit log storage directory of each component and then transmitted to the EdgeDB Log Server through the EdgeDB Log Agent, and the EdgeDB Log Server stores the received audit data in the local DBMS linked with the TOE. (FAU_STG.1)

The EdgeDB Log Server checks the usage of the local DB that stores audit data every 60 seconds. The maximum capacity of the audit data repository is the total capacity of the disk on which the data directory of the local DB is located, and the usage is calculated as the ratio (%) of the size of the audit data stored in the local DB to the maximum capacity. (FAU_STG.4, FAU_STG.5)

When the local DB usage checked by the EdgeDB Log Server exceeds the specified limit, a function is provided to notify the authorized administrator designated by the chief administrator

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

of the relevant details by email. The specified limit is set to 70% by default and can be set by the chief administrator from 60% to 90%. (FAU_STG.4)

When the local DB usage checked by the EdgeDB Log Server exceeds the saturation threshold of 95%, a function is provided to notify the authorized administrator designated by the chief administrator of the relevant details by email. In addition, when the local DB usage is saturated, audit data generated thereafter is ignored and not stored in the local DB. (FAU_STG.5)

※ **Related security functional requirements**
- FAU_STG.1, FAU_STG.4, FAU_STG.5

7.2. Cryptographic Support

The cryptographic support functions of the TOE are provided through the TOE's internal operation processes, or through the cryptographic keys generated by the chief administrator and the DB encryption policy, in order to protect TSF data. Cryptographic operations according to the DB encryption policy generated by the chief administrator are performed through the library module in plug-in or API form provided by the EdgeDB Key Agent, and the keys are safely destroyed using the zeroization function immediately after use. All cryptographic support functions are performed using the approved cryptographic algorithms of the validated cryptographic module, whose stability and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP), as shown in [Table 7-7].

Classification		Description
Validated cryptographic module name		EdgeCrypto v4.2
Developer		ITCEN PNS Co., Ltd.
Validation number		CM-299-2031.7
Validation date		2026.07.13
Expiration date		2031.07.13
Library name	Linux	libEdgeCrypto.so

[Table 7-7] Validated Cryptographic Module

7.2.1. Cryptographic Key Generation

When the chief administrator generates a cryptographic key on the administrator page, the EdgeDB

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Key Server generates the User data Key, which is the key for encrypting user data, with the cryptographic key length in [Table 7-8], using the approved cryptographic algorithm of the validated cryptographic module in [Table 7-8], whose stability and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP), in accordance with the standard list in [Table 7-8]. When the generated cryptographic key is used in a 128-bit cryptographic algorithm, only the first 128 bits are used. (FCS_CKM.1(1))

Standard list	Validated cryptographic module's approved cryptographic algorithm	Cryptographic key size	Usage
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits	User data encryption/decryption

[Table 7-8] User Data Cryptographic Key Generation

To encrypt TSF data such as cryptographic keys and security policies, keys are generated using the approved cryptographic algorithm of the validated cryptographic module, whose stability and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP). In addition, the random number generation and the HMAC-SHA256 algorithm used by the self-implemented PBKDF2 algorithm also use the approved algorithms of the validated cryptographic module. These TSF data encryption keys are generated using the cryptographic algorithms in [Table 7-9], which comply with the standard list in [Table 7-9], with the cryptographic key lengths in [Table 7-9]. (FCS_CKM.1(2))

Standard list	Cryptographic algorithms	Cryptographic key size	Usage	Key type	Key generating entity
TTAK.KO-12.0334-Part2	PBKDF(HMAC-SHA256)	256 bits	Key encryption/decryption	Master Key	EdgeDB Key Server EdgeDB Log Server EdgeDB Key Agent EdgeDB Log Agent
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits	TSF data encryption/decryption	Local Key	EdgeDB Key Server EdgeDB Key Agent EdgeDB Log Agent

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits	TSF and TSF data integrity value generation	Audit Key	EdgeDB Key Server
ISO/IEC 11770-3	ECDH(ECC-P256)	256 bits	Session Key generation	Session Key	EdgeDB Key Server EdgeDB Log Server EdgeDB Key Agent EdgeDB Log Agent
ISO/IEC 14888-2	RSA-PSS	2048 bits	Auth Key Pair generation, signing, and signature verification	Auth Key Pair	EdgeDB Key Server

[Table 7-9] TSF Data Cryptographic Key Generation

※ Related security functional requirements
- FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1

7.2.2. Cryptographic key derivation

The TOE derives the Master Key, which is a Key Encryption Key (KEK), from the Master Password entered by the chief administrator. Key derivation uses the PBKDF (HMAC-SHA256) algorithm conforming to the standard list in [Table 6-7], and derives a 256-bit cryptographic key using the Master Password, a Salt value, and an iteration count as inputs. The Salt value is generated with a length of 128 bits by the HASH-DRBG-SHA512 algorithm using the approved random bit generator of the validated cryptographic module, and the iteration count is set to 1024. (FCS_CKM.5)

※ **Related security functional requirements**
- FCS_CKM.5

7.2.3. Cryptographic key distribution

The EdgeDB Key Server and EdgeDB Log Server distribute the cryptographic keys required by each component so that the corresponding TOE can properly protect TSF data and user data. All distributed cryptographic keys except the Auth Key and Session Key are distributed after the self-

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

implemented mutual authentication mechanism has been performed, and the Auth Key and Salt value are distributed during the initial installation process.

The Auth Pub Key for Server and the Auth Priv Key for Agent are distributed offline from the EdgeDB Key Server in the form of key files. In this case, the Auth Priv Key is distributed as a key file encrypted by the EdgeDB Key Server with the Master Key. The cryptographic keys in [Table 7-10] are distributed from the sender TOE in [Table 7-10] to the corresponding receiver TOE in [Table 7-10] through the distribution method in [Table 7-10]. The key file in which the distributed cryptographic key is recorded is placed in the folder containing the configuration file of the TOE component that received the cryptographic key, and key distribution is completed by performing the key injection procedure in that TOE component. The distributed keys are used by each Agent to perform mutual authentication with the EdgeDB Key Server and EdgeDB Log Server. (FCS_CKM.2)

Standard list	Delivering TOE	Receiving TOE	Cryptographic key	Distribution method
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Pub Key (Server)	During the installation procedure of the receiver TOE, Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Priv Key (Agent)	During the installation procedure of the receiver TOE, Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Pub Key (Server)	During the installation procedure of the receiver TOE, Distributed offline, then key injected through the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Priv Key (Agent)	During the installation procedure of the receiver TOE,

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

				Distributed offline, then key injected through the TOE interface

[Table 7-10] Auth Key Pair Distribution

The Audit Key is distributed after the self-implemented mutual authentication mechanism has been fully performed, and the User data Key is delivered together with the security policy when the security policy is delivered to the EdgeDB Key Agent, according to the cryptographic key set in the security policy by the authorized chief administrator. The sender TOE in [Table 7-11] distributes the cryptographic key in [Table 7-11] to the receiver TOE in [Table 7-11] through the distribution method in [Table 7-11], which uses the approved cryptographic algorithm of the validated cryptographic module whose stability and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP). (FCS_CKM.2)

Standard list	Delivering TOE	Receiving TOE	Cryptographic key	Distribution method
ISO/IEC 11770-3, KS X 1213, ISO/IEC 10118-3	EdgeDB Key Server	EdgeDB Key Agent	Audit Key	Hash using the SHA256 cryptographic algorithm, include the hash value, encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver
ISO/IEC 11770-3, KS X 1213, ISO/IEC 10118-3	EdgeDB Log Server	EdgeDB Log Agent	Audit Key	Hash using the SHA256 cryptographic algorithm, include the hash value, encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver
ISO/IEC 11770-3, KS X 1213, ISO/IEC 10118-3	EdgeDB Key Server	EdgeDB Key Agent	User data Key	Hash using the SHA256 cryptographic algorithm, include the hash value, encrypt with the Session Key using ARIA-256-CBC-PKCS#5, and deliver

[Table 7-11] Audit Key and User data Key Distribution

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

※ **Related security functional requirements**
- FCS_CKM.2

7.2.4. Cryptographic Key Destruction

The TOE can safely destroy the cryptographic keys in [Table 7-12] stored in the locations in [Table 7-12] by performing the deletion method in [Table 7-12] at the timing of deletion in [Table 7-12]. (FCS_CKM.6)

Cryptographic key	TOE	Location	Deletion method	Deletion timing
User data Key	EdgeDB Key Agent	Memory	Zeroization	Immediately after encryption/decryption of user data
Master Key	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
Local Key	EdgeDB Key Server	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	key file	Zeroize the file area, then delete	Upon deletion of the TOE
Audit Key	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Session Key	EdgeDB Key Server	Memory	Zeroization	Upon session termination
	EdgeDB Log Server	Memory	Zeroization	Upon session termination
	EdgeDB Key Agent	Memory	Zeroization	Upon session termination
	EdgeDB Log Agent	Memory	Zeroization	Upon session termination
Auth Key Pair	EdgeDB Key Server	key file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Server	Memory	Zeroization	After signature value generation
	EdgeDB Log Server	Memory	Zeroization	After signature value generation
	EdgeDB Key Agent	key file (private key)	Zeroize the file area, then delete	After key injection
	EdgeDB Key Agent	key file (server public key)	Zeroize the file area, then delete	After key injection
	EdgeDB Key Agent	Configuration file	Zeroize the file area, then delete	Upon deletion of the TOE
	EdgeDB Key Agent	Memory	Zeroization	After signature value generation
	EdgeDB Log Agent	key file (private key)	Zeroize the file area, then delete	After key injection
	EdgeDB Log Agent	key file (server public key)	Zeroize the file area, then delete	After key injection
	EdgeDB Log Agent	Configuration file	Zeroize the file area, then delete	Upon deletion of the TOE

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	EdgeDB Log Agent	Memory	Zeroization	After signature value generation
ECDH Private Key	EdgeDB Key Server	Memory	Zeroization	Upon Session Key generation
	EdgeDB Log Server	Memory	Zeroization	Upon Session Key generation
	EdgeDB Key Agent	Memory	Zeroization	Upon Session Key generation
	EdgeDB Log Agent	Memory	Zeroization	Upon Session Key generation

[Table 7-12] Cryptographic Key Destruction

※ **Related security functional requirements**
- FCS_CKM.6

7.2.5. Cryptographic Operation

The library module provided by the EdgeDB Key Agent uses the cryptographic algorithms in [Table 7-13], which are subject to validation of a validated cryptographic module whose security and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP) in compliance with the standards listed in [Table 7-13], and performs the operations listed in [Table 7-13] on user data according to the cryptographic key lengths in [Table 7-13]. (FCS_COP.1(1))

The User data Key used by the library module to encrypt user data is decrypted with ARIA-256-CBC using the Master Key generated by the EdgeDB Key Agent before it is used.

Standard list	Cryptographic algorithm	Cryptographic key size	Operation mode	Padding	Operation list
KS X 1213	ARIA	128 bits	CBC	PKCS#5	Encryption·Decryption
KS X 1213	ARIA	256 bits	CBC	PKCS#5	Encryption·Decryption
TTAS.KO-12.0004/R1	SEED	128 bits	CBC	PKCS#5	Encryption·Decryption
ISO/IEC 10118-3	SHA256	None	None	None	Hash

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

ISO/IEC 10118-3	SHA384	None	None	None	Hash
ISO/IEC 10118-3	SHA512	None	None	None	Hash

[Table 7-13] User Data Cryptographic Operations

Among the cryptographic algorithms in [Table 7-13], the ARIA and SEED cryptographic algorithms additionally use an initialization vector. To use an unpredictable initialization vector value, the initialization vector is generated with a length of 128 bits by the HASH-DRBG-SHA512 generation algorithm, using the random bit generator that is subject to validation of a validated cryptographic module whose security and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP). By using such an initialization vector, a different ciphertext is generated every time the same plaintext of user data is encrypted. (FDP_UDE.1, FCS_RBG.1)

TSF data is used for the purposes in [Table 7-14] by performing the operations listed in [Table 7-14] on the TSF data, according to the cryptographic key lengths in [Table 7-14], using the cryptographic algorithms in [Table 7-14], which are subject to validation of a validated cryptographic module whose security and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP) in compliance with the standards listed in [Table 7-14]. (FCS_COP.1(2))

Standard list	Cryptographic algorithm	Cryptographic key size	Operation mode	Padding	Operation list	Usage
KS X 1213	ARIA	256 bits	CBC	PKCS#5	Encryption·Decryption	Encryption·Decryption
ISO/IEC 10118-3	SHA256	None	None	None	Hash	Administrator/Master password hash generation, during encrypted communication integrity verification value

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

						generation
ISO/IEC 9797-2	HMAC-SHA256	256 bits	None	None	Integrity verification	Generation of integrity verification values for the TSF, TSF data, and audit data
ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	None	None	Signature generation/ verification	TOE Components mutual authentication

[Table 7-14] TSF Data Cryptographic Operations

※ Related security functional requirements
- FCS_COP.1(1), FCS_COP.1(2), FDP_UDE.1

7.2.6. Random Bit Generation

In addition to the purposes described above, to provide security functions securely, the TOE generates random numbers using the random bit generator subject to validation of a validated cryptographic module whose security and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP) in compliance with the standards listed in [Table 7-15], with the random bit generation algorithm in [Table 7-15] and the lengths in [Table 7-15], and uses them for the purposes in [Table 7-15]. (FCS_RBG.1)

Standard list	Random Bit Generation Algorithm	size	Usage
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	128 bits	Server/Agent random values used during mutual authentication
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	128 bits	For block cipher operations, IV value used
TTAK.KO-	HASH-DRBG-SHA512	128 bits	Salt value used for

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

12.0331-Part1, TTAK.KO-12.0331-Part2			Master Key generation
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	256 bits	Token value issued to the Agent after mutual authentication
TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2	HASH-DRBG-SHA512	512 bits	For self-encoding, encoding value used

[Table 7-15] Use of the Random Bit Generator for Providing Other Security Functions

For random bit generation, the TOE uses the random bit generator subject to validation of the validated cryptographic module "EdgeCrypto v4.2" and provides a deterministic random bit generation service with the HASH DRBG algorithm in accordance with [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2]. (FCS_RBG.1)
For initialization and seeding of the DRBG, three TSF software-based entropy sources provided by the operating system on which the TOE is installed are used: gettimeofday, clock_gettime, and /dev/urandom. (FCS_RBG.4)
The DRBG is seeded using minimum entropy of 13 bits from 16 bytes (collected once) for gettimeofday, 20 bits from 16 bytes (collected once) for clock_gettime, and 280 bits from 40 bytes (collected 40 times) for /dev/urandom. (FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3)) The outputs of the collected entropy sources are concatenated and then combined by applying the derivation function (Hash_df) defined in [TTAK.KO-12.0331-Part1, TTAK.KO-12.0331-Part2], producing a seed with a minimum entropy of at least 256 bits. In addition, after the TOE collects random numbers 2^27-1 times, it updates the DRBG state by re-seeding using the same entropy sources. (FCS_RBG.5, FCS_RBG.1)

※ **Related security functional requirements**
- FCS_RBG.1, FCS_RBG.3(1), FCS_RBG.3(2), FCS_RBG.3(3), FCS_RBG.4, FCS_RBG.5

7.3. User Data Protection

The library module provided by the EdgeDB Key Agent operates according to the DB encryption

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

policy that the chief administrator creates through the administrator page provided by the EdgeDB Key Server. Depending on how the user applies the library provided by the EdgeDB Key Agent, a different DB encryption policy can be used for each column, enabling encryption/decryption of user data using different cryptographic keys, cryptographic algorithms, etc. for each column, or one-way encryption, empty-value encryption, and double encryption depending on the cryptographic algorithm. Empty-value encryption is a function that can also encrypt a request that has no input value, and double encryption is a function that can also encrypt a request whose input value is already encrypted ciphertext. One-way encryption is a function that encrypts the input value and cannot be decrypted again. (FDP_UDE.1)

To encrypt and decrypt user data, the cryptographic algorithms listed in FCS_COP.1(1) are provided. For the ARIA and SEED block cipher algorithms, the IV value used in the cryptographic operation is a 128-bit random number, so that different ciphertexts are generated even when the same plaintext is encrypted with the same cryptographic key, and the IV value used in each operation is concatenated to the front of the ciphertext and managed. For one-way cryptographic algorithms, the SHA-256, SHA-384, and SHA-512 algorithms are provided, and the salt value is a 128-bit random number so that different one-way ciphertexts are generated for the same plaintext. To encrypt and decrypt user data, the EdgeDB Key Agent provides these functions as a library module in the form of the API method or the plug-in method. (FDP_UDE.1)

Residual plaintext information remaining in memory after user data encryption/decryption operations is securely removed using the zeroization function. (FDP_RIP.1)
User data ciphertext is provided in text-type and binary-type (including one-way encryption) forms.

※ Related security functional requirements
- FDP_UDE.1, FDP_RIP.1

7.4. Identification and Authentication

The identification and authentication function provided by the TOE is provided to perform identification and authentication of the administrator who can access the administrator page provided by the EdgeDB Key Server, and mutual authentication between TOE components.

7.4.1. Identification and Authentication of the Administrator

Before allowing access to and control of the administrator page provided by the EdgeDB Key Server through the WAS of the operational environment, the EdgeDB Key Server must successfully

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

perform identification and authentication. The EdgeDB Key Server uses the administrator's ID as identification information and the administrator's password as authentication information. When it receives the ID and password entered by the user, it identifies the administrator by checking whether an administrator ID matching the entered ID exists; if the administrator is correctly identified, it performs authentication by generating a hash value of the entered password with the SHA-256 one-way cryptographic algorithm and comparing it with the password hash value of the identified administrator. (FIA_UAU.2, FIA_UID.2)

All passwords entered during the creation, modification, and authentication of any password are masked with ("*") and cannot be identified on the screen, and when identification and authentication fails, only the message "Login failed" is displayed. (FIA_UAU.7)

During administrator account authentication, if authentication fails consecutively for the fixed number of times (5) set as the number of allowed authentication failures, the EdgeDB Key Server blocks connection attempts to the account for 5 minutes (fixed value) and stores an audit record of the authentication failure. (FIA_AFL.1)

The Key Server requires the administrator in [Table 7-16] to comply with the secret information criteria for the secret information in [Table 7-16] at the timing in [Table 7-16], performs the action corresponding to success in [Table 7-16] when secret information verification succeeds, and performs the action corresponding to failure in [Table 7-16] when secret information verification fails. The secret information criteria are a combination rule of at least one each of uppercase English letters (26 characters: A ~ Z) / lowercase English letters (26 characters: a ~ z) / digits (10 characters: 0 ~ 9) / special characters (32 characters: `~!@#$%^&*()-_+=[]{}₩|;:'",.<>/?), and a length of 9 to 20 characters. (FIA_SOS.1)

Administrator	Timing	Secret Information	Success	Failure
Chief Administrator	Chief Administrator logs in for the first time	Password	To the entered value, change the password	Display the message "Password validation failed."
Chief Administrator	When the chief administrator's password is	Password	To the entered value, change the	Display the message "Password validation failed."

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	changed		password	
Chief Administrator	When the general administrator's password is changed	Password	To the entered value, change the password	Display the message "Password validation failed."
General Administrator	When the general administrator logs in for the first time	Password	To the entered value, change the password	Display the message "Password validation failed."

[Table 7-16] Secret Information Verification on the EdgeDB Key Server

Setting a password identical to the user account (ID), continuous repeated input of the same characters or digits, sequential input of consecutive keyboard characters or digits, and reuse of the immediately previously used password are prohibited. (FIA_SOS.1)

For every session, the EdgeDB Key Server generates a 256-bit authentication session value using the HASH-DRBG-SHA-512 random bit generation algorithm and uses it as the administrator's unique sessionId to prevent reuse of the authentication session. (FIA_UAU.4)

※ Related security functional requirements
- FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

7.4.2. mutual authentication

Before communicating, the TOE components in [Table 7-17] perform mutual authentication by the mutual authentication method in [Table 7-17] at the mutual authentication timing in [Table 7-17], in order to verify that each other is a correct TOE component. (FIA_IMA.1)

Standard list	TOE Components	Timing of Mutual Authentication	Mutual Authentication Method
Not applicable	EdgeDB Key Server EdgeDB Key Agent	When the EdgeDB Key Agent connects to the EdgeDB Key Server	self mutual authentication protocol
Not applicable	EdgeDB Log Server EdgeDB Log Agent	When the EdgeDB Log Agent connects to the EdgeDB Log Server	self mutual authentication protocol

[Table 7-17] Mutual Authentication between TOE Components

Mutual authentication is performed when the EdgeDB Key Agent and the EdgeDB Log Agent, after being started, first communicate (connect) with the EdgeDB Key Server and the EdgeDB Log Server, respectively (see [Table 7-17]). Mutual authentication is achieved through mutual digital signature generation and verification using the Auth Key Pair (RSA-PSS, 2048 bits, ISO/IEC 14888-2) and session key agreement based on ECDH (ECC-P256, 256 bits, ISO/IEC 11770-3), and subsequent communication and cryptographic key distribution are permitted only between TOE components that have successfully completed mutual authentication. (FIA_IMA.1)

※ **Related security functional requirements**
- FIA_IMA.1

7.5. Security Management

The EdgeDB Key Server provides security management functions through the administrator interface to the authorized administrator who has completed the identification and authentication process.

7.5.1. Security Roles

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

In the TOE, administrators are divided into the chief administrator, who can perform all security roles, and the general administrator, who can perform only monitoring functions. The chief administrator holds the status of the sole administrator. (FMT_SMR.1)

7.5.2. Management of security functions behavior

The TOE provides the administrators in [Table 7-18] with the management functions in [Table 7-18]. (FMT_MOF.1, FMT_SMF.1, FMT_SMR.1)

Administrator	Function list
Chief Administrator	Modify and query rules related to potential security violations
Chief Administrator	Modify and query the response actions to be taken when audit storage failure is anticipated
Chief Administrator	Modify, delete, and query EdgeDB Key Agent
Chief Administrator	Query, add, modify, and delete DB encryption policy
General Administrator	Query rules related to potential security violations
General Administrator	Query the response actions to be taken when audit storage failure is anticipated
General Administrator	Query EdgeDB Key Agent
General Administrator	Query DB encryption policy

[Table 7-18] Managed Security Functions

※ Related security functional requirements
- FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

7.5.3. Management of TSF data

With respect to security attributes and TSF data, the TOE provides the administrators in [Table 7-19] with the management functions in [Table 7-19]. (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1)

Administrator	TSF data list

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

Chief Administrator	Grant privileges to user accounts
Chief Administrator	Add, delete, and modify user IDs
Chief Administrator	Add, delete, and modify passwords of users (Chief Administrator, General Administrator)
Chief Administrator	Set the audit trail threshold for notifying the administrator when audit record loss is predicted
Chief Administrator	Register, delete, modify, and query IP addresses of management terminals (security management access)
Chief Administrator	Query agents – agent version, security policy applied to the agent, agent operating status (enabled/disabled), agent integrity verification result (success/failure)
Chief Administrator	Manage agent security policy
Chief Administrator	Set authentication information for accessing external IT entities (SMTP)
Chief Administrator	Change the default password used to access TOE internal components or external IT entities
Chief Administrator	Set the execution interval of TOE server integrity verification
Chief Administrator	Query identification information of the TOE and TOE components (Key Server, Key Agent, Log Server, Log Agent)
Chief Administrator	Set the number of concurrent sessions for monitoring administrators
Chief Administrator	Query audit records
Chief Administrator	Query the maximum number of allowable failed authentication attempts
Chief Administrator	Query, add, and delete cryptographic keys
General Administrator	Modify own password
General Administrator	Query the audit trail threshold for notifying the administrator when audit record loss is predicted

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

General Administrator	Query IP addresses of management terminals (security management access)
General Administrator	Query agents – agent version, security policy applied to the agent, agent operating status (enabled/disabled), agent integrity verification result (success/failure)
General Administrator	Query agent security policy
General Administrator	Query authentication information for accessing external IT entities (SMTP)
General Administrator	Query the execution interval of TOE server integrity verification
General Administrator	Query identification information of the TOE and TOE components (Key Server, Key Agent, Log Server, Log Agent)
General Administrator	Query the number of concurrent sessions for monitoring administrators
General Administrator	Query audit records
General Administrator	Query the maximum number of allowable failed authentication attempts
General Administrator	Query cryptographic keys

[Table 7-19] TSF Data Subject to Management

※ **Related security functional requirements**
- FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.5.4. Management of ID and Password

The TOE provides a function for the chief administrator to change the ID and password when the chief administrator succeeds in authentication using the ID and password of the initial administrator account on the TOE interface after the TOE is installed. After the chief administrator creates a general administrator account, the TOE provides a function for the general administrator to change the password when the general administrator succeeds in authentication on the TOE administrator interface using the ID created by the chief administrator and the password set to the initial value. In addition, the TOE provides the chief administrator with a function to change the passwords of all

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

administrators. Administrator passwords are encrypted with the SHA256 algorithm and follow the administrator password generation rules in [Table 7-20]. The TOE does not provide a function to change the administrator ID generation rules or the administrator password generation rules. (FMT_PWD.1)

To use these identification and authentication functions, the ID and password of the chief administrator created by default must first be changed. On the first login to the administrator page, the user is moved to a page that forces a change of the administrator ID and password, and when the desired chief administrator account ID and password are entered, the account information is changed to the entered ID and password. A general administrator account is created when the chief administrator registers the general administrator's ID. At first login, the general administrator is moved to the password change page and can change the password.

Classification	Password length	9 to 20 characters
	Combination rule	A combination of four or more of numbers, uppercase English letters, lowercase English letters, and special characters
	Allowed numbers	0 to 9
	Allowed uppercase English letters	A to Z
	Allowed lowercase English letters	a to z
	Allowed special characters	`~!@#$%^&*()-_+=[]{}₩|;:'",.<>/?)

[Table 7-20] Administrator Password Generation Rules

※ **Related security functional requirements**
- FMT_PWD.1

7.6. Protection of the TSF

The TOE protects the TSF using the cryptographic algorithms subject to validation of the validated cryptographic module "EdgeCrypto v4.2", whose stability and implementation conformance have been confirmed through the Korea Cryptographic Module Validation Program (KCMVP).

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

7.6.1. Basic internal TSF data transfer protection

When TSF data is transmitted between TOE components, the TOE hashes the TSF data to be transmitted with SHA256, appends the hash to the TSF data, encrypts it with ARIA-256-CBC using the Session Key, and then transmits it, thereby protecting the transmitted TSF data from unauthorized disclosure and modification. When a violation of received data integrity is detected, the received data of that TSF data is discarded and related audit data is generated. (FPT_ITT.1)

※ **Related security functional requirements**
- FPT_ITT.1

7.6.2. Basic Protection of Stored TSF Data

The TOE protects the TSF data of [Table 7-21] stored in the TOE components of [Table 7-21] by the protection methods of [Table 7-21]. The cryptographic operations used to protect the TSF data are performed using the validated cryptographic module "EdgeCrypto v4.2". (FPT_PST.1(extended))

TOE Components	TSF data	Protection method
EdgeDB Key Server	Master password	Hashed with the SHA-256 algorithm and the hash value is stored in the DB
	Administrator password	A salt value is added using the SHA-256 algorithm so that a different hash value is stored in the DB each time
	SMTP password	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Administrator security alert recipient email	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Threshold related to local DB storage of audit data and threshold check interval	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Threshold for failed authentication attempts	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Maximum allowed number of concurrent	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	general administrator sessions	stored in the DB
	Self-test, forgery/tampering, and process check audit cycle and audit time	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Communication cycle of the Key Agent	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Validity period of administrator password and master password	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	DBMS Account Information	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and written to the configuration file
	Access control policy	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Audit data (Temporary file)	Obfuscated by a self-encoding technique that rearranges the Base64 encoding index table on its own, and written to the 'EdgeSvr_Audit_YYYYMMDD.log.0' file
	DB encryption policy	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and stored in the DB
	Master Key	Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Audit Key	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded, stored in the DB, and written to the 'audit.key' file
		Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Auth Priv Key(Server)	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and written to the 'ksprivate.key' file
	Auth Priv Key(Agent)	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and written to the 'kaprivate.key' file
	Local Key	Encrypted with the ARIA-256-CBC algorithm using the

t ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

		Master Key, and the ciphertext is self-encoded, stored in the DB, and written to the 'local.key' file
		Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Session Key	Obfuscated by the self-encoding technique and stored in memory, then deleted when the session or the TOE terminates
	User data Key	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and stored in the DB
EdgeDB Key Agent	Server IP	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Server PORT	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Agent ID	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Network interface	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Audit data (Temporary file)	Obfuscated by a self-encoding technique that rearranges the Base64 encoding index table on its own, and written to the 'EdgeAgent_YYYYMMDD.log.0' file
	DB encryption policy	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	Master Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	Audit Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	Local Key	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and stored as a file
		Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Auth Priv Key(Agent)	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

		written to the configuration file
	Session Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	User data Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
EdgeDB Log Server	Port information	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and written to the configuration file
	DBMS Account Information	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and written to the configuration file
	Network interface	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and written to the configuration file
	Audit data (Temporary file)	Obfuscated by a self-encoding technique that rearranges the Base64 encoding index table on its own, and written to the 'EdgeLogSvr_YYYYMMDD.log.0' file
	Master Key	Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Audit Key	Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Auth Priv Key(Server)	Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Session Key	Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
EdgeDB Log Agent	Server IP	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Server PORT	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Network interface	Encrypted with the ARIA-256-CBC algorithm using the Local Key, and the ciphertext is self-encoded and the value is written to the configuration file
	Audit data (Temporary file)	Obfuscated by a self-encoding technique that rearranges the Base64 encoding index table on its own, and written to the 'EdgeLogAgent_YYYYMMDD.log.0'

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	Master Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	Audit Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates
	Auth Priv Key(Agent)	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and written to the configuration file
	Local Key	Encrypted with the ARIA-256-CBC algorithm using the Master Key, and the ciphertext is self-encoded and
		Obfuscated by the self-encoding technique and stored in memory, then deleted when the TOE terminates
	Session Key	Obfuscated by self-encoding and stored in memory, then deleted when the TOE terminates

[Table 7-21] Protection Methods for Stored TSF Data

Cryptographic keys and Critical Security Parameters loaded into memory are obfuscated by the self-encoding technique and kept in memory, and are securely destroyed by the zeroization function after use.

※ **Related security functional requirements**
- **FPT_PST.1(extended)**

7.6.3. Self-Test

To demonstrate the correct operation of its components, namely EdgeDB Key Agent, EdgeDB Log Agent, EdgeDB Key Server, and EdgeDB Log Server, the TOE performs self-tests at start-up, periodically during normal operation, or on demand by the authorized administrator (chief administrator), which include checking whether the key security function processes are running correctly, performing the self-test of the validated cryptographic module, and performing TSF integrity checks on files such as the validated cryptographic module, executable files, installation scripts, start scripts, stop scripts, and library modules. In addition, the TOE performs integrity checks on some TSF data of the EdgeDB Key Server specified in [Table 7-23] and on the Local Key of all TOE components. The integrity checks of the TSF and TSF data are performed by comparing the HMAC-SHA256 MAC values of the integrity check targets. In addition, the authorized administrator (chief administrator) can request a self-test of all TOE components through the "Real-time self-test execution" function on the administrator page, regardless of the configured cycle, and each

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

component that receives the request performs the same items as the self-tests performed periodically during normal operation and records the results as audit data.
The cycle of self-tests performed during normal operation is, for the EdgeDB Key Server, EdgeDB Key Agent, and EdgeDB Log Server, the self-test cycle specified by the chief administrator; the default value of the cycle that the chief administrator can specify on the administrator page is every day at 00:00, and it can be set to run at 00:00 to 23:00 every 1 to 100 days. The EdgeDB Log Agent performs its self-test every day at 00:05 regardless of the self-test cycle specified by the chief administrator. In addition, the EdgeDB Key Server, EdgeDB Key Agent, EdgeDB Log Server, and EdgeDB Log Agent can perform a self-test when the chief administrator clicks the real-time button on the administrator page as needed.
When a violation occurs as a result of the periodic self-tests performed during normal operation, an email is sent to the authorized administrator designated by the chief administrator. In addition, the authorized administrator can perform an integrity check of the TSF data stored in the internal DB when moving to the detailed query page of a management function on the administrator page, and when the data integrity check fails, an integrity failure message is displayed on the administrator page and an email is sent to the authorized administrator designated by the chief administrator.

The following [Table 7-22] lists the self-test items by TOE, [Table 7-23] lists the TSF data integrity verification items by TOE, and [Table 7-24] lists the TSF integrity verification items by TOE. The self-test items and integrity verification items below are performed identically regardless of the operational environment of the physical server on which the TOE is installed. (FPT_TST.1)

TOE Components	Timing of self-test execution	Test item	Test method
EdgeDB Key Server	Performed at start-up	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Self-check of whether the EdgeDB Key Server process exists in the OS process list
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Checked from the EdgeDB Log Server, by verifying whether the EdgeDB Key Server process exists in the OS process list, that

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	demand by the chief administrator		the EdgeDB Key Server is operating normally
EdgeDB Key Agent	Performed at start-up	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Self-check of whether the EdgeDB Key Agent process exists in the OS process list
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Verified from the EdgeDB Key Server whether the EdgeDB Key Agent communicates normally at every connection cycle
EdgeDB Log Server	Performed at start-up	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Self-check of whether the EdgeDB Log Server process exists in the OS process list
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Checked from the EdgeDB Key Server whether the EdgeDB Log Server process exists in the OS process list
EdgeDB Log Agent	Performed at start-up	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
		Process	Self-check of whether the EdgeDB Log Agent process exists in the OS process list

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	- Performed every day at 00:05 after start-up - Performed on demand by the chief administrator	KCMVP Cryptographic module	Checked by calling the self-verification function of the KCMVP cryptographic module
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	Process	Verified from the EdgeDB Log Server whether the EdgeDB Log Agent communicates normally at every connection cycle

[Table 7-22] Self-Test Items by TOE

TOE Components	Timing of integrity verification	Integrity verification item
EdgeDB Key Server	Performed at start-up	local.key
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	
	Performed when management functions and setting values are queried in detail on the administrator page	Audit log (occurrence date/time / storage date/time / occurrence IP / request IP / log category / log level / occurrence module / process / success or failure / executing administrator ID / execution object / execution target / execution type / result code / result message) DB encryption policy (protection policy name / policy enabled or not / encryption-decryption log storage flag / encryption-decryption permission /

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

		plaintext format / key length / protection policy algorithm list) Agent registration information (agent ID / applied policy / encryption-decryption log storage flag / agent name / agent MAC value / agent IP / agent enabled or not) Module check cycle Module check time Agent communication cycle Number of concurrent general administrator users Audit log storage check cycle Audit log storage threshold Allowed number of login failures Administrator password validity period Master password validity period User data cryptographic key (key name / key version / key value) Administrator information (administrator ID / administrator name / administrator password / administrator enabled or not / administrator privilege / number of login failures) Email settings (SMTP server IP / SMTP server port / SMTP server user / recipient email / header / footer / email transmission items)
EdgeDB Log Server	Performed at start-up - Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	local.key

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved I Confidential

EdgeDB Key Agent	Performed at start-up	local.key
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	
EdgeDB Log Agent	Performed at start-up	local.key
	- Performed every day at 00:05 after start-up - Performed on demand by the chief administrator	

[Table 7-23] TSF Data Integrity Verification Items by TOE

TOE Components	Timing of integrity verification	Integrity verification item
EdgeDB Key Server	Performed at start-up	EdgeDB Key Server library Installation and start/stop scripts KCMVP cryptographic module
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	
EdgeDB Log Server	Performed at start-up	EdgeDB Log Server library Installation and start/stop scripts KCMVP cryptographic module
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	
EdgeDB Key Agent	Performed at start-up	EdgeDB Key Agent library Installation and start/stop scripts
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief	

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

	administrator	
	Performed at start-up	API library KCMVP cryptographic module
	- Performed at the specified time at each self-test cycle specified by the chief administrator - Performed on demand by the chief administrator	
	Performed every day at 00:05 after start-up	
EdgeDB Log Agent	Performed at start-up	EdgeDB Log Agent library Installation and start/stop scripts KCMVP cryptographic module
	- Performed every day at 00:05 after start-up - Performed on demand by the chief administrator	

[Table 7-24] TSF Integrity Verification Items by TOE

※ **Related security functional requirements**
- FPT_TST.1

7.6.4. Failure with preservation of secure state

The TOE preserves a secure state when a random bit generator failure occurs. The TOE performs the self-test of the validated cryptographic module "EdgeCrypto v4.2" at start-up, and if the self-test of the random bit generator fails, it halts the process start-up. In addition, if a random number generation request fails during normal operation, the TOE aborts the corresponding cryptographic operation and returns an error so that a predictable value is not used as a cryptographic key or initialization vector. (FPT_FLS.1)

※ **Related security functional requirements**
- FPT_FLS.1

7.7. TOE Access

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

7.7.1. Limitation on Multiple Concurrent Sessions

The EdgeDB Key Server blocks concurrent access to the same account by limiting the maximum number of concurrent sessions to 1 for the same account for both the chief administrator and general administrators. When a new connection is made to an account that is already connected, the existing session ID in the administrator login session list managed by the EdgeDB Key Server is overwritten with the new session ID, and the existing connection session is terminated. The maximum number of concurrent connections of general administrators having the same privilege is initially limited to 5, and the chief administrator can change it to between 5 and 100 on the server information setting screen. When general administrators with different accounts connect in excess of the maximum number of concurrent connections, the connections of administrators beyond that maximum number of concurrent connections are blocked. (FTA_MCS.2)

※ **Related security functional requirements**
- FTA_MCS.2

7.7.2. Session Management and Configuration

The TOE restricts TOE access so that the EdgeDB Key Server, which is the administrator interface, can be accessed only from registered IP addresses, and terminates the session if it is not used for 10 minutes after the authorized administrator logs in. (FTA_SSL.3, FTA_TSE.1(1))

The IP address used for the first login after the TOE is installed is automatically set as the allowed access IP address, and the chief administrator can change the allowed access IP address or add one at a time on the administrator settings screen. Configuration that specifies an IP address range is not permitted. (FTA_TSE.1(1))

※ **Related security functional requirements**
- FTA_SSL.3, FTA_TSE.1(1)

7.8. Trusted Path/Channels

7.8.1. Inter-TSF trusted channel

When sending a security alert email, the EdgeDB Key Server and EdgeDB Log Server initialize an encrypted communication channel with the mail server using TLS v1.2, and the Cipher Suites used

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved | Confidential

for the encrypted communication support the Cipher Suites specified in [Table 7-25]. (FTP_ITC.1)

Cipher Suites
ssTLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256

[Table 7-25] List of Cipher Suites Selected for TLS v1.2 Communication with the Mail Server

※ **Related security functional requirements**

- FTP_ITC.1

Copyright ⓒ 2026 ITCENPNS Co. Inc. All rights Reserved ㅣ Confidential