


EdgeDB v4.0

Security Target(ST) for Public

v1.5



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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Revision History		
Title		EdgeDB v4.0_Security Target(ST) for Public
Version	Date	Description
v1.0	2020.09.08	Convert EdgeDB v4.0 Security Target(ST) v1.11 to public purpose
v1.1	2020.09.10	Incorporation of the review findings
v1.2	2020.09.11	Incorporation of the review findings
v1.3	2020.09.14	Incorporation of the review findings
v1.4	2020.09.15	Convert EdgeDB v4.0 Security Target(ST) v1.12 to public purpose
v1.5	2020.09.28	Incorporation of the review findings




	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Table of Contents


- 1. SECURITY TARGET INTRODUCTION 9**
 - 1.1. ST REFERENCE..... 9
 - 1.2. TOE REFERENCE 10
 - 1.3. TOE OVERVIEW 11
 - 1.3.1. TOE Usage and Key Security Features..... 11
 - 1.3.2. TOE Type..... 13
 - 1.3.3. Identification of non-TOE HW/SW 15
 - 1.4. TOE DESCRIPTION..... 21
 - 1.4.1. Physical Scope of the TOE..... 21
 - 1.4.2. Logical Scope of the TOE 24
 - 1.5. TERMS AND DEFINITIONS..... 32
 - 1.6. CONVENTIONS 41
- 2. CONFORMANCE CLAIM..... 42**
 - 2.1. CC CONFORMANCE CLAIM..... 42
 - 2.2. PP CONFORMANCE CLAIM..... 42
 - 2.3. PACKAGE CONFORMANCE CLAIM 44
- 3. SECURITY OBJECTIVES 45**
 - 3.1. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT..... 45
- 4. EXTENDED COMPONENTS DEFINITION 47**
 - 4.1. CRYPTOGRAPHIC SUPPORT 47
 - 4.1.1. Random Bit Generation 47
 - 4.2. IDENTIFICATION & AUTHENTICATION 48
 - 4.2.1. TOE Internal mutual authentication..... 48
 - 4.3. USER DATA PROTECTION 49
 - 4.3.1. User data encryption 49
 - 4.4. SECURITY MANAGEMENT 50
 - 4.4.1. ID and password 50
 - 4.5. PROTECTION OF THE TSF 51
 - 4.5.1. Protection of stored TSF data..... 51
 - 4.6. TOE ACCESS..... 52
 - 4.6.1. Session locking and termination..... 52

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5. SECURITY REQUIREMENTS	54
5.1. SECURITY FUNCTIONAL REQUIREMENTS.....	54
5.1.1. Security Audit (FAU)	56
5.1.2. Cryptographic Support (FCS).....	60
5.1.3. User Data Protection (FDP).....	67
5.1.4. Identification and Authentication (FIA)	68
5.1.5. Security Management (FMT).....	70
5.1.6. Protection of the TSF (FPT)	73
5.1.7. TOE Access (FTA).....	75
5.1.8. Trusted path/channels (FTP)	76
5.2. SECURITY ASSURANCE REQUIREMENTS	77
5.2.1. Security Target Evaluation	77
5.2.2. Development	82
5.2.3. Guidance Documents	82
5.2.4. Life-cycle support.....	84
5.2.5. Tests	85
5.2.6. Vulnerability assessment	86
5.3. SECURITY REQUIREMENTS RATIONALE	86
5.3.1. Dependency of the SFRs.....	87
5.3.2. Assurance Requirements Rationale	88
6. TOE SUMMARY SPECIFICATION	89
6.1. SECURITY AUDIT	90
6.1.1. Audit data generation	90
6.1.2. Audit data review	92
6.1.3. Potential violation analysis and response	93
6.1.4. Protection of audit data and action against data loss	93
6.2. CRYPTOGRAPHIC SUPPORT.....	94
6.2.1. Cryptographic Key Generation.....	94
6.2.2. Cryptographic Key Distribution	96
6.2.3. Destruction of Cryptographic Key	97
6.2.4. Cryptographic Operation	100
6.3. USER DATA PROTECTION.....	102
6.4. IDENTIFICATION AND AUTHENTICATION	102
6.4.1. Identification and Authentication by Administrator.....	103


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- 6.4.2. Mutual Authentication 104
- 6.5. SECURITY MANAGEMENT 104
 - 6.5.1. Security Role 104
 - 6.5.2. Security Function Management..... 105
 - 6.5.3. TSF Data Management 105
 - 6.5.4. ID and Password Management..... 106
- 6.6. PROTECTION OF THE TSF..... 107
 - 6.6.1. Basic Protection of internally transmitted TSF Data..... 107
 - 6.6.2. Basic Protection for Stored TSF Data 107
 - 6.6.3. Testing of external entity 110
 - 6.6.4. Self-testing..... 111
- 6.7. TOE ACCESS..... 114
 - 6.7.1. Limiting the Number of Access Sessions 114
 - 6.7.2. Session Management and Configuration..... 114
- 6.8. TRUSTED PATH/CHANNELS 114
 - 6.8.1. Trusted Channel between TSF 114

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


List of Figures

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


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

List of Tables

[TABLE 1-1] ST REFERENCE	9
[TABLE 1-2] TOE REFERENCE	10
[TABLE 1-3] TLS v1.2 CIPHER SUITS APPROVED FOR ACCESS TO THE ADMINISTRATOR PAGE BY WAS	15
[TABLE 1-4] OPERATIONAL ENVIRONMENT BASED ON THE API TYPE	17
[TABLE 1-5] OPERATIONAL ENVIRONMENT BASED ON THE PLUG-IN TYPE	18
[TABLE 1-6] MINIMUM HW AND SW REQUIREMENTS FOR TOE INSTALLATION AND OPERATION.....	19
[TABLE 1-7] THE ROLE OF THIRD-PARTY SW USED IN TOE.....	20
[TABLE 1-8] EXTERNAL IT ENTITY.....	20
[TABLE 1-9] PHYSICAL SCOPE OF THE TOE	22
[TABLE 1-10] VALIDATED CRYPTOGRAPHIC MODULE	22
[TABLE 2-1] CONFORMANCE TO CC.....	42
[TABLE 2-2] RATIONALE FOR PP CONFORMANCE CLAIM.....	44
[TABLE 5-1] SECURITY FUNCTIONAL REQUIREMENTS (SFR).....	55
[TABLE 5-2] AUDIT EVENT.....	58
[TABLE 5-3] TYPE OF AUDIT DATA AND SELECTION CRITERIA.....	60
[TABLE 5-4] KEY GENERATION ALGORITHM USED BY TOE TO GENERATE CRYPTOGRAPHIC KEY FOR USER DATA	61
[TABLE 5-5] KEY GENERATION ALGORITHM USED BY TOE TO GENERATE CRYPTOGRAPHIC KEY FOR TSF DATA	61
[TABLE 5-6] CRYPTOGRAPHIC KEY DISTRIBUTION METHOD	63
[TABLE 5-7] CRYPTOGRAPHIC KEY DESTRUCTION METHOD.....	65
[TABLE 5-8] CRYPTOGRAPHIC OPERATION OF USER DATA	66
[TABLE 5-9] CRYPTOGRAPHIC OPERATION OF TSF DATA.....	67
[TABLE 5-10] MUTUAL AUTHENTICATION METHOD BETWEEN TOE COMPONENTS.....	69
[TABLE 5-11] SECURITY FUNCTION BEHAVIOR OF ADMINISTRATOR.....	71
[TABLE 5-12] TSF DATA AND MANAGEMENT ABILITY.....	72
[TABLE 5-13] TESTING OF EXTERNAL ENTITIES	75
[TABLE 5-14] SECURITY ASSURANCE REQUIREMENTS.....	77
[TABLE 5-15] RATIONALE OF THE DEPENDENCIES	88
[TABLE 6-1] LIST OF TOE SECURITY FUNCTIONS.....	90
[TABLE 6-2] AUDITABLE EVENTS FOR THE TOE.....	92
[TABLE 6-3] ADDITIONAL AUDIT RECORDS FOR CERTAIN AUDIT EVENTS	92
[TABLE 6-4] VALIDATED CRYPTOGRAPHIC MODULE	94
[TABLE 6-5] CRYPTOGRAPHIC KEY GENERATION FOR USER DATA.....	95
[TABLE 6-6] GENERATE CRYPTOGRAPHIC KEY FOR TSF DATA	96

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

[TABLE 6-7] AUTH KEY PAIR DISTRIBUTION.....	97
[TABLE 6-8] AUDIT KEY, USER DATA KEY DISTRIBUTION	97
[TABLE 6-9] DESTRUCTION OF CRYPTOGRAPHIC KEY.....	100
[TABLE 6-10] CRYPTOGRAPHIC OPERATION OF USER DATA.....	101
[TABLE 6-11] CRYPTOGRAPHIC OPERATION OF TSF DATA.....	101
[TABLE 6-12] SECRET INFORMATION VERIFICATION ON EDGEDB KEY SERVER	104
[TABLE 6-13] MUTUAL AUTHENTICATION BETWEEN TOE COMPONENTS.....	104
[TABLE 6-14] SECURITY FUNCTIONS REQUIRING MANAGEMENT.....	105
[TABLE 6-15] TSF DATA REQUIRING MANAGEMENT	106
[TABLE 6-16] COMBINATION RULES FOR GENERATING ADMINISTRATOR'S PASSWORD	107
[TABLE 6-17] PROTECTION METHOD FOR STORED TSF DATA.....	110
[TABLE 6-18] TESTING ITEMS FOR EXTERNAL ENTITY	110
[TABLE 6-19] SELF-TESTING ITEMS FOR TOE.....	112
[TABLE 6-20] TSF DATA INTEGRITY VERIFICATION ITEMS FOR TOE COMPONENTS.....	113
[TABLE 6-21] TSF INTEGRITY VERIFICATION ITEMS FOR TOE COMPONENTS	113
[TABLE 6-22] LIST OF CIPHER SUITES TO SELECT WHEN COMMUNICATING WITH MAIL SERVER TLS V1.2	115

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1

1. Security Target Introduction

This document states the Security Target (ST) of EdgeDB v4.0 (hereinafter referred to as "TOE"), a database (hereinafter referred to as 'DB') encryption product of SECUCEN Co., Ltd. and defines TOE security functions and assurance requirements, and describes and provides the rationale for TOE's security objectives and IT requirements.


The ST is composed of the following sections.

- Section 1 : Identifies the TOE by providing information on ST reference, TOE reference, TOE overview, and TOE description.
- Section 2 : States the conformance claim that TOE complies with Common Criteria (CC), Protection Profile (PP), and Package, and also provides the rationale (or theoretical background).
- Section 3 : States TOE's security objective for the operational environment.
- Section 4 : Provides the definition and explanation for the extended component.
- Section 5 : States the TOE's security requirements and assurance requirements, and also provides the rationale (or theoretical background).
- Section 6 : States the TOE summary specification for the security functional requirements defined in Section 5.

1.1. ST Reference

Classification	Description
Title	EdgeDB v4.0 Security Target(ST) for Public
Version	1.5
Developer	SECUCEN Co., Ltd.
Publication Date	2020.09.28
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning Notice No. 2013-51, Aug. 8, 2013)
Common Criteria Version	CC V3.1 r5
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Keywords	DB, Encryption.

[Table 1-1] ST Reference


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1.2. TOE Reference

This ST is compliant with the following TOE description.

Classification		Description	
TOE Identification		EdgeDB v4.0	
TOE Version		v4.0.4.11	
TOE Component	EdgeDB Key Agent	EdgeDB Key Agent v4.0.4.11 for Windows - EdgeDB_Key_agent_4.0.4.11_win_64bit.exe EdgeDB Key Agent v4.0.4.11 for Linux - EdgeDB_Key_Agent_4.0.4.11_Linux-x86_64.run	S/W (CD Dist.)
	EdgeDB Log Agent	EdgeDB Log Agent v4.0.4.11 for Windows - EdgeDB_Log_Agent_4.0.4.11_win_64bit.exe EdgeDB Log Agent v4.0.4.11 for Linux - EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	
	EdgeDB Key Server	EdgeDB Key Server v4.0.4.11 - EdgeDB_Key_Server_4.0.4.11_Linux-x86_64.run	
	EdgeDB Log Server	EdgeDB Log Server v4.0.4.11 - EdgeDB_Log_Server_4.0.4.11_Linux-x86_64.run	
Guidance		EdgeDB v4.0 Preparative Procedure(PRE) v1.9 - EdgeDB v4.0_Preparative Procedure(PRE)_v1.9.pdf	PDF (CD Dist.)
		EdgeDB v4.0 Operational User Guidance(OPE) v1.8 - EdgeDB v4.0_Operational User Guidance(OPE)_v1.8.pdf	
		EdgeDB v4.0 Developer User's Guidance(DUG) v1.6 - EdgeDB v4.0_Developer User's Guidance(DUG)_v1.6.pdf	
Developer		SECUCEN Co., Ltd.	

[Table 1-2] TOE Reference

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1.3. TOE Overview


EdgeDB v4.0 (hereinafter referred to as TOE) is a DB encryption product provided in the form of software, which encrypts data stored in DB to prevent unauthorized disclosure to confidential data such as personal information and sensitive information. TOE consists of EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, EdgeDB Log Agent.

1.3.1. TOE Usage and Key Security Features

TOE encrypts user data within the DB managed by the organization's database management system (hereinafter referred to as the 'DBMS'). User data is the data before and after encrypted and stored in the DB, and typically includes the organization's confidential data that should be protected against threats, in other words, personal information and sensitive information managed by an organization. Part or all of the user data can be the encryption target, depending on the organizational security policies that runs the TOE. TOE performs encryption/decryption user data as 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 confidential data from the risk of unauthorized disclosure.

TOE's encryption type is divided into two types: a plug-in type and an API type. In the case of the plug-in type, the user data is encrypted and decrypted by cryptographic procedure call in the query used by the application program in DBMS, where the Linux server supports Oracle DBMS and Windows supports MS-SQL DBMS. In the API type, the user data is encrypted and decrypted by the API call of the application program's application service on the application server. The API type requires modification of the application program's Source Code, and the plug-in type requires modification of the application program query. Once encryption and decryption are complete, any residual information is safely deleted and protected from unauthorized disclosure.

TOE provides security and management functions, and records major audit events as audit data during initial start-up, periodically during normal operation, and TOE provides protection of the TSF by protection data stored in the TSF control repository and self-testing. Additionally, 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 for authentication token issuance, and distribution and cryptographic operation functions; security management functions such as security function management and configuration; and TOE access function to manage access session of the

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

authorized administrator.

The administrator in charge of managing the TOE can use the administrator interface provided by the TOE for security management, and to inquire TOE audit records, etc. For secure communication between the TOE administrator interface and the access manager, TLS 1.2 protocol configuration of the TOE operating environment, WAS is used to provide the secure path and channel functions, and, run a suite of self tests during initial start-up, periodically during normal operation.


The following depicts the major functions evaluated for each component of the TOE:

- EdgeDB Key Server
 - Integration management server for EdgeDB Key Agent, administrator, cryptographic key, DB encryption policy, etc.
 - Provision of administrator interface for TOE security management
 - Prevention of duplicate login by chief administrator as a result of prolonged real-time authentication sessions
 - Provision of the inquiry function to look up audit data stored in the local DB
 - Provision of security audit functions such as generating (selectable) audit records, security alerts, (selectable) audit review

- EdgeDB Log Server
 - Server for storing encryption and decryption log received from the EdgeDB Log Agent, operational log data, and audit log data in the local DB.
 - Response against an anticipated saturation of audit trail storage, etc.

- EdgeDB Key Agent
 - The module that receives encryption and decryption related policies from the EdgeDB Key Server to provide DB encryption service, which can encrypt and decrypt user data with different cryptographic keys, cryptographic algorithms, etc. for each column.
 - EdgeDB Key Agent installed on DB Server provides a plug-in library to perform user data encryption and decryption.
 - EdgeDB Key Agent installed on the Application Server provides an API-based library that supports JAVA and C-based platforms to perform user data encryption and decryption.

- EdgeDB Log Agent

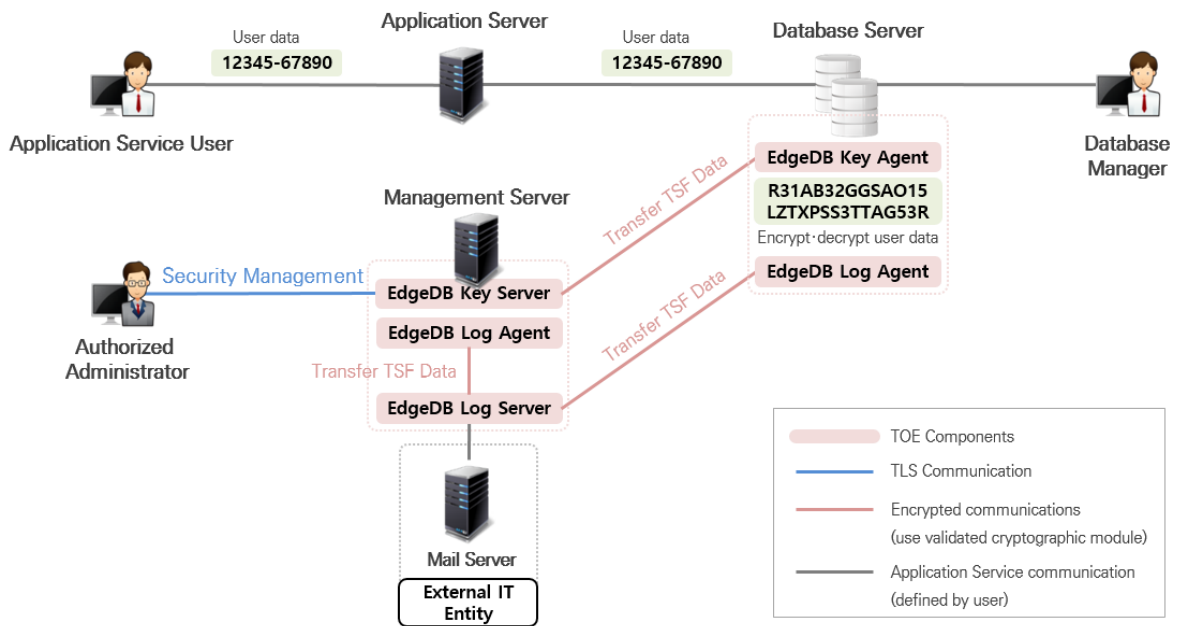
	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- The module that delivers encryption and decryption logs, operational log data, 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


TOE is divided into two types; 'Plug-in type,' which performs column-level encryption and decryption on user data within the DB using query based on UDF(User Define Function); and 'API type,' which performs column-level encryption and decryption on user data by calling cryptographic API at the source level. While either can be adopted, the 'API type' is recommended if the program source for encryption and decryption can be modified. But if not, the 'Plug-in type,' where only the query for delivery to the DB needs modification, is recommended. Both types are composed of four components; EdgeDB Key Agent, EdgeDB Log Agent, EdgeDB Key Server, and EdgeDB Log Server.

TOE Operational Environment is depicted in [Figure 1-1], [Figure 1-2].



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

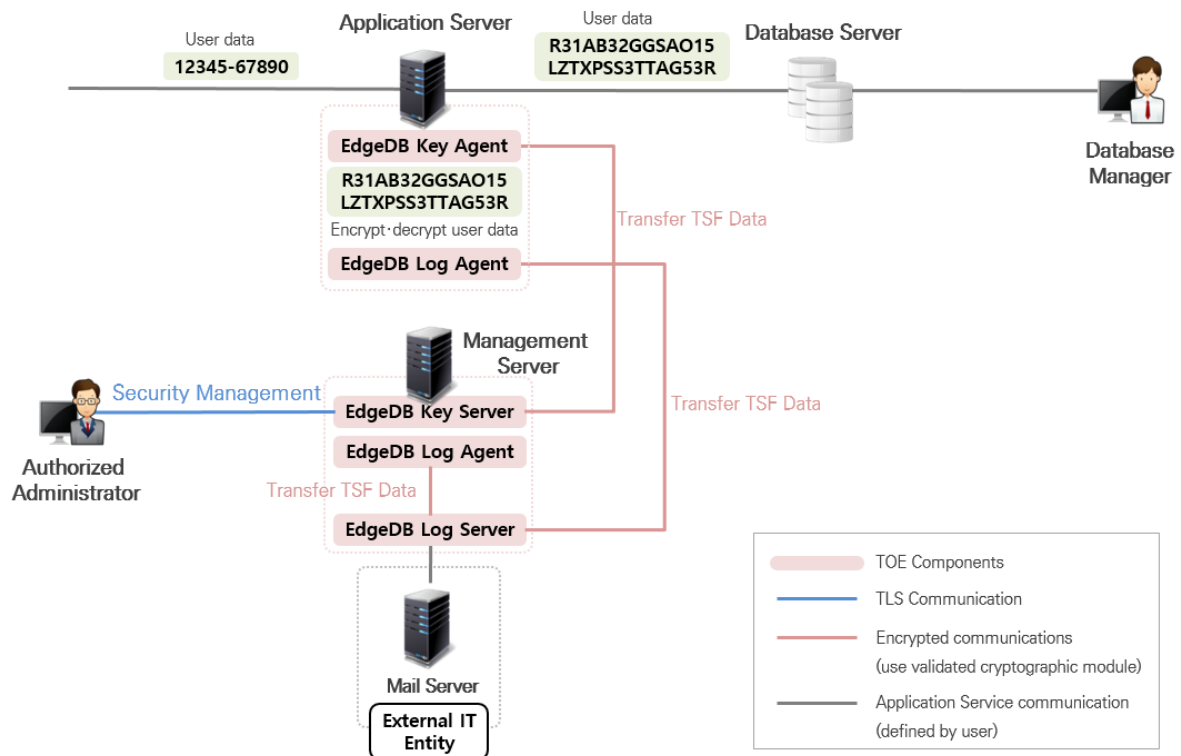
In the case of the plug-in type, the EdgeDB Key Agent is installed within the DB Server where the protected DB exists, and the management server is operated separately. EdgeDB Key Server and EdgeDB Log Server are to be installed in the Management Server, and EdgeDB Log Agent is installed in both the Management Server and the DB Server with TOE components. DBMS that can support the plug-in type include MS-SQL for Windows and Oracle for Linux. Additionally, a Mail Server is

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

required for the TOE Operational Environment to send alarm emails in case of security violations and detections as a result of operating the TOE.


When the authorized chief administrator sets the TOE security policy through a web browser on the administrator PC, the EdgeDB Key Server delivers the DB encryption policy to the EdgeDB Key Agent. Then encrypts the user data received from the Application Server before saving it within the DB following the DB encryption policy and the library provided by EdgeDB Key Agent, and decrypts the encrypted user data being delivered from DB Server to the Application Server. EdgeDB Log Agent, installed in both DB Server and Management Server, delivers the log generated from TOE components to EdgeDB Log Server, which then saves the collected log inside the DB.

Communication between the administrator PC and EdgeDB Key Server is protected using the TLS v1.2 protocol set in WAS. And, all communications between the TOE components that transmit TSF data are encrypted using approved cryptographic algorithm of the validated cryptographic module.



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

In the API type, EdgeDB Key Agent is installed in the Application Server, and the Management Server and DB Server are operated separately. EdgeDB Key Server and EdgeDB Log Server are

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

installed in the Management Server, whereas the EdgeDB Log Agent with TOE components are installed in both the Application Server and Management Server. Additionally, a Mail Server is required for the TOE Operational Environment to send alarm emails in case of security violations and detections as a result of operating the TOE.

When the authorized chief administrator sets the TOE security policy through a web browser on the administrator PC, the EdgeDB Key Server delivers the DB encryption policy to the EdgeDB Key Agent. Then encrypts the user data received from the Application user before transmitting to the DB following the DB encryption policy and the library provided by EdgeDB Key Agent, and decrypts the encrypted user data received from the DB. EdgeDB Log Agent, installed in both Application Server and the Management Server, delivers the log generated from TOE components to EdgeDB Log Server, which then saves the collected log inside the DB.


Communication between the administrator PC and EdgeDB Key Server is protected using the TLS v1.2 protocol set in WAS. The table below lists the TLS v1.2 Cipher Suites approved by 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 Suits approved for access to the administrator page by WAS

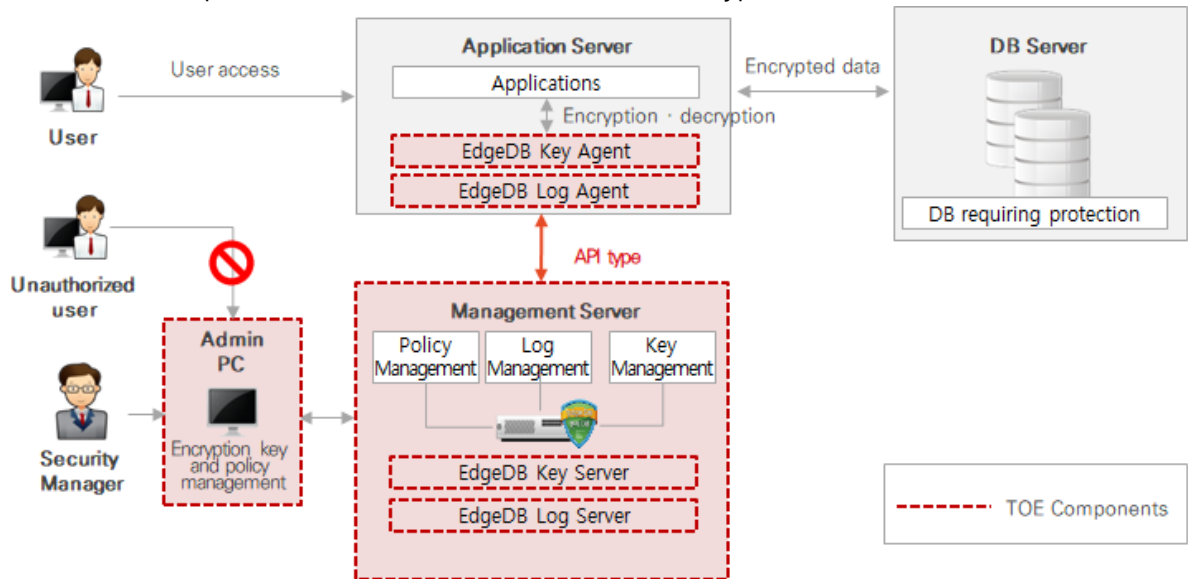
All communications between the TOE components that transmit TSF data are encrypted using approved cryptographic algorithm of the validated cryptographic module.

1.3.3. Identification of non-TOE HW/SW

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Operating the TOE requires supplementary HW and SW, which are not subject to evaluation. The third-party SW Apache-tomcat 8.5.57 and MariaDB 10.4.14 x86_64, which are specified as requirements for EdgeDB Key Server / EdgeDB Log Server, are provided on a separate CD. Each TOE component and supplementary SW must be installed on the correct HW, which varies depending on the Operational Environment and operating type, to operate the TOE.


The following explains the required TOE components and third-party SW to be installed in each HW to construct an Operational Environment based on the API type.



[Figure 1-3] Operational Environment based on the API type

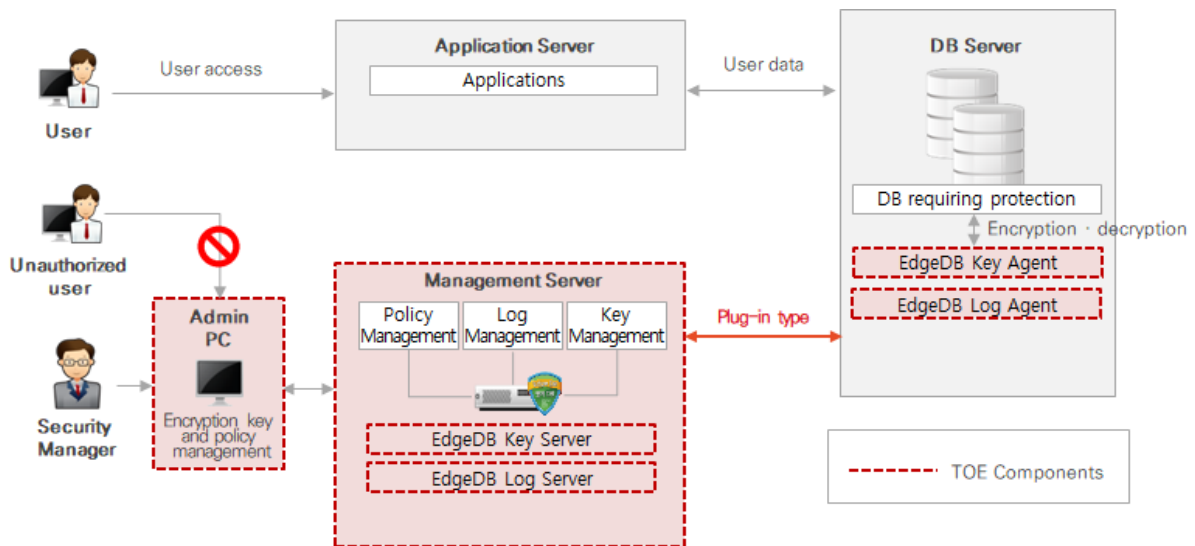
Correct TOE components must be installed to each HW, as in [Figure 1-3] above, to operate the TOE using the API type. And as for the Application Server, different TOE components should be installed depending on the Operational Environment of the Application Server. The following describes the TOE components to be installed, depending on the Operational Environment and HW conditions.

Classification	TOE Components	Third-party SW
Management Server	EdgeDB_Key_Server_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Server_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	jre 8u261 linux x64 MariaDB 10.4.14 x86_64 Apache-tomcat 8.5.57

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Application Server (Linux Environment)	EdgeDB_Key_Agent_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	jre 8u261 linux x64
Application Server (Windows Environment)	EdgeDB_Key_agent_4.0.4.11_win_64bit.exe EdgeDB_Log_agent_4.0.4.11_win_64bit.exe	jre 8u261 windows x64 Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.3050) (x64)


[Table 1-4] Operational Environment based on the API type



[Figure 1-4] Operational Environment based on the Plug-in type

Correct TOE components must be installed to each HW, as in [Figure 1-4] above, to operate the TOE using the plug-in type. And as for the DB Server, different TOE components should be installed depending on the Operational Environment of the DB Server. The following describes the TOE components to be installed, depending on the Operational Environment and HW conditions.

Classification	TOE Components	Third-party SW
Management Server	EdgeDB_Key_Server_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Server_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	jre 8u261 linux x64 MariaDB 10.4.14 x86_64 Apache-tomcat 8.5.57


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Database Server (Linux Environment)	EdgeDB_Key_Agent_4.0.4.11_Linux-x86_64.run EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	jre 8u261 linux x64 Oracle Database 11g Release 2 (11.2.0.1.0) Enterprise Edition for Linux x86-64
Database Server (Windows Environment)	EdgeDB_Key_agent_4.0.4.11_win_64bit.exe EdgeDB_Log_agent_4.0.4.11_win_64bit.exe	jre 8u261 windows x64 Microsoft® SQL Server® 2012 Express (X64) Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.30501) (x64)

[Table 1-5] Operational Environment based on the Plug-in type

The following are minimum HW and SW requirements for TOE installation and operation.

Classification		Minimum Requirements	
Application Server for Windows	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	4GB or more
		HDD	At least 200MB to install the TOE
		NIC	At least one or more 10/100/1000 Base-T Port
	SW	OS	Windows Server 2012 R2 Standard (64bit)
		JRE	jre 8u261 windows x64
Application Server for Linux	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB to install the TOE
		NIC	At least one or more 10/100/1000 Base-T Port
	SW	OS	CentOS 6.10 x86_64 (Kernel 2.6.32-754)
		JRE	jre 8u261 linux x64
Database Server for Windows	HW	CPU	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz or higher
		RAM	4GB or more
		HDD	At least 200MB to install the TOE
		NIC	At least one or more 10/100/1000 Base-T Port
	SW	OS	Windows Server 2012 R2 Standard (64bit)
		DBMS	Microsoft® SQL Server® 2012 Express (X64)


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

		JRE	jre 8u261 windows x64
		VC++	Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.30501) (x64)
Database Server for Linux	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB to install the TOE
		NIC	At least one or more 10/100/1000 Base-T Port
	SW	OS	CentOS 6.10 x86_64 (Kernel 2.6.32-754)
		DBMS	Oracle Database 11g Release 2 (11.2.0.1.0) Enterprise Edition for Linux x86-64
		JRE	jre 8u261 linux x64
Management Server for Linux	HW	CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz or higher
		RAM	16GB or more
		HDD	At least 200MB to install the TOE
		NIC	At least one or more 10/100/1000 Base-T Port
	SW	OS	CentOS 6.10 x86_64 (Kernel 2.6.32-754)
		DBMS	MariaDB 10.4.14 x86_64
		JRE	jre 8u261 linux x64
		WAS	Apache-tomcat 8.5.57
Administrator PC for Windows	SW	ETC	Chrome 80.0 64bit

[Table 1-6] Minimum HW and SW Requirements for TOE Installation and Operation

The third-party SW used in the TOE's operational requirements described above performs the following roles:

Third-party SW	Role
jre 8u261 windows x64	Java Runtime Environment required for TOE components to function in a Windows operating environment
jre 8u261 linux x64	Java Runtime Environment required for TOE components to function in a Linux operating environment
Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.30501) (x64)	Visual C++ re-distribution package required for TOE components to function in a Windows operating environment

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


Microsoft® SQL Server® 2012 Express (x64)	DBMS service provided by TOE in a Windows operating environment using the plug-in type
Oracle Database 11g Release 2 (11.2.0.1.0) Enterprise Edition for Linux x86-64	DBMS service provided by TOE in a Linux operating environment using the plug-in type
MariaDB 10.4.14 x86_64	DB in Management Server used to save TSF data such as cryptographic key
Apache-tomcat 8.5.57	A Web-based dynamic application server that provides management services by forming a secure SSL security channel through the administrative interface of the EdgeDB Key Server. Uses cipher suite of [Table 1-3] to form secure SSL security channel.
Chrome 80.0 64bit	Web browser used to access the administrator interface

[Table 1-7] The Role of Third-party SW used in TOE

A separate and external IT entity is required to operate the TOE. External IT entity other than those required by the TOE for evaluation include the following:

Classification	Description
Mail Server	Server to send email to authorized administrator(s) when the system detects potential security violations

[Table 1-8] External IT Entity

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1.4. TOE Description


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

1.4.1. Physical Scope of the TOE

TOE's physical scope and boundary include the EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, EdgeDB Log Agent; and guidance, namely EdgeDB v4.0 Preparative Procedure (PRE), EdgeDB v4.0 Operational User Guidance (OPE), and EdgeDB v4.0 Developer User's Guidance (DUG).

The TOE consists of SW and Guidances, as depicted of [Table 1-9] below.

Classification		Contents	TOE Scope	File Format	Distribution Format
TOE Components	EdgeDB Key Agent	EdgeDB Key Agent v4.0.4.11 for Windows - EdgeDB_Key_agent_4.0.4.11_win_64bit.exe EdgeDB Key Agent v4.0.4.11 for Linux - EdgeDB_Key_Agent_4.0.4.11_Linux-x86_64.run	O	S/W	CD
	EdgeDB Log Agent	EdgeDB Log Agent v4.0.4.11 for Windows - EdgeDB_Log_Agent_4.0.4.11_win_64bit.exe EdgeDB Log Agent v4.0.4.11 for Linux - EdgeDB_Log_Agent_4.0.4.11_Linux-x86_64.run	O	S/W	CD
	EdgeDB Key Server	EdgeDB Key Server v4.0.4.11 - EdgeDB_Key_Server_4.0.4.11_Linux-x86_64.run	O	S/W	CD
	EdgeDB Log Server	EdgeDB Log Server v4.0.4.11 - EdgeDB_Log_Server_4.0.4.11_Linux-x86_64.run	O	S/W	CD
Guidance		EdgeDB v4.0 Preparative Procedure(PRE) v1.9 - EdgeDB v4.0_Preparative Procedure(PRE)_v1.9.pdf	O	PDF	CD
		EdgeDB v4.0 Operational User Guidance(OPE) v1.8 - EdgeDB v4.0_Operational User Guidance(OPE)_v1.8.pdf			
		EdgeDB v4.0 Developer User's Guidance(DUG) v1.6 - EdgeDB v4.0_Developer User's Guidance (DUG)_v1.6.pdf			
Third-party SW	MariaDB 10.4.14 x86_64 - mariadb-10.4.14-linux-x86_64.tar.gz Apache-tomcat 8.5.57 - apache-tomcat-8.5.57.tar.gz Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.30501) (x64)	X	S/W	Distributed through a separate CD	

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	- vcredist_x64.exe			
validated cryptographic module	USCryptoLib V1.2	O	S/W	Distributed as part of TOE component

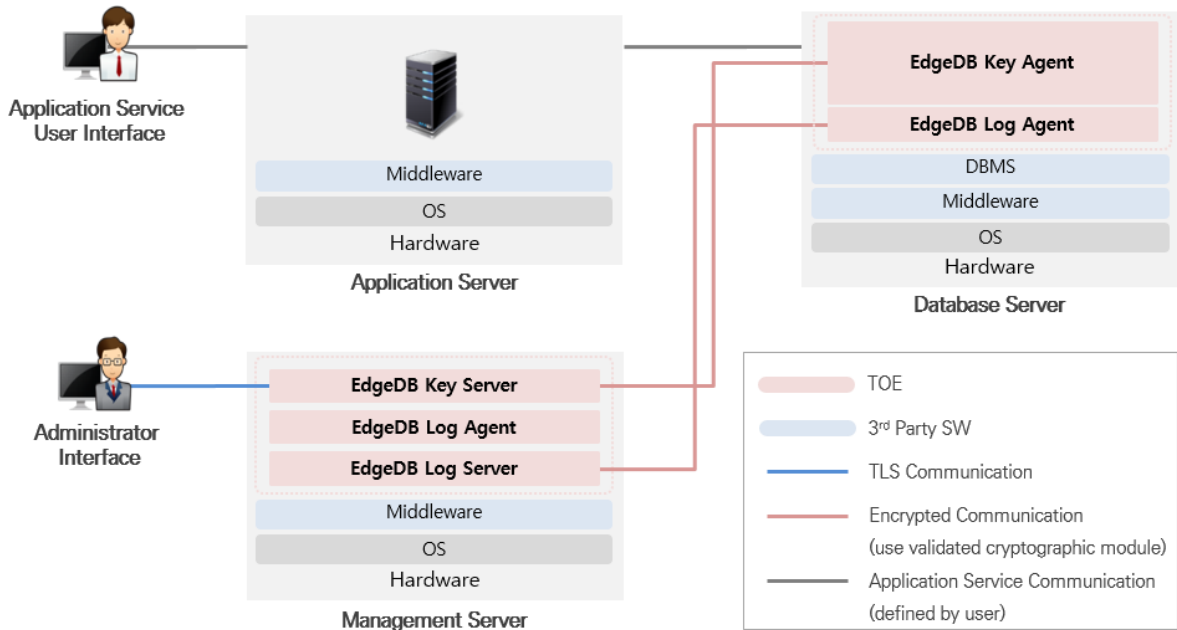
[Table 1-9] Physical Scope of the TOE

Validated cryptographic module used by the TOE

Cryptographic module name	Validated cryptographic module info	TOE used
USCryptoLib V1.2	Verification No. : CM-148-2023.12 Verified Date : 2018.12.05	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 depicted below on [Figure 1-5] and [Figure 1-6].



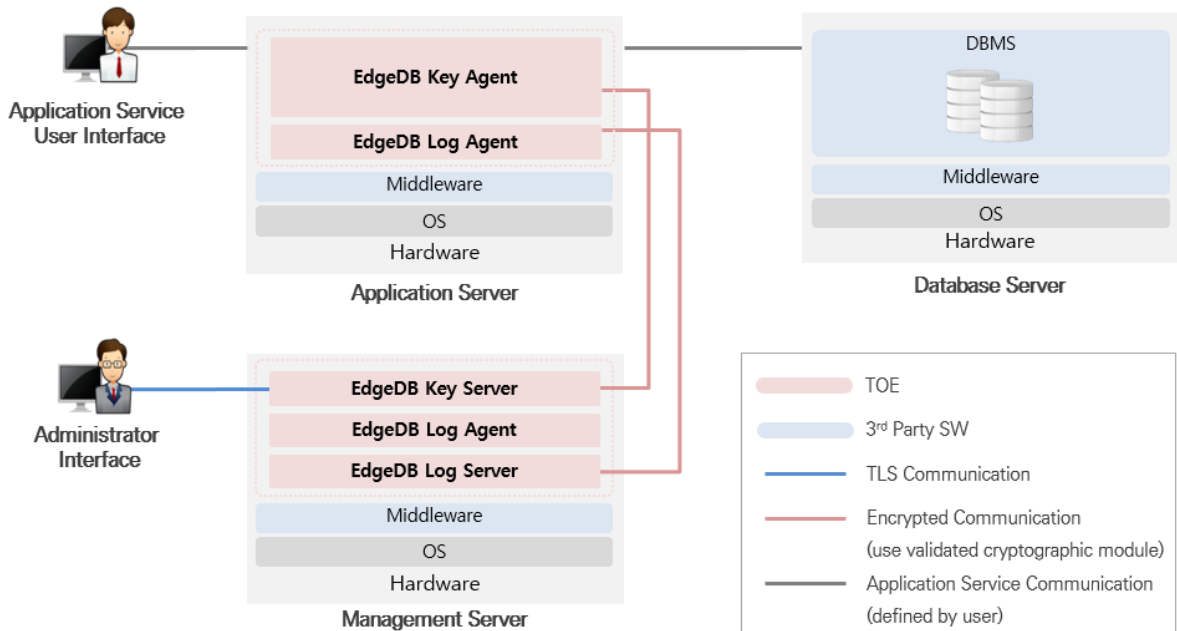
[Figure 1-5] Physical Scope of the TOE (plug-in type)

In the case of the plug-in type, the EdgeDB Key Agent is installed within the DB Server, where the protected DB exists. The EdgeDB Key Server and EdgeDB Log Server are both installed within a

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

physically identical Management Server, and the EdgeDB Log Agent is installed in all servers with TOE components installed in them.


Since the Database Server encrypts and decrypts user data by SQL Query, it is necessary to develop a plug-in function to be executed by modifying the query transmitted from the Application Server to the Database Server.



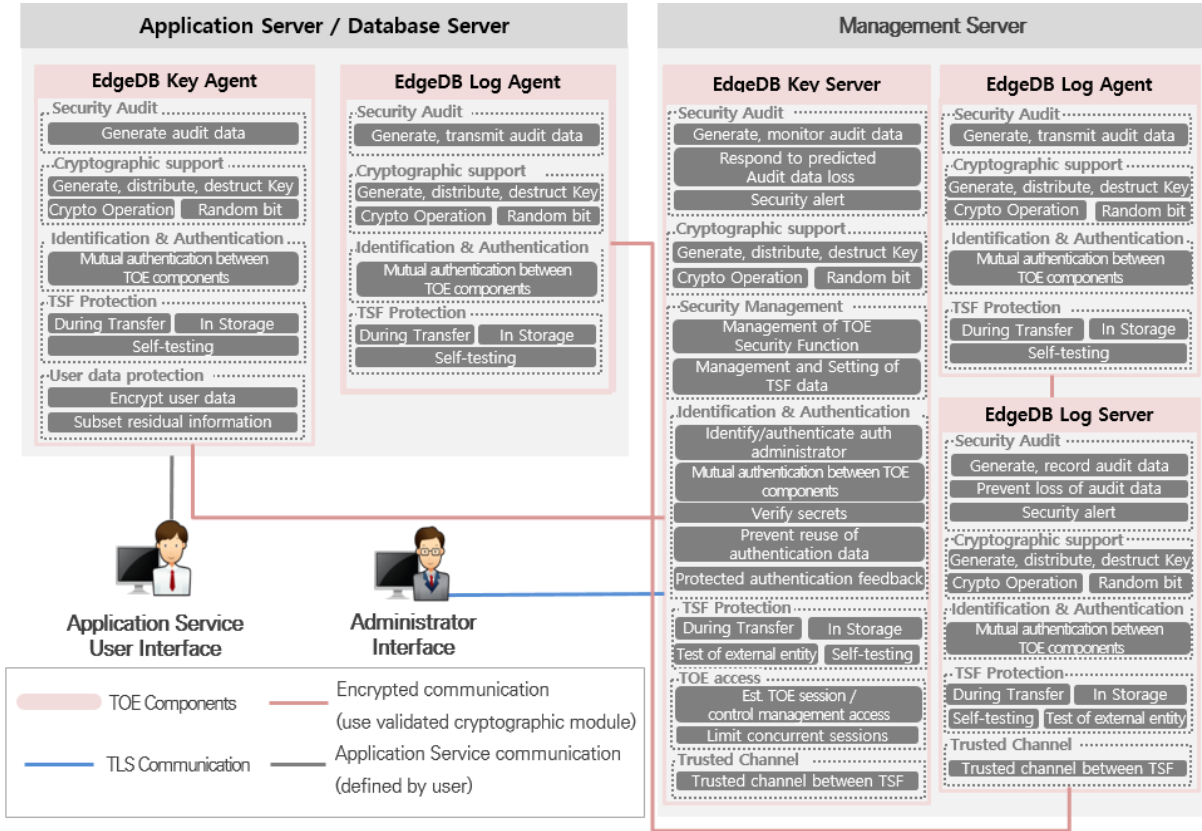
[Figure 1-6] Physical Scope of the TOE (API type)

In the case of the API type, EdgeDB Key Agent is installed on the Application Server. The EdgeDB Key Server and EdgeDB Log Server are both installed within a physically identical Management Server, and the EdgeDB Log Agent is installed in all servers with TOE components installed in them. User data will be encrypted before being transmitted from the Application Server to the Database Server, and decryption occurs after user data is received from the Database Server. Therefore, it should be developed to perform encryption and decryption for user data that is the target of encryption in the Application Server's Source Code.

The HW platform and OS(Operating System) where TOE is installed, and third-party SW required to operate the TOE, such as DBMS, are excluded from the scope of the TOE.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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 that records the date, time, IP, type of event, subject of event, and event history, etc.

The EdgeDB Key Server is installed on the same server as the EdgeDB Log Server, providing access to the DB where audit data is stored, and allowing the authorized administrator to search and view all security audit data through the administrator page provided by the EdgeDB Key Server. The retrieved data can be sorted in ascending or descending order according to the date and time of occurrence or storage. If certain security audit data requires revision, specific conditions can be applied to allow for review by selective audit data filtering.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

EdgeDB Key Server also provides selective audit data generation function. At the time of developing the security policy, the library module of the EdgeDB Key Agent can be used to select whether encryption/decryption/success/fail events are to be included in the list which is subject to audit.

The EdgeDB Key Server sends a real-time alert email to the registered email of the chief administrator, provided that the administrator had activated the list to receive such email, in case of potential violations in each TOE requiring audit (authentication failure of the administrator, process verification failure of EdgeDB Log Server and EdgeDB Key Agent, integrity violation, self-testing failure of validated cryptographic module, expired license, etc.)


② Cryptographic Support (FCS)

The EdgeDB Key Server performs the following cryptographic support: mutual authentication with TOE components, protect the transmission of TSF data, protect stored TSF data, encrypt user data, and verification of TSF/TSF data integrity, etc.

- Cryptographic key generation: generate Master Key, Local Key, Audit Key, Auth Key Pair, Session Key, User data Key with a cryptographic algorithm and cryptographic key length in accordance with [Table 5-4] and [Table 5-5].
- Cryptographic key distribution: online or offline distribution of Audit Key, Auth Key, Use data Key using the method depicted of [Table 5-6].
- Cryptographic operation: perform the cryptographic operation of TSF data using cryptographic algorithms of [Table 5-9].
- Cryptographic Key Destruction: TOE will overwrite the cryptographic key and critical security parameter with zero twice, as of [Table 5-7].

③ Identification and Authentication (FIA)

Enabling access to the security management function provided by the EdgeDB Key Server requires identity verification via identification and authentication process, which is carried out prior to all actions of the authorized administrator for access to any of the security functions. All administrators' passwords must meet the combination rules regarding the use of the English alphabet, numbers, and special characters, and all passwords entered during the password creation, modification, and authentication of passwords are masked with ("*").

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Feedback is not provided for cases of authentication failure. If login attempt fails over a certain number of times (default: 5 times, or set 3~10 times), identification and authentication function is deactivated for 5 minutes.

The Edge DB Key Server prevents re-use of authentication sessions, by issuing a session ID guaranteeing the uniqueness of authentication sessions for the authorized administrator(s).

In the case of authentication request by the EdgeDB Key Agent, the EdgeDB Key Server performs mutual authentication through the creation and validation of mutual signatures by Auth Key Pair.

④ Security Management (FMT)

Through the administrator page, the EdgeDB Key Server provides security management functions, such as setting and managing security policies and confidential data, and it allows all authorized administrators to modify the ID and/or password upon initial access.


The administrator group is divided into two groups, the chief administrator who is generated at the time of the system's inception, and general administrator(s) who can be generated by the chief administrators. The only mandate of the general administrators is the monitoring function.

⑤ Protection of the TSF (FPT)

The EdgeDB Key Server checks the normal operation of the Mail Server and local DB according to the conditions set forth by the TOE and alert to the administrator in case of a problem, in order to ensure the normal operation of the external entity.

The EdgeDB Key Server protects stored TSF data such as administrator password, cryptographic key, CSP, TOE configuration values, and file-type audit data, etc. using ARIA-256-CBC encryption and self-implemented encoding techniques, and SHA-256 hash, etc. Cryptographic keys and CSP loaded into memory are stored in memory using self-implemented encoding techniques.

The EdgeDB Key Server uses ARIA-256-CBC encryption and SHA-256 hash to protect the TSF data to be transmitted to the EdgeDB Key Agent from exposure and modification.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

During server initiation, the EdgeDB Key Server periodically performs self-testing during the normal server operation term to check whether key TOE component-specific processes are running correctly, and also self-tests validated cryptographic module. Some TSF and TSF data are verified for integrity during either initiation, upon receiving a request, or periodically, and, if, in the case of integrity violation, the system notifies the authorized administrator.

⑥ TOE Access (FTA)

The security management interface of the EdgeDB Key Server controls TOE access to ensure that login is permitted for a registered IP address only. Using the security management interface provided by the EdgeDB Key Server, the administrator can add or modify IP addresses permitted for access, one at a time. By limiting the number of sessions that can simultaneously access the same interface, the system blocks concurrent access by an identical account and identical authority. In case of duplicate access attempts by identical account, the existing session is terminated until a new access attempt is made, and audit data is generated

Only one account is provided the mandate of the chief administrator. The system limits the number of general administrators for concurrent access (default: 5, or set 5~100). The security management interface session is automatically terminated 10 minutes after login.

⑦ Trusted path/channels (FTP)


The EdgeDB Key Server performs cryptographic communication using a cryptographic algorithm that satisfies TLS v1.2 and the complexity of 112 bits or more to safely send email containing critical information to the authorized administrator.

1.4.2.2. EdgeDB Log Server

① Security Audit (FAU)

EdgeDB Log Server generates audit data that records the date, time, IP, type of event, subject of event, and event history, etc.

Once EdgeDB Log Agent sends audit data from the server on which TOE components are installed, the data is stored in a local DB that exists on the Management Server on which EdgeDB Log Server is installed.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Setting notification for DB's audit data storage usage allows the user to specify a threshold between 60% to 90%, and an alert email is sent out to the authorized administrator if the usage exceeds the designated threshold. If audit trail storage is saturated, then audit data is no longer stored in the DB, and the system sends a security alert email to the authorized administrator designated by the chief administrator to inform that audit data can no longer be stored.

② Cryptographic Support (FCS)

EdgeDB Log Server performs the following cryptographic support: mutual authentication with TOE components, protect the transmission of TSF data, and verification of TSF and TSF data integrity, etc.

- Cryptographic key generation: generate Master Key, Session Key, Local Key with an cryptographic algorithm and cryptographic key length in accordance with [Table 5-4] and [Table 5-5].
- Cryptographic key distribution: online or offline distribution of Audit Key using the method depicted of [Table 5-6].
- Cryptographic operation: perform the cryptographic operation of TSF data using cryptographic algorithms of [Table 5-9].
- Cryptographic Key Destruction: TOE will overwrite the cryptographic key and critical security parameter with zero twice, as of [Table 5-7].


③ Identification and Authentication (FIA)

In the case of authentication request by the EdgeDB Log Agent, the EdgeDB Log Server performs mutual authentication through the creation and validation of mutual signatures by Auth Key Pair.

④ Protection of the TSF (FPT)

The EdgeDB Log Server protects stored TSF data such as cryptographic key, CSP, TOE configuration values, and file-type audit data, etc. using ARIA-256-CBC encryption and self-implemented encoding techniques, etc. Cryptographic keys and CSP loaded into memory are stored in memory using self-implemented encoding techniques.

The EdgeDB Log Server uses ARIA-256-CBC encryption and SHA-256 hash to protect the TSF data to be transmitted to the EdgeDB Log Agent from exposure and modification.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

During server initiation, the EdgeDB Log Server periodically performs self-testing during the normal server operation term to check whether key processes pertaining to the security function is running correctly, and also self-tests validated cryptographic module. Some TSF and TSF data are verified for integrity during either initiation, upon receiving a request, or periodically, and, if, in the case of integrity violation, the system notifies the authorized administrator.

⑤ Trusted path/channels (FTP)

The EdgeDB Log Server performs cryptographic communication using a cryptographic algorithm that satisfies TLS v1.2 and the complexity of 112 bits or more to safely send email containing critical information to the authorized administrator.

1.4.2.3. EdgeDB Key Agent

① Security Audit (FAU)


EdgeDB Key Agent generates audit data that records the date, time, IP, type of event, subject of event, and event history, etc. Library modules in the form of plug-in or API provided by EdgeDB Key Agent also generate audit data, and the information generated is the same.

② Cryptographic Support (FCS)

EdgeDB Key Agent performs the following cryptographic support: mutual authentication with TOE components, protect the transmission of TSF data, and verification of TSF and TSF data integrity, etc.

- Cryptographic key generation: generate Master Key, Session Key, Local Key with a cryptographic algorithms and cryptographic key length in accordance with [Table 5-4] and [Table 5-5].
- Cryptographic key distribution: online or offline distribution of Audit Key, User data Key, Auth Key, using the method depicted of [Table 5-6].
- Cryptographic operation: perform the cryptographic operation of TSF data using cryptographic algorithms of [Table 5-8] and user data using cryptographic algorithms of [Table 5-9].
- Cryptographic Key Destruction: TOE will overwrite the cryptographic key and critical security parameter with zero twice, as of [Table 5-7].

③ Protect User Data (FDP)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

EdgeDB Key Agent enables user data encryption, decryption or one-way encryption, empty value encryption, and double encryption by using different DB encryption policies for each column. After encryption and decryption, the plaintext information of user data is safely deleted from memory using the zeroing function to ensure unauthorized disclosure.

④ Identification and Authentication (FIA)

EdgeDB Key Agent can request EdgeDB Key Server for mutual authentication and perform mutual authentication through the creation and validation of mutual signatures by Auth Key Pair.

⑤ Protection of the TSF (FPT)

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

The EdgeDB Key Agent uses ARIA-256-CBC encryption and SHA-256 hash to protect the TSF data to be transmitted to the EdgeDB Key Server from exposure and modification.


During initiation, the EdgeDB Key Agent periodically performs self-testing during the normal server operation term to check whether key processes pertaining to the security function is running correctly, and also self-tests validated cryptographic module. Some TSF and TSF data are verified for integrity during either initiation, upon receiving a request, or periodically, and, if, in the case of integrity violation, the system notifies the authorized administrator.

1.4.2.4. EdgeDB Log Agent

① Security Audit (FAU)

EdgeDB Log Agent generates audit data that records the date, time, IP, type of event, subject of event, and event history, etc. Since EdgeDB Log Agent is installed in all physical servers with different TOE components, any audit data generated by other TOE components within physically identical servers (with EdgeDB Log Agent) is accessible. The generated audit data is transmitted to the EdgeDB Log Server.

② Cryptographic Support (FCS)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

EdgeDB Log Agent performs the following cryptographic support: mutual authentication with TOE components, protect the transmission of TSF data, and verification of TSF and TSF data integrity, etc.

- Cryptographic key generation: generate Session Key, Local Key with an cryptographic algorithms and cryptographic key length in accordance with [Table 5-4] and [Table 5-5].
- Cryptographic key distribution: online or offline distribution of Audit Key, Auth Key, using the method depicted of [Table 5-6].
- Cryptographic operation: perform the cryptographic operation of TSF data using cryptographic algorithms of [Table 5-9].
- Cryptographic Key Destruction: TOE will overwrite the cryptographic key and critical security parameter with zero twice, as of [Table 5-7].

③ Identification and Authentication (FIA)


EdgeDB Log Agent can request EdgeDB Log Server for mutual authentication and perform mutual authentication through the creation and validation of mutual signatures by Auth Key Pair.

④ Protection of the TSF (FPT)

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

The EdgeDB Key Agent uses ARIA-256-CBC encryption and SHA-256 hash to protect the TSF data to be transmitted to the EdgeDB Key Server from exposure and modification.

During server initiation, the EdgeDB Log Agent periodically performs self-testing during the normal server operation term to check whether key processes pertaining to the security function is running correctly, and also self-tests validated cryptographic module. Some TSF and TSF data are verified for integrity during either initiation, upon receiving a request, or periodically, and, if, in the case of integrity violation, the system notifies the authorized administrator.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1.5. Terms and Definitions

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

Approved cryptographic algorithm

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

Application Server

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

Assets

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

Assignment

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

Attack potential

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

Audit Key


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

Augmentation

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

Auth Key Pair

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Auth Priv Key

Private key among key pairs to perform mutual authentication.

Auth Pub Key

Public key among key pairs to perform mutual authentication.

Authentication Data

Information used to verify the claimed identity of a user.

Authorized Administrator

Users who operate and manage the TOE safely. (subdivided into Chief Administrator and General Administrator)

Authorized User

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

Chief Administrator

An authorized administrator of the person having the right to add, modify, delete the security features of the TOE and TSF data management.

Class

Set of CC families that share a common focus.

Classification for Execution


The behavior of the execution target that generated audit data is classified into inquiry, creation, modification, deletion, etc.

Column

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

Critical Security Parameters (CSP)

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Component

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

Database

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

Database Manager

A person who manages or manages data stored in a database in an accurate and integrated manner.

Database Server

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

DB table space usage

The percentage of the space used to store the actual data in the database object.

DBMS Account Information

Account information to access DBMS.

DBMS (Database Management System)


A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

Decryption

The act that restoring the cipher text into the plaintext using the decryption key.

Dependency

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Element

Indivisible statement of a security need.

Encryption

The act that converts the plaintext into the cipher text using the encryption key.

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.

Execution Object

It is a function that generates audit data and is classified into system, administrator, environment setting, agent, etc.

External Entity

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

Family

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

General Administrator

Among the authorized administrators, those who have only the authority to inquiry the security functions of the TOE and TSF data.

Identity


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

Iteration

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

License

File that allows the use of the TOE.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Local Key

Cryptographic Key that encrypts and decrypts TSF data existing in the server where EdgeDB Key Server, EdgeDB Key Agent, and EdgeDB Log Agent are installed among TOE components.

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, WARNING for selective review.

Management access

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

Master Key

Key that encrypts and decrypts another cryptographic key.

Master Password

Password to generate Master Key through PBKDF2-HMAC-SHA-256 algorithm by direct input by Authorized Administrator.

Object


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

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.

Operation(on a component of the CC)

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Operation(on a subject)

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

Organizational Security Policies

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

Personal Information

Information on a surviving individual that can identify the individual by name, resident registration number, etc. (Even if the information alone cannot identify a specific individual, it includes items that can be easily combined and identified with other information)

Private Key

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

Process

It is a program that drives each TOE component and is classified by the name of the application program that uses the Java Runtime Environment or the cryptographic library.

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type.

Public Key


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

Public Key(asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys.

Random bit generator (RBG)

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Refinement

Addition of details to a component.

Request IP

IP address of the client requesting administrator function with EdgeDB Key Server.

Result Code

Result code from audit data.

Result Message

Result message of audit data.

Role

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

Secret Key

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

Security Target (ST)

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

Security attribute


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

Selection

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

Self-test

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Sensitive Information

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

Session Key

Key used for encrypted communication between TOE components.

SSL (Secure Sockets Layer)

This is a security protocol proposed by Netscape to ensure confidentiality, integrity and security over a computer network.

Storage space usage Threshold

Standard value for sending security warning email on the use rate of DB table space where audit data is stored.

Subject

Active entity in the TOE that performs operations on objects.

Subject of Execution

This is the execution target that created the audit data, and the administrator's ID is the target.

Symmetric cryptographic technique


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

Target of Evaluation (TOE)

Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

Threat Agent

Entity that can adversely act on assets.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

TLS (Transport Layer Security)

This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246.

User

Refer to "External entity".

User Data


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

User data Key

Cryptographic Key to encrypt user data.

Zeroization

In order not to leave any residual data in the memory or the storage space of the file, the process of overwriting the data twice as long as 0 is repeated.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1.6. Conventions

This ST is consistent with the Common Criteria for Information Technology Security Evaluation and uses the same conventions for selection, assignment, iteration, refinement, and iteration.

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

Iteration

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

Assignment


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

Selection

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

Refinement

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

2. Conformance Claim

This section states the Common Criteria (CC), Protection Profile (PP), and Package complied by this ST, and describes how the PP and ST follows the PP.

2.1. CC Conformance claim

CC		<p>Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5</p> <ul style="list-style-type: none"> - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1r5 (CCMB-2017-04-001, April, 2017) - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1r5 (CCMB-2017-04-002, April, 2017) - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1r5 (CCMB-2017-04-003, April, 2017)
Conformance Format	Part 2 Security Functional Requirements	Extended: FCS_RBG.1, FIA_IMA.1, FDP_UDE.1, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security Assurance Requirements	<i>Conformant</i>
	Package	Augmented: EAL1 <i>augmented</i> (ATE.FUN.1)

[Table 2-1] Conformance to CC

2.2. PP conformance claim

This ST strictly complied with the 'National PP of Database Encryption V1.1'(KECS-PP-0820a-2017_PP_KR).'


Classification	PP	ST	Rationale
Type of TOE	DB Encryption	DB Encryption	Same as PP
Security	FAU_ARP.1	FAU_ARP.1	Same as PP
Function	FAU_GEN.1	FAU_GEN.1	Same as PP



EdgeDB v4.0

	Title	Version
	Security Target(ST) for Public	1.5

Requirement (SFR)	FAU_SAA.1	FAU_SAR.1	Same as PP
	FAU_SAR.1	FAU_SAR.1	Same as PP
	FAU_SAR.3	FAU_SAR.3	Same as PP
	FAU_SEL.1	FAU_SEL.1	Same as PP
	FAU_STG.3	FAU_STG.3	Same as PP
	FAU_STG.4	FAU_STG.4	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.4	FCS_CKM.4	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(Extended)	FCS_RBG.1(Extended)	Same as PP
	FDP_UDE.1(Extended)	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(Extended)	FIA_IMA.1(Extended)	Same as PP
	FIA_SOS.1	FIA_SOS.1	Same as PP
	FIA_UAU.1	FIA_UAU.2	Limited than PP and requirements (Hierarchical relation)
	FIA_UAU.4	FIA_UAU.4	Same as PP
	FIA_UAU.7	FIA_UAU.7	Same as PP
	FIA_UID.1	FIA_UID.2	Limited than PP and requirements (Hierarchical relation)
	FMT_MOF.1	FMT_MOF.1	Same as PP
	FMT_MTD.1	FMT_MTD.1	Same as PP
	FMT_PWD.1(Extended)	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_ITT.1	FPT_ITT.1	Same as PP
	FPT_PST.1(Extended)	FPT_PST.1(Extended)	Same as PP
	FPT_STM.1	FPT_STM.1	Same as PP

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


	FPT_TEE.1	FPT_TEE.1	Same as PP
	FPT_TST.1	FPT_TST.1	Same as PP
	FTA_MCS.2	FTA_MCS.2	Same as PP
	FTA_SSL.5(Extended)	FTA_SSL.5(Extended)	Same as PP
	FTA_TSE.1	FTA_TSE.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

This ST conforms to PP assurance requirement package EAL 1, augmented with the following.

- Assurance Package : EAL1 *augmented*(ATE_FUN.1)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

3. Security Objectives

This ST defines the security objective by dividing it into two categories: TOE security objective and security objective for the operational environment. TOE security objective is those objectives directly addressed by the TOE. And the security objective for the operational environment is those objectives handled through technical and procedural means supported by the operational environment to ensure that the TOE can accurately provide security functionality.

3.1. Security Objectives for the Operational Environment

The following are the security objectives handled through technical and procedural means supported by the operational environment to provide TOE security functionality accurately.

OE.Physical Security (OE.PHYSICAL_CONTROL)

The place of TOE installation and operation shall be equipped with access control and protection facilities so that only authorized administrator can access.


OE.Trusted Administrator (OE.TRUSTED_ADMIN)

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

OE.Safe Channel (OE.SAFE_CHANNEL)

Safe channel should be managed to ensure secure communication between authorized administrator of the TOE and WAS, the operating environment of the Management Server. To configure a safe channel, use the TLS v1.2 protocol provided by WAS by following the Preparative Procedure (PRE) supplied with the TOE.

※ In accordance with the disclaimer for when applying FTP_TRP.1 (within the Protection Profile complied with by this ST), which states "the following security functional requirement can be applied if implemented through the communication between the administrator PC's web browser and the Management Server (TOE component). If management access is provided through the communication between the administrator PC's web browser and the webserver (operating environment of the Management Server), then the author of the ST shall replace the security functional requirement with security objective for operation."

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

OE.Secure Development (OE.SECURE_DEVELOPMENT)

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

OE.Log Backup (OE.LOG_BACKUP)

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

OE.Operation System Reinforcement (OE.OPERATION SYSTEM_REINFROCEMENT)


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

OE.Time Stamp (OE.TIME_STAMP)

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

OE.Audit Data Protection

The DBMS interacting with the TOE stores audit trail records, and hence should be protected from unauthorized deletion or modification.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

4. Extended components definition

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

Cryptographic support

- FCS_RBG.1 Random bit generation

Identification & authentication

- FIA_IMA.1 TOE Internal mutual authentication

User data protection

- FDP_UDE.1 User data encryption

Security Management

- FMT_PWD.1 Management of ID and password

Protection of the TSF

- FPT_PST.1 . Basic protection of stored TSF data

TOE Access

- FTA_SSL.5 Management of TSF-initiated sessions

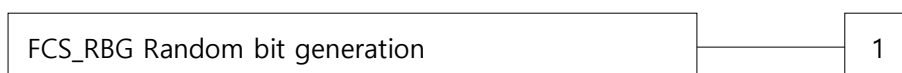
4.1. Cryptographic support

4.1.1. Random Bit Generation


Family Behaviour

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

Component leveling



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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen

4.1.1.1. FCS_RBG.1 Random bit generation

Hierarchical to No other components.

Dependencies No dependencies.

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

4.2. Identification & authentication

4.2.1. TOE Internal mutual authentication

Family Behaviour

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

Component leveling




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

Management: FIA_IMA.1

There are no management activities foreseen.

Audit: FIA_IMA.1

The following actions are recommended to record if FAU_GEN Security audit data generation

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

family is included in the PP/ST:

- a) Minimal: Success and failure of mutual authentication
- b) Minimal: Modification of authentication protocol

4.2.1.1. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components.

Dependencies No dependencies.

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

4.3. User data protection

4.3.1. User data encryption

Family Behaviour

This family provides requirements to ensure confidentiality of user data.

Component leveling



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

Management : FDP_UDE.1


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

- a) Management of user data encryption/decryption rules

Audit : FDP_UDE.1

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

- a) Minimal : Success and failure of user data encryption/decryption

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

4.3.1.1. FDP_UDE.1 User data encryption

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

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

4.4. Security Management

4.4.1. ID and password

Family Behaviour

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

Component leveling



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

Management: FMT_PWD.1

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

- a) Management of ID and password configuration rule


Audit: FMT_PWD.1

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

- a) Minimal: All changes of the password.

4.4.1.1. FMT_PWD.1 Management of ID and password

Hierarchical to No other components.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- Dependencies FMT_SMF.1 Specification of management functions
 FMT_SMR.1 Security roles
- FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: list of functions] to [assignment: the authorized identified roles].
 1. [assignment: password combination rules and/or length]
 2. [assignment: other management such as management of special characters unusable for password, etc.]
- FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: list of functions] to [assignment: the authorized identified roles].
 1. [assignment: ID combination rules and/or length]
 2. [assignment: other management such as management of special characters unusable for ID, etc.]
- FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time]

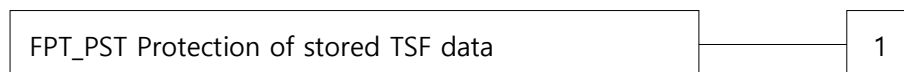
4.5. Protection of the TSF

4.5.1. Protection of stored TSF data


Family Behaviour

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

Component leveling



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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

4.5.1.1. FPT_PST.1 Basic protection of stored TSF data

Hierarchical to No other components.

Dependencies No dependencies.

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

4.6. TOE Access

4.6.1. Session locking and termination


Family Behaviour

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

Component leveling



In CC Part 2, the session locking and termination family consists of four components. In this PP, it

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

consists of five components by extending one additional component as follows.

※ The relevant description for four components contained in CC Part 2 is omitted.

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

Management: FTA_SSL.5

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

- a) Specification for the time interval of user inactivity that is occurred the session locking and termination for each user
- b) Specification for the time interval of default user inactivity that is occurred the session locking and termination

Audit: FTA_SSL.5

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


- a) Minimal: Locking or termination of interactive session

4.6.1.1. FTA_SSL.5 Management of TSF-initiated sessions

Hierarchical to No other components.

Dependencies [FIA_UAU.1 Timing of authentication or No dependencies.]

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


5. Security Requirements

The security requirements section describes the security functional requirements and assurance requirements that the TOE shall satisfy.

5.1. Security Functional Requirements


The security functional requirements defined in this ST are expressed by selecting the relevant security components from the extended component definitions in CC Part 2 and Chapter 4.

Security Functional Classes	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_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	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.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
User Data Protection (FDP)	FDP_UDE.1(Extended)	User data encryption
	FDP_RIP.1	Subset residual information protection
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1 (Extended)	TOE internal mutual authentication

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	Authentication
	FIA_UAU.4	Single-use authentication mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	Identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(1) (Extended)	Management of ID and password
	FMT_PWD.1(2) (Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1 (Extended)	Basic protection of stored TSF data
	FPT_STM.1	Reliable time stamps
	FPT_TEE.1	Testing of external entities
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA.MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5 (Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel

[Table 5-1] Security Functional Requirements (SFR)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.1.1. Security Audit (FAU)

5.1.1.1. FAU_ARP.1 Security alarms

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


FAU_ARP.1.1 The TSF shall take [
a) Generate warning message to the administrator's page
b) Send email to the administrator designated by the chief administrator
c) Disable access to the administrator menu] upon detection of a potential security violation.

5.1.1.2. FAU_GEN.1 Audit data generation


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

FAU_GEN.1.1 The TSF shall be able to generate audit record of the following auditable events:
 a) Start-up and shutdown of the audit functions;
 b) All auditable events for the *not specified* level of audit; and
 c) [Refer to "auditable events" in [Table 5-2], *None*]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
 a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
 b) For each audit event type, based on the auditable event definitions of the functional components included in PP/ST [Refer to the contents of "Additional audit record" in [Table 5-2] Audit events, [date and time of Occurrence/Save AND Occurrence/Request IP AND Log classification AND Log level AND Occurrence Module AND Process AND Execution Object AND Subject of Execution AND Classification for Execution AND Results code AND Results message]]

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

		or execution code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.5	Locking or termination of interactive sessions	
FTA_TSE.1	Denial of session establishment due to the session establishment mechanism All attempts at establishment of a user session	
FTP_ITC.1	All attempts made to use trusted channel function	
FPT_TEE.1	Execution of the tests of the external entities and the results of the tests	

[Table 5-2] Audit event


5.1.1.3. FAU_SAA.1 Potential violation analysis

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

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

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

- a) Accumulation or combination of [authentication failure audit event among auditable events of FIA_UAU.2, integrity violation audit event and selftest failure event of validated cryptographic module among auditable events of FPT_TST.1, [verification failure of major security function processes, license expiration, failure to save audit log] known to indicate a potential security violation.
- b) [Activation of FAU_ARP.1 in case of accumulation of failed attempts at authentication above the number designated by the chief administrator from auditable events under FIA_UAU.2, Activation of FAU_ARP.1 in case of audit event of integrity violation and validated cryptographic module self-testing failure from auditable events under FPT_TST.1, verification

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

failure of major security function processes, exceeding the DB table space usage rate threshold specified in FAU_STG.3, license expiration, and Activation of FAU_ARP.1 in case of failure to save audit log]

5.1.1.4. FAU_SAR.1 Audit review

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

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


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

5.1.1.5. FAU_SAR.3 Selectable audit review

Hierarchical to No other components
 Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the capability to apply [date and time of occurrence AND Occurrence IP AND Request IP AND Log classification AND Log level AND occurred module AND success or failure AND the result code AND number of posts] of audit data based on [select, and sort based on ascending/descending order of date and time of occurrence/storage].

Selection Criteria (AND)	Permitted Functions
Date and time of occurrence	Selective search and sorting based on ascending/descending order of date and time of occurrence/storage
Occurrence IP	
Requested IP	
Log classification	
Log level	
Occurred module	
Success or failure	

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Result code	
No. of posting	

[Table 5-3] Type of Audit Data and Selection Criteria

5.1.1.6. FAU_SEL.1 Selective audit

Hierarchical to No other components
 Dependencies FAU_GEN.1 Audit data generation
 FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes.
 a) Event type
 b) [Encryption and decryption log { combination of [*encryption, decryption, success, failure*] }]

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

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


FAU_STG.3.1 The TSF shall [Notification to the authorized administrator, [None] if the audit trail exceeds [the percentage of the DB table space usage rate (60%~90%) set by the chief administrator]].

5.1.1.8. FAU_STG.4 Prevention of audit data loss

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

FAU_STG.4.1 The TSF shall ignore audited events and [send email alert to the administrator authorized by the chief administrator of audit storage failure] if the audit trail is full.

5.1.2. Cryptographic Support (FCS)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.1.2.1. FCS_CKM.1(1) Cryptographic key generation (User Data Encryption)

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Key generation algorithm of [Table 5-4]] and specified cryptographic key sizes [Cryptographic key size of [Table 5-4]] that meet the following: [Standard list of [Table 5-4]].

Standard list	Key generation algorithm	Cryptographic key size
TTAK.KO-12.0191	HMAC-DRBG-SHA512	256 bits

[Table 5-4] Key Generation Algorithm used by TOE to generate cryptographic Key for User Data


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

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

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

Standard list	Key generation algorithm	Key size
TTAK.KO-12.0334-Part1, TTAK.KO-12.0334-Part2	PBKDF(HMAC-SHA256)	256 bits
TTAK.KO-12.0191	HMAC-DRBG-SHA512	256 bits
TTAK.KO-12.0191	HMAC-DRBG-SHA512	256 bits
ISO/IEC 11770-3	ECDH(ECC-P256)	256 bits
ISO/IEC 14888-2	RSA-PSS	2048 bits

[Table 5-5] Key Generation Algorithm used by TOE to generate cryptographic Key for TSF Data


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.1.2.3. 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] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall destruct cryptographic keys in accordance with a specified cryptographic key distribution method [Cryptographic key distribution Method of [Table 5-6]] that meet the following: [Standard list of [Table 5-6]].

Standard list	TOE (Sender)	TOE (Receiver)	Cryptographic Key	Distribution Method
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Pub Key (Server)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Priv Key (Agent)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Pub Key (Server)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Priv Key (Agent)	Distribute offline during installation, and insert the key using 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 and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash values, to Session Key
ISO/IEC 11770-3, KS X 1213, ISO/IEC	EdgeDB Log Server	EdgeDB Log Agent	Audit Key	Hash using the SHA256 cryptographic algorithm and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

10118-3				values, to Session Key
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 and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash values, to Session Key


[Table 5-6] Cryptographic key distribution method

5.1.2.4. FCS_CKM.4 Cryptographic key destruction


Hierarchical to No other components
 Dependencies [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destruct cryptographic keys in accordance with the specified cryptographic key destruction method [[Table 5-7] Destruction method] that meets the following: [None].

Cryptographic Key	TOE	Location	Destruction method	Timing of destruction
User data Key	EdgeDB Key Agent	Memory	Zeroization	Immediately after encrypting and decrypting user data
Master Password	EdgeDB Key Server	Memory	Zeroization	Immediately upon generating the Master Key
	EdgeDB Key Agent	Memory	Zeroization	Immediately upon generating the Master Key
	EdgeDB Log Server	Memory	Zeroization	Immediately upon generating the Master Key
	EdgeDB Key Agent	Memory	Zeroization	Immediately upon generating the Master Key


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Log Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	key file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	key file	Overwrite the file area with zero then delete	When deleting 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
Session Key	EdgeDB Key Server	Memory	Zeroization	When terminating the session
	EdgeDB Log Server	Memory	Zeroization	When terminating the session
	EdgeDB Key Agent	Memory	Zeroization	When terminating the session
	EdgeDB Log Agent	Memory	Zeroization	When terminating the session
Auth Key Pair	EdgeDB Key Server	key file	Overwrite the file area with zero then delete	When deleting the TOE

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	EdgeDB Key Server	Memory	Zeroization	After generating signature value
	EdgeDB Log Server	Memory	Zeroization	After generating signature value
	EdgeDB Key Agent	key file (personal key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Key Agent	key file (server public key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Key Agent	Properties file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Agent	Memory	Zeroization	After generating signature value
	EdgeDB Log Agent	key file (personal key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Log Agent	key file (server public key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Log Agent	Properties file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Log Agent	Memory	Zeroization	After generating signature value
ECDH Private Key	EdgeDB Key Server	Memory	Zeroization	When generating the Session Key
	EdgeDB Log Server	Memory	Zeroization	When generating the Session Key
	EdgeDB Key Agent	Memory	Zeroization	When generating the Session Key
	EdgeDB Log Agent	Memory	Zeroization	When generating the Session Key

[Table 5-7] Cryptographic Key Destruction Method

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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

Hierarchical to No other components
 Dependencies [FDP_ITC.1 Import of user data without security attributes, or
 FDP_ITC.2 Import of user data with security attributes, or
 FCS_CKM.1 Cryptographic key generation]
 FCS_CKM.4 Cryptographic key destruction


FCS_COP.1.1 The TSF shall perform [Operations list of [Table 5-8]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 5-8]] and cryptographic key sizes [Key size of [Table 5-8]] that meet the following: [Standard list of [Table 5-8]].

Standard list	Cryptographic algorithms	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
ISO/IEC 10118-3	SHA384	None	None	None	Hash
ISO/IEC 10118-3	SHA512	None	None	None	Hash

[Table 5-8] Cryptographic Operation of User Data

5.1.2.6. FCS.COP.1(2) Cryptographic operation (TSF data encryption)

Hierarchical to No other components
 Dependencies [FDP_ITC.1 Import of user data without security attributes, or
 FDP_ITC.2 Import of user data with security attributes, or
 FCS_CKM.1 Cryptographic key generation]
 FCS_CKM.4 Cryptographic key destruction

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

FCS_COP.1.1 The TSF shall perform [Operations list of [Table 5-9]] in accordance with a specified cryptographic algorithm [Cryptographic algorithms of [Table 5-9]] and cryptographic key sizes [Key size of [Table 5-9]] that meet the following: [Standard list of [Table 5-9]].

Standard list	Cryptographic algorithms	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 9792-2	HMAC-SHA256	256 bits	None	None	Integrity verification
ISO/IEC 14888-2	RSA-PSS	2048 bits	None	None	Signature generation and verification

[Table 5-9] Cryptographic Operation of TSF Data

5.1.2.7. FCS_RBG.1 Random bit generation (extended)

Hierarchical to No other components
 Dependencies No dependencies


FCS_RBG.1.1 The TSF shall generate random bits required to generate an cryptographic key using the specified random bit generator that meets the following [TTAK.KO 12.0191].

5.1.3. User Data Protection (FDP)

5.1.3.1. FDP_UDE.1 User data encryption (extended)

Hierarchical to No other components
 Dependencies FCS_COP.1 Cryptographic operation

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.1.3.2. FDP_RIP.1 Subset residual information protection

Hierarchical to No other components
 Dependencies No dependencies

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

5.1.4. Identification and Authentication (FIA)

5.1.4.1. FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.1 The TSF shall detect when "an administrator configurable positive integer within [3~10]" 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 (default: 5 minutes)].

5.1.4.2. FIA_IMA.1 TOE Internal mutual authentication

Hierarchical to No other components
 Dependencies No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication using [Authentication protocol of [Table 5-10]] in accordance with [Standard list of [Table 5-10]] between [TOE components of [Table 5-10]].

Standard list	TOE components	Authentication protocol
None	EdgeDB Key Agent, EdgeDB Key Server	Mutual signature verification through

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

		Pre-Auth Key distribution
None	EdgeDB Log Agent, EdgeDB Log Server	Mutual signature verification through Pre-Auth Key distribution

[Table 5-10] Mutual Authentication method between TOE Components

5.1.4.3. FIA_SOS.1 Verification of secrets

Hierarchical to No other components
 Dependencies No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [three combinations of the English alphabet (52 letters : a ~ z, A ~ Z) / Numbers (10 strings : 0 ~ 9) / special characters (32 characters : `~!@#\$\$%^&*()-_+=[{}|;:~".<>/?), where the combination rules dictate that digits be between 9 ~ 20]

5.1.4.4. FIA_UAU.2 User authentication before any action

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

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


5.1.4.5. FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to No other components
 Dependencies No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [Password Authentication Method].

5.1.4.6. FIA_UAU.7 Protected authentication feedback

Hierarchical to No other components

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Dependencies FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [Masking (example: "****"), which is invisible on the screen as the password is being typed, and blinds the reason for failure in the event of identification of authentication failure] to the user while the authentication is in progress.

5.1.4.7. FIA_UID.2 User identification before any action

Hierarchical to FIA_UID.1 Timing of identification

Dependencies No dependencies

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

5.1.5. Security Management (FMT)


5.1.5.1. FMT_MOF.1 Management of security functions behaviour

Hierarchical to No other components

Dependencies FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF1.1 The TSF shall restrict the ability to ***conduct management actions of*** the functions [Security functions behavior of [Table 5-11]] to [Administrator of [Table 5-11]].

Administrator	Security functions behavior
Chief Administrator	Modify or query rules regarding potential security violations
Chief Administrator	Modify or query actions to be taken in case of imminent audit storage failure
Chief Administrator	Modify, delete, and query - EdgeDB Key Agent
Chief Administrator	Modify, delete, quire, and add - DB encryption policy
General Administrator	Query rules concerning potential security violations
General Administrator	Query responses in the case of anticipated audit storage failure
General Administrator	Query EdgeDB Key Agent

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

General Administrator	Query DB encryption policy
-----------------------	----------------------------


[Table 5-11] Security function behavior of administrator

5.1.5.2. FMT_MTD.1 TSF 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 and management ability of [Table 5-12]] to [Administrator of [Table 5-12]].

Administrator	TSF data and management ability
Chief Administrator	Modify the master password
Chief Administrator	Modify audit data generation settings for success and failure events of user data encryption and decryption
Chief Administrator	Query, add, modify, or delete cryptographic key
Chief Administrator	Query audit data
Chief Administrator	Query or modify the storage space usage threshold for audit data
Chief Administrator	Query or modify the maximum number of allowable failed authentication attempts
Chief Administrator	Modify authentication data of chief administrator, modify authentication data of general administrator
Chief Administrator	Query or modify the identity of chief administrator; query, modify, add, or delete the identity of general administrator
Chief Administrator	Query or modify the maximum number of concurrent sessions for general administrators
Chief Administrator	Query, modify, add, or delete IP addresses access for security management
General Administrator	Query administrators
General Administrator	Query cryptographic key
General Administrator	Query audit data
General Administrator	Query the storage space usage threshold for audit data
General Administrator	Query the maximum number of allowable failed authentication attempts
General Administrator	Modify authentication data by the user

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

General Administrator	Query user identity
General Administrator	Query the maximum number of concurrent sessions for general administrators
General Administrator	Query IP addresses accessed for security management


[Table 5-12] TSF Data and management ability

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

Hierarchical to	No other components
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [None] to [None]. 1. [None] 2. [None]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [None] to [None]. 1. [None] 2. [None]
FMT_PWD.1.3	The TSF shall provide the capability for <u>changing the ID and password when the authorized chief administrator accesses for the first time.</u>

5.1.5.4. FMT_PWD.1(2) Management of ID and Password (Extended)

Hierarchical to	No other components
Dependencies	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles
FMT_PWD.1.1	The TSF shall restrict the ability to manage the password of [None] to [None]. 1. [None] 2. [None]
FMT_PWD.1.2	The TSF shall restrict the ability to manage the ID of [None] to [None].

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

1. [None]

2. [None]

FMT_PWD.1.3 The TSF shall provide the capability for changing the password when the authorized general administrator accesses for the first time.

5.1.5.5. FMT_SMF.1 Specification of management functions

Hierarchical to No other components

Dependencies No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- a) Management functions specified in FMT_MOF.1
- b) Management functions specified in FMT_MTD.1
- c) Management functions specified in FMT_PWD.1

]

5.1.5.6. FMT_SMR.1 Security roles

Hierarchical to No other components

Dependencies FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Chief Administrator, General Administrator].

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


5.1.6. Protection of the TSF (FPT)

5.1.6.1. FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to No other components

Dependencies No dependencies

FPT_ITT.1.1 The TSF shall protect the TSF data from disclosure, modification by **verifying encryption and message integrity** when the TSF data is

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

transmitted among TOE's separated parts.

5.1.6.2. 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's password, DBMS account information, SMTP password, security alert email for administrator, audit data storage threshold for local DB and threshold inspection cycle, maximum number of allowable failed authentication attempts, maximum number of concurrent sessions for general administrators, self-testing, audit cycle and audit time for counterfeit, falsification and process check, communication cycle of the Key Agent, expiration date for administrator's password and master password, access control policy, DB encryption policy, audit data saved in file format, cryptographic key] stored in containers controlled by the TSF from unauthorized disclosure, modification.


5.1.6.3. FPT_TEE.1 Testing of external entities

Hierarchical to No other components
 Dependencies No dependencies

FPT_TEE.1.1 The TSF shall run a suite of tests [timing for testing external entities specified of [Table 5-13]] to check the fulfillment of [testing items for corresponding external entities of [Table 5-13]].

FPT_TEE.1.2 If the test fails, the TSF shall [perform response actions of [Table 5-13]].

External entities	Timing for testing external entities	Testing items	Response actions
Mail Server	Every time management function is used in the administrator page after when email had been sent	Operating status	Display warning alert on the administrator page

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Maria DB	During start-up	Operating status	Display warning alert on the administrator page
	Every 5 seconds during normal operation	Operating status	Display warning alert on the administrator page

[Table 5-13] Testing of external entities

5.1.6.4. FPT_TST.1 TSF testing

Hierarchical to No other components
 Dependencies No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [TSF Data Integrity Verification Items for TOE Components of [Table 6-20]].

FPT_TST.1.3 The TSF shall provide **authorized administrators** with the capability to verify the integrity of [TSF Integrity Verification Items for TOE Components of [Table 6-21]].


5.1.7. TOE Access (FTA)

5.1.7.1. FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

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

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions [belonging to the same **administrator** according to the rules for the list of management functions defined in FMT_SMF1.1]

a) Limit the maximum number of concurrent sessions to 1 for management access by the same administrator who has the right to perform FMT_MOF.1.1 "Management actions" and FMT_MTD.1.1 "Management".

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- b) Limit the maximum number of concurrent sessions to { 5~100 } for management aces by the same administrator who doesn't have the right to perform FMT_MOF.1.1 "Management actions" but has the right to perform a query in FMT_MTD.1.1 "Management" only.
- c) [None]

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

5.1.7.2. FTA_SSL.5 Management of TSF-initiated sessions (extended)

Hierarchical to No other components
Dependencies FIA_UAU.1 Authentication or No dependencies

FTA_SSL.5.1 The TSF shall terminate the administrator's interactive session after a [10 minutes].

5.1.7.3. FTA_TSE.1 TOE session establishment

Hierarchical to No other components
Dependencies No dependencies


FTA_TSE.1.1 The TSF shall be able to refuse the **management access session of the administrator**, based on [Access IP, None].

5.1.8. Trusted path/channels (FTP)

5.1.8.1. 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 and provides assured identification of its end points and protection of the channel data from modification or disclosure.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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 [capability of chief administrator to send email authorized administrators].

5.2. Security Assurance Requirements

Assurance requirements of this Security Target are comprised of assurance components in CC Part 3, and the evaluation assurance level is EAL+1. The following table summarizes assurance components.

Security Assurance Class	Security Assurance Component	
Security Target Evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended Component definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

[Table 5-14] Security Assurance Requirements


5.2.1. Security Target Evaluation

5.2.1.1. ASE_INT.1 introduction

Dependencies No dependencies

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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 summaries the usage and major security features of the TOE.
- ASE_INT.1.5C The TOE overview shall identify the TOE type.
- ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
- ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.
- ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

- ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.2.1.2. ASE_CCL.1 Conformance claims


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

Developer action elements

- ASE_CCL.1.1D The developer shall provide a conformance claim.
- ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- part 3 as either CC Part 3 conformant or CC Part 3 extended.
- ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.
- ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
- ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
- ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
- ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
- ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
- ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

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

5.2.1.3. ASE_OBJ.1 Security objectives for the operational environment

Dependencies No dependencies


Developer action elements

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

Content and presentation elements

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

Evaluator action elements

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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

5.2.1.4. ASE_ECD.1 Extended component definition

Dependencies No dependencies

Developer action elements

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

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

Content and presentation elements

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

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

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

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

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


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

5.2.1.5. ASE_REQ.1 Stated security requirements

Dependencies ASE_ECD.1 Extended components definition

Developer action elements

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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

Content and presentation elements

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

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements

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

5.2.1.6. ASE_TSS.1 TOE summary specification

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

Developer action elements

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


Content and presentation elements

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

Evaluator action elements

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

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.2.2. Development

5.2.2.1. ADV_FSP.1 Basic functional specification

Dependencies No dependencies

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

5.2.3. Guidance Documents


5.2.3.1. AGD_OPE.1 Operational user guidance

Dependencies ADV_FSP.1 Basic functional specification

Developer action elements

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

Content and presentation elements

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

- AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
- AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
- AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
- AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

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

5.2.3.2. AGD_PRE.1 Preparative procedures


Dependencies No dependencies

Developer action elements

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

Content and presentation elements

- AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
- AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

- AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4. Life-cycle support

5.2.4.1. ALC_CMC.1 TOE Labeling of the TOE

Dependencies ALC_CMS.1 TOE CM coverage

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

5.2.4.2. ALC_CMS.1 TOE CM coverage


Dependencies No dependencies

Developer action elements

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

Content and presentation elements

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

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

Evaluator action elements

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

5.2.5. Tests

5.2.5.1. ATE_FUN.1 Functional testing

Dependencies ATE_COV.1 Evidence of coverage

Developer action elements

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the test to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.


ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

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

5.2.5.2. ATE_IND.1 Independent testing: conformance

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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Developer action elements

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

Content and presentation elements

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

Evaluator action elements

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

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

5.2.6. Vulnerability assessment

5.2.6.1. AVA_VAN.1 Vulnerability survey

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

Developer action elements

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

Content and presentation elements

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


Evaluator action elements

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

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

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


5.3. Security Requirements Rationale

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

5.3.1. Dependency of the SFRs

The table below shows dependencies of SFR.

No.	SFR	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_SEL.1	FAU_GEN.1	2
		FAU_MTD.1	26
7	FAU_STG.3	FAU_STG.1	Rationale (2)
8	FAU_STG.4	FAU_STG.1	Rationale (2)
9	FCS_CKM.1(1)	[FCS_CKM.2 OR FCS_COP.1]	11, 13
		FCS_CKM.4	12
10	FCS_CKM.1(2)	[FCS_CKM.2 OR FCS_COP.1]	11, 14
		FCS_CKM.4	12
11	FCS_CKM.2	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	9,10
		FCS_CKM.4	12
12	FCS_CKM.4	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	9,10
13	FCS_COP.1(1)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	9
		FCS_CKM.4	12
14	FCS_COP.1(2)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	10
		FCS_CKM.4	12
15	FCS_RBG.1	-	-
16	FDP_UDE.1	FCS_COP.1	14
17	FDP_RIP.1	-	-
18	FIA_AFL.1	FIA_UAU.1	
19	FIA_IMA.1	-	-
20	FIA_SOS.1	-	-
21	FIA_UAU.1	FIA_UID.1	24
22	FIA_UAU.4	-	-
23	FIA_UAU.7	FIA_UAU.1	21
24	FIA_UID.1	-	-
25	FMT_MOF.1	FMT_SMF.1	28

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

		FMT_SMR.1	29
26	FMT_MTD.1	FMT_SMF.1	28
		FMT_SMR.1	29
27	FMT_PWD.1(1)	FMT_SMF.1	28
	FMT_PWD.1(2)	FMT_SMR.1	29
28	FMT_SMF.1	-	-
29	FMT_SMR.1	FIA_UID.1	24
30	FPT_ITT.1	-	-
31	FPT_PST.1	-	-
32	FPT_TST.1	-	-
33	FTA_MCS.2	FIA_UID.1	24
34	FTA_SSL.5	FIA_UAU.1	21
35	FTP_TSE.1	-	-

[Table 5-15] Rationale of the Dependencies


Rationale (1) : FAU_GEN.1 has the dependency on FPT_STM.1. However, reliable time stamps provided by the security objective OE.TIME_STAMP for the operational environment of this ST are used, thereby satisfying the dependency.

Rationale (2) : FAU_STG.3 and FAU_STG.4 have the dependency on FAU_STG.1, which is satisfied by the operational environment of OE.Audit Data Protection.

5.3.2. Assurance Requirements Rationale

The dependency of the EAL1 assurance package provided in Common Criteria for Information Technology Security Evaluation is already satisfied, therefore details into its rationale are excluded.


ATE_FUN.1, which is an augmented assurance requirement, includes ATE_COV.1 by dependency. ATE_FUN.1 was added to ensure that the developer accurately tests the testing items and records them in the test paper. ATE_COV.1 was not added to this ST, as the proof of consistency between the testing items and the TSFI was not deemed strictly necessary.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

6. TOE Summary Specification

This section provides a detailed description of the security functions of the TOE, and how the SFRs are met by the TOE. The following depicts all security functional components in this section.

Security Functional Classes	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_SEL.1	Selective audit
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	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.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (User data encryption)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(extended)	Random bit generation
User Data Protection (FDP)	FDP_UDE.1(extended)	User data encryption
	FDP_RIP.1	Residual information protection
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	Authentication
	FIA_UAU.4	Single-use authentication mechanism
	FIA_UAU.7	Protection of authentication feedback
	FIA_UID.2	Identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(1)(extended)	Management of ID and password

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	d)	
	FMT_PWD.1(2)(extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic protection of internally transmitted TSF data
	FPT_PST.1(extended)	Basic protection of stored TSF data
	FPT_TEE.1	Testing of external entities
	FPT_TST.1	TSF self-testing
TOE Access (FTA)	FTA.MCS.2	Limitation of concurrent sessions depending on user attributes
	FTA_SSL.5(extended)	Management of sessions initiated by the TSF
	FTA_TSE.1	TOE session establishment
Trusted path/channels (FTP)	FTP_ITC.1	Trusted channel between TSF


[Table 6-1] List of TOE Security Functions

6.1. Security Audit

This section describes the security auditing features provided by the TOE and how they meet the declared SFRs.


6.1.1. Audit data generation

All TOE components generate audit data in the form of temporary files for auditable events, except for "success or failure of user data encryption and decryption," which is part of the component initiated events of [Table 6-2]. The event, "success or failure of user data encryption and decryption," generates only the activated events among success, failure, encryption, and decryption in the form of audit data file in accordance with the protection policy applied by the chief administrator to the corresponding EdgeDB Key Agent on the administrator's page. Audit data can be generated by combining success and failure events and encryption and decryption events, to form successful encryption event or failed decryption event, etc. (FAU_GEN.1, FAU_SEL.1)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

The default value is set to generate a log of all encryption and decryption success and failure events. The chief administrator can set the conditions for creating audit data according to the success or failure of encryption and decryption.

SFR	Auditable Event
FAU_ARP.1	Actions taken in response to potential security violations
FAU_SAA.1	Enabling and disabling of analysis mechanisms, Automated responses performed by the tool
FAU_STG.3	Actions taken in response to exceeding the threshold
FAU_STG.4	Actions taken in response to the failure to save audit
FCS_CKM.1(1)	Success or failure of the activity
FCS_CKM.2	Success or failure of the activity (applies only to key distribution pertaining user data encryption and decryption)
FCS_CKM.4	Success or failure of the activity (applies only to key destruction pertaining user data encryption and decryption)
FCS_COP.1(1)	Success or failure of cryptographic operation, type of cryptographic operation
FDP_UDE.1	Success or failure of user data encryption and decryption
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and response actions, and, if appropriate, the subsequent restoration to the normal state
FIA_IMA.1	Success or failure of mutual authentication, modification of authentication protocol
FIA_UAU.2	Exhaust all available authentication mechanism
FIA_UAU.4	Attempt to re-use authentication data
FIA_UID.2	Exhaust all user identification mechanism, including those user identities already provided
FMT_MOF.1	All modifications in in the behavior of the TSF functions
FMT_MTD.1	All modifications to the values of TSF data
FMT_PWD.1(1)	All changes to the password
FMT_PWD.1(2)	All changes to the password
FMT_SMF.1	Use of the management functions
FMT_SMR.1	Modification of the user group with divisional roles
FPT_TST.1	Execution of the TSF self-tests and their results
FTA_MCS.2	Denial of a new session based on the limitation placed on the number of

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	concurrent sessions
FTA_SSL.5	Locking or termination of interactive sessions
FTA_TSE.1	Denial of session establishment as a result of session mechanism, all attempts to establish user session
FTP_ITC.1	All attempts made to use trusted channel function
FPT_TEE.1	Execution of the tests for external entity and their results

[Table 6-2] Auditable Events for the TOE

All TOE components generate audit data for auditable events of [Table 6-2], including audit records such as occurrence date, occurrence IP, request IP, log classification, log level, occurrence module, process, success or failure, id of execution administrator, execution object, execution subject, execution classification, result code, result message. (FAU_GEN.1)

Auditable events of [Table 6-3] generate audit data in addition to those of [Table 6-2], as well as additional audit records of [Table 6-3]. (FAU_GEN.1)

Auditable events	Additional audit records
All changes made to the TSF data value	Modified values of TSF data
Execution of TSF self-tests and their results	Modified TSF data or execution code in case of integrity violation


[Table 6-3] Additional Audit Records for certain Audit Events

- ※ **SFR to be satisfied**
- FAU_GEN.1, FAU_SEL.1

6.1.2. Audit data review

Audit data stored in the local DB's audit repository can be retrieved from the administrator's page by an authorized administrator.

Audit data files generated by all TOE components are sent to EdgeDB Log Server by EdgeDB Log Agent, which exists in the same physical server as the TOE component, the EdgeDB Log Server then stores the data in a local DB that exists on the Management Server. When audit data stored in a local DB is requested by an authorized administrator through the security management interface provided by EdgeDB Key Server, the EdgeDB Key Server inquires audit data stored in the local DB to provide review and selective review of audit data collected from the entire TOE component through the security management interface.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

For the collected audit data, it is possible to query based and operation on occurrence date, occurrence IP, request IP, log classification, log level, occurrence module, success or failure, result code, number of posts criteria and sort the results in ascending/descending order based on the occurrence/save date and time.

- ※ **SFR to be satisfied**
- FAU_SAR.1, FAU_SAR.3

6.1.3. Potential violation analysis and response

Audit data generated in accordance with the description in FAU_GEN.1 from all TOEs is forwarded by the EdgeDB Log Agent to the EdgeDB Log Server and stored by the EdgeDB Log Server in the local DB. The EdgeDB Key Server checks local DB for any audit of potential violation FIA_UAU.2, as defined in FAU_SAA.1, such as authentication failure audit event, self-test failure of validated cryptographic module, verification failure of major security function processes, DB table space utilization exceeding the threshold specified in FAU_STG.3, audit log storage failure, and license expiration events.

The Log Server shall inquire immediately upon receipt of an audit of integrity violations among the auditable cases in FPT_TST.1. (FAU_SAA.1)


In the event of audit of potential violations, the EdgeDB Key Server and EdgeDB Log Server will send a security alert email to the authorized administrator designated by the chief administrator or output a warning message on the administrator page. In addition, an error message is displayed on the CLI for potential violation audit events that occur during startup. (FAU_ARP.1)

- ※ **SFR to be satisfied**
- FAU_ARP.1, FAU_SAA.1,

6.1.4. Protection of audit data and action against data loss

EdgeDB Log Server periodically checks the usage of the local DB to store audit data. (FAU_STG.3, FAU_STG.4)

If the local DB usage identified by the EdgeDB Log Server exceeds the specified limit, the administrator page provides the ability to notify the authorized administrator designated by the

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

chief administrator via email if "Resource Threshold Exceeded" of the email dispatch items is enabled. The specified limit is set at 60% as the default value and can be set from 60% to 90% by the Chief Administrator. (FAU_STG.3)

If the local DB usage identified by EdgeDB Log Server exceeds the saturation threshold of 95%, the administrator page provides the ability to notify the authorized administrator designated by the chief administrator via email, provided that the "Failed to Save Audit Logs" of the email dispatch items has been activated. Additionally, when local DB usage is saturated, audit data is no longer stored in DB.

(FAU_STG.4)

※ **SFR to be satisfied**

- FAU_STG.3, FAU_STG.4


6.2. Cryptographic Support

TOE's cryptographic support is enabled by either its internal operation to protect TSF data, or the cryptographic key and DB encryption policy set by the chief administrator. The cryptographic operation following the DB encryption policy set by the chief administrator, is performed through the library module in API form or plug-in provided by the EdgeDB Key Agent, and is destroyed safely using the zeroization function immediately after use. All cryptographic support functions are performed using the approved cryptographic algorithm of the validated cryptographic module, which, as of [Table 6-4].

Classification		Description
validated cryptographic module name		USCryptoLib V1.2
Developer		Korea Electronic Certification Authority
Verification No.		CM-148-2023.12
Verification Date		2018.12.05
Expiration Date		2023.12.05
Library	Windows	libUSCrypto.dll
	Linux	libUSCrypto.so

[Table 6-4] validated cryptographic module

6.2.1. Cryptographic Key Generation

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


The User data key (the key for encrypting user data), if generated by the chief administrator via the administrator page, is generated on the EdgeDB Key Server with a key length as of [Table 6-5] using approved cryptographic algorithm of [Table 6-5], which is a validated cryptographic module as in standard list of [Table 6-5]. When the generated cryptographic key is used in a 128-bit cryptographic algorithm, only the previous 128-bit length is used. (FCS_CKM.1(1))

Standard list	Approved Cryptographic algorithm	key length	Usage
TTAK.KO-12.0191	HMAC-DRBG-SHA512	256 bits	Encrypt-decrypt user data

[Table 6-5] Cryptographic Key Generation for User Data

Encryption for TSF data such as cryptographic keys and security policies, is generated using approved cryptographic algorithm of the validated cryptographic module. Additionally, the random bit generation and HMAC-SHA256 algorithm used by self-implemented PBKDF2 algorithms also use the approved cryptographic algorithm of the validated cryptographic module. Cryptographic keys for TSF data cipher are generated with the key length as of [Table 6-6] using cryptographic algorithms of [Table 6-6] and follows the standard list of [Table 6-6]. (FCS_CKM.1(2))

Standard list	Cryptographic algorithm	Key length	Purpose	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-12.0191	HMAC-DRBG-SHA512	256 bits	Encryption and decryption of TSF data's essential encryption data	Local Key	EdgeDB Key Server EdgeDB Log Server EdgeDB Key Agent EdgeDB Log Agent
TTAK.KO-12.0191	HMAC-DRBG-SHA512	256 bits	Generate integrity value for TSF and TSF data	Audit Key	EdgeDB Key Server
ISO/IEC 11770-3	ECDH(ECC-P256)	256 bits	Generate Session Key	Session Key	EdgeDB Key Server EdgeDB Log Server EdgeDB Key Agent EdgeDB Log Agent
ISO/IEC 14888-3	RSA-PSS	2048 bits	Generation and validation of Auth	Auth Key Pair	EdgeDB Key Server

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

			Key Pair signature		
--	--	--	--------------------	--	--

[Table 6-6] Generate Cryptographic key for TSF Data

※ **SFR to be satisfied**


- FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1(extended)

6.2.2. Cryptographic Key Distribution

EdgeDB Key Server and EdgeDB Log Server distribute the cryptographic keys required by each component so that the corresponding TOE can correctly protect TSF data and user data. All distributed cryptographic keys except the Auth Key and Session Key are distributed after performing the mutual signature verification through Auth Key distribution in advance, 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 on EdgeDB Key Server in the form of a key file. Auth Priv Key is distributed by the EdgeDB Key Server as a key file encrypted with the Master Key. The cryptographic keys of [Table 6-7] shall be distributed by the distribution method of [Table 6-7] to the receiver TOE of [Table 6-7] from the sender TOE of [Table 6-7]. The key file with record of the distributed cryptographic key is placed in a folder containing the properties file of the TOE component to which the cryptographic key had been distributed, and the key distribution is completed by performing key insertion procedure in the corresponding 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	TOE (Sender)	TOE (Receiver)	Cryptographic Key	Distribution method
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Pub Key (Server)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB Key Server	EdgeDB Key Agent	Auth Priv Key (Agent)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB Key Server	EdgeDB Log Agent	Auth Pub Key (Server)	Distribute offline during installation, and insert the key using the TOE interface
None	EdgeDB	EdgeDB	Auth Priv Key	Distribute offline during

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	Key Server	Log Agent	(Agent)	installation, and insert the key using the TOE interface
--	------------	-----------	---------	--

[Table 6-7] Auth Key Pair Distribution

The Audit Key is distributed after performing all of self-implemented mutual authentication mechanisms, and the User data key is delivered to the EdgeDB Key Agent according to the cryptographic key set by the authorized chief administrator, along with the corresponding User data key. Key of [Table 6-8] is distributed by the sending TOE of [Table 6-8] to the receiving TOE of [Table 6-8] through the distribution method of [Table 6-8], which is approved cryptographic algorithm of the validated cryptographic module. (FCS_CKM.2)


Standard list	TOE (Sender)	TOE (Receiver)	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 and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash values, to Session Key
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 and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash values, to Session Key
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 and encrypt then deliver ARIA-256-CBC-PKCS#5, including hash values, to Session Key

[Table 6-8] Audit Key, User data Key Distribution

※ **SFR to be satisfied**
- FCS_CKM.2


6.2.3. Destruction of Cryptographic Key

The TOE uses the deletion method of [Table 6-9] at the timing of deletion of [Table 6-9] to destroy


	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

the keys of [Table 6-9] stored in the location as specified of [Table 6-9]. (FCS_CKM.4)

Key	TOE	Location	Deletion method	Timing of deletion
User data Key	EdgeDB Key Agent	Memory	Zeroization	Immediately after encrypting user data
Master Password	EdgeDB Key Server	Memory	Zeroization	Immediately after generating the Master Key
	EdgeDB Key Agent	Memory	Zeroization	Immediately after generating the Master Key
	EdgeDB Log Server	Memory	Zeroization	Immediately after generating the Master Key
	EdgeDB Key Agent	Memory	Zeroization	Immediately after generating the Master Key
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	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Server	Memory	Zeroization	Immediately after use
	EdgeDB Key Agent	key file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	Memory	Zeroization	Immediately after use
	EdgeDB Log Agent	key file	Overwrite the file area with zero then delete	When deleting 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

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Session Key	EdgeDB Key Server	Memory	Zeroization	When terminating the session
	EdgeDB Log Server	Memory	Zeroization	When terminating the session
	EdgeDB Key Agent	Memory	Zeroization	When terminating the session
	EdgeDB Log Agent	Memory	Zeroization	When terminating the session
Auth Key Pair	EdgeDB Key Server	key file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Server	Memory	Zeroization	After generating signature value
	EdgeDB Log Server	Memory	Zeroization	After generating signature value
	EdgeDB Key Agent	key file (personal key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Key Agent	key file (server public key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Key Agent	Properties file	Overwrite the file area with zero then delete	When deleting the TOE
	EdgeDB Key Agent	Memory	Zeroization	After generating signature value
	EdgeDB Log Agent	key file (personal key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Log Agent	key file (server public key)	Overwrite the file area with zero then delete	After inserting the Key
	EdgeDB Log Agent	Properties file	Overwrite the file area with zero then delete	When deleting the TOE

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	EdgeDB Log Agent	Memory	Zeroization	After generating signature value
ECDH Private Key	EdgeDB Key Server	Memory	Zeroization	When generating the Session Key
	EdgeDB Log Server	Memory	Zeroization	When generating the Session Key
	EdgeDB Key Agent	Memory	Zeroization	When generating the Session Key
	EdgeDB Log Agent	Memory	Zeroization	When generating the Session Key

[Table 6-9] Destruction of Cryptographic Key

The source code optimization of the compiler may not zero the memory area as much as the actual key length, so that the source code is not optimized by the compiler, the anti-optimization keyword "volatile" is used to ensure that the memory area is zeroed correctly as the length of the zeroing target.


- ※ **SFR to be satisfied**
- FCS_CKM.4

6.2.4. Cryptographic Operation

The library module provided by EdgeDB Key Agent performs a list of operations on [Table 6-10] for user data in accordance with the key length of [Table 6-10] using the cryptographic algorithm of [Table 6-10] that approved cryptographic algorithm of the validated cryptographic module, that complies with the standard list of [Table 6-10]. (FCS_COP.1(1))

The User Data Key used to encrypt user data in the library module is decrypted with the ARIA-256-CBC and Master Key created in EdgeDB Key Agent.

Standard list	Cryptographic Algorithm	Key length	Operating 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·

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

					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 6-10] Cryptographic Operation of User Data

Among the cryptographic algorithms of [Table 6-10], ARIA and SEED cryptographic algorithms use additional initialization vectors, and use the verified random bit generator of the cryptographic modules to in order to use an unexpected initialization vector value, whilst compliant to the NIST SP 800-38A Annex C, generate the HMAC-DRBG-SHA512 generation algorithm with 128 bits in length. (FDP_UDE.1(extended), FCS_RGB.1(extended))

TSF data of [Table 6-11] is used for [Table 6-15] purposes by performing a list of operations of [Table 6-11] on TSF data in accordance with the key length of [Table 6-11] using the cryptographic algorithm of [Table 6-11], which is approved cryptographic algorithm of the validated cryptographic module. (FCS_COP.1(2))

Standard list	Cryptographic algorithm	Key length	Operating Mode	Padding	List of operations	Purpose
KS X 1213	ARIA	256 bits	CBC	PKCS#5	Encryption· Decryption	Encryption· Decryption
ISO/IEC 10118-3	SHA256	None	None	None	Hash	Admin / Master Password hash generation, During encrypted communication generate integrity verification value
ISO/IEC 9792-2	HMAC-SHA256	256 bits	None	None	Verify integrity	Generate integrity verification value
ISO/IEC 14888-2	RSA-PSS (SHA-256)	2048 bits	None	None	Create· validate Signature	Mutual authentication of TOE components

[Table 6-11] Cryptographic Operation of TSF Data

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

In addition to the above-described uses, TOE uses the approved random bit generation algorithm HMAC-DRBG-SHA-512 of the validated cryptographic module to provide security functions safely, when generates random number. And, the length of the generated random number is 128/256/512 bits. (FCS_RGB.1(extended))

※ **SFR to be satisfied**

- FCS_COP.1(1), FCS_COP.1(2), FDP_UDE.1(extended), FCS_RGB.1(extended)

6.3. User Data Protection

The library module provided by EdgeDB Key Agent operates according to the DB encryption policy created by the chief administrator through the administrator's page provided by EdgeDB Key Server, and enables one-way encryption, blank encryption, and encryption of user data using different cryptographic keys, cryptographic algorithms, etc. by column, using different DB encryption policies depending on the method provided by the user's EdgeDB Key Agent. Empty-value encryption is a feature that can encrypt requests without input values, and double-encryption is a feature that can encrypt requests for cryptographic statements that are already encrypted. (FDP_UDE.1(extended))

The cryptographic algorithm listed in FCS_COP.1(1) for encryption and encryption of user data is provided, and the block cryptographic algorithm allowing different cipher statements to be generated even if the same statement is encrypted with the same cryptographic key. While the one-way cryptographic algorithm provides SHA-256, SHA-384, SHA-512 and different one-way cipher texts are generated for the same plaintext. EdgeDB Key Agent provides API or plug-in in the form of library modules for encryption and decryption of user data. (FDP_UDE.1(extended))


After the user data encryption and decryption operation, the plaintext user data remaining in memory uses the zeroing function to safely remove the remaining information. (FDP_RIP.1)

※ **SFR to be satisfied**

- FDP_UDE.1(extended), FDP_RIP.1

6.4. Identification and Authentication

Identification and Authentication feature provided by the TOE is to provide mutual authentication among TOE components, identification and authentication of administrators for access to the administrator page provided by the EdgeDB Key Server.

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

6.4.1. Identification and Authentication by Administrator


The EdgeDB Key Server must successfully identify and authenticate before allowing access and control to the administrator page provided by the EdgeDB Key Server. The EdgeDB Key Server uses the administrator's ID as identification information, uses the administrator's password as authentication information, and identifies the administrator. (FIA_UAU.2, FIA_UID.2)

All passwords entered during the creation, modification, and authentication of all passwords are masked as ("*") and cannot be identified on screen, and only the message "Login failed" is displayed in the event of identification and authentication failure. (FIA_UAU.7)

The EdgeDB Key Server blocks access attempts to the account for 5 minutes (fixed value) and stores audit records for authentication failures if the authentication fails consecutively by (3-10 times/default: 5 times), which had been set as the number of authentication failures allowed during administrator account authentication. (FIA_AFL.1)

Key Server requires the administrator of [Table 6-12] to comply with the criteria for secret information at the timing of [Table 6-12], performs actions corresponding to the success of [Table 6-12] when the secret information verification is successful, and performs actions corresponding to the failure of [Table 6-12] when the secret information verification fails. Criteria for secret information is three combinations of the English alphabet (52 letters : a ~ z, A ~ Z) / Numbers (10 strings : 0 ~ 9) / special characters (32 characters : `~!@#\$\$%^&*()-_+=[\]{}|;:~",.<>/?), where the combination rules dictate that digits be between 9 ~ 20. (FIA_SOS.1)

Administrator	Timing	Secret	Success	Failure
Chief Administrator	When chief administrator login for the first time	PW	Change the password to the inserted value	Display the message "password should be a three combination of English alphabet, numbers, special characters. (9~20 digits)"
Chief Administrator	When chief administrator changes PW	PW	Change the password to the inserted value	Display the message "password should be a three combination of English alphabet, numbers, special characters. (9~20 digits)"
Chief Administrator	When general administrator changed PW	PW	Change the password to the inserted value	Display the message "password should be a three combination of English alphabet, numbers, special characters. (9~20 digits)"

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

General Administrator	When general administrator login for the first time	PW	Change the password to the inserted value	Display the message "password should be a three combination of English alphabet, numbers, special characters. (9~20 digits)"
-----------------------	---	----	---	--

[Table 6-12] Secret information verification on EdgeDB Key Server

EdgeDB Key Server uses the administrator's unique sessionId to prevent reuse of authentication sessions. (FIA_UAU.4)

※ **SFR to be satisfied**

- FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

6.4.2. Mutual Authentication

To ensure that the TOE components of [Table 6-13] are correct TOE components prior to communication, mutual authentication method of [Table 6-13] is carried out at the timing of mutual authentication of [Table 6-13]. (FIA_IMA.1)

Standard list	TOE components	Timing of mutual authentication	Mutual authentication method
N/A	EdgeDB Key Server EdgeDB Key Agent	When EdgeDB Key Agent accesses EdgeDB Key Server	Mutual signature verification through pre-auth key distribution
N/A	EdgeDB Log Server EdgeDB Log Agent	When EdgeDB Log Agent accesses EdgeDB Log Server	Mutual signature verification through pre-auth key distribution

[Table 6-13] Mutual Authentication between TOE Components


※ **SFR to be satisfied**

- FIA_IMA.1

6.5. Security Management

EdgeDB Key Server provides security management features through the administrator interface to authorized administrators who passed the identification and authentication process.

6.5.1. Security Role

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Administrators of the TOE include, the chief administrator with the mandate for all security roles, and general administrators who are limited to monitoring functions. The chief administrator has a unique status as the sole administrator. (FMT_SMR.1)

6.5.2. Security Function Management

TOE provided the administrators of [Table 6-14] the management functions of [Table 6-14]. (FMT_MOF.1, FMT_SMF.1, FMT_SMR.1)

Administrator	List of functions
Chief Administrator	Modify or query rules regarding potential security violations
Chief Administrator	Modify or query responses in the case of anticipated audit storage failure
Chief Administrator	Modify, delete, and query - EdgeDB Key Agent
Chief Administrator	Modify, delete, query, and add - DB encryption policy
General Administrator	Query rules concerning potential security violations
General Administrator	Query responses in the case of anticipated audit storage failure
General Administrator	Query EdgeDB Key Agent
General Administrator	Query DB encryption policy


[Table 6-14] Security Functions requiring Management

- ※ **SFR to be satisfied**
- FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

6.5.3. TSF Data Management

TOE provides the administrators of [Table 6-15] the management functions of [Table 6-15] for security attributes and TSF data. (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1)

Administrator	TSF data list
Chief Administrator	Modify the master password
Chief Administrator	Modify audit data generation settings for success and failure events of user data encryption and decryption
Chief Administrator	Query, add, modify, or delete cryptographic key
Chief Administrator	Query audit data
Chief Administrator	Query or modify the storage space usage threshold for audit data
Chief Administrator	Query or modify the maximum number of allowable failed authentication attempts

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Chief Administrator	Modify authentication data of chief administrator, modify authentication data of general administrator
Chief Administrator	Query or modify the identity of chief administrator; query, modify, add, or delete the identity of general administrator
Chief Administrator	Query or modify the maximum number of concurrent sessions for general administrators
Chief Administrator	Query, modify, add, or delete IP addresses access for security management
General Administrator	Query administrators
General Administrator	Query cryptographic key
General Administrator	Query audit data
General Administrator	Query the storage space usage threshold for audit data
General Administrator	Query the maximum number of allowable failed authentication attempts
General Administrator	Modify authentication data by the user
General Administrator	Query user identity
General Administrator	Query the maximum number of concurrent sessions for general administrators
General Administrator	Modify IP addresses accessed for security management


[Table 6-15] TSF Data requiring Management

※ **SFR to be satisfied**

- FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.5.4. ID and Password Management

TOE provides the ability for the chief administrator to use the ID and password of the initial administrator account in the interface of TOE after the TOE installation to modify the ID and password upon successful authentication, and after the chief administrator creates a general administrator account, the general administrator uses the ID generated by the chief administrator in the TOE's administrator interface and the password set to the initial value. TOE provides the function to change the password when the general administrator authentication is successful. TOE also provides the chief administrator with the ability to modify passwords for all administrators. Follow [Table 6-16] the rules for generating administrator passwords. TOE does not provide the ability to modify administrator ID generation rules and administrator password generation rules. (FMT_PWD.1(1)(extended), FMT_PWD.1(2)(extended))

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

Classification	Password length	9~20 digits
	Combination rules	Three combinations of letters (English alphabet small and capital), special characters, and numbers
	Number	0~9
	English capital letter	A~Z
	English small letter	a~z
	Special character	`~!@#\$%^&*()-_+=[\]{} ;:'",.<>/?)

[Table 6-16] Combination Rules for Generating Administrator's Password

※ **SFR to be satisfied**

- FMT_PWD.1(1)(extended), FMT_PWD.1(2)(extended)

6.6. Protection of the TSF

The TOE protects the TSF by using the approved cryptographic algorithm of "USCryptoLib V1.2", a verified cryptographic module.

6.6.1. Basic Protection of internally transmitted TSF Data


TOE adds the TSF data it wishes to send when TSF data is transmitted between TOE components after a SHA256 hash to the TSF data it wishes to send, and protects the TSF data from unauthorized exposure and modification by encrypting and sending ARIA-256-CBC with the Session Key. Upon detection of a violation of incoming data integrity, the TSF will discard the received data and generate audit data for this event. (FPT_ITT.1)

※ **SFR to be satisfied**


- FPT_ITT.1

6.6.2. Basic Protection for Stored TSF Data


TOE protects stored TSF data by means of protection of [Table 6-17] to protect the TSF data of [Table 6-17] stored in the TOE component of [Table 6-17]. The cryptographic operation to protect TSF data is performed using validated cryptographic module "USCryptoLib V1.2". (FPT_PST.1(extended))

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

TOE Components	TSF data	Method of protection
EdgeDB Key Server	Master Password	Use SHA-256 algorithm to perform hash
	Admin Password	Use SHA-256 algorithm to perform hash
	SMTP password	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Admin security alert email	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit data local DB storage threshold, and threshold check cycle	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Limit for no. of failed authentication attempts	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Maximum no. of concurrent sessions for general administrator	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Self-test, falsification, process check audit cycle, and audit time	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Communication cycle of the Key Agent	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Expiration dates for administrator PW and master PW	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	DBMS account information	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	SMTP password	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Access control policy	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit Data (Temporary file)	Obfuscate with self-encoding
	DB encryption policy	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit Key	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Auth Priv Key(Server)	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Auth Priv Key(Agent)	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
Local Key	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.	

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

		Obfuscate with self-encoding
	Session Key	Obfuscate with self-encoding
	User data Key	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
EdgeDB Key Agent	Server IP	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Server PORT	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Agent ID	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Network interface	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit Data (Temporary file)	Obfuscate with self-encoding
	DB encryption policy	Obfuscate with self-encoding
	Local Key	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Auth Priv Key(Agent)	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
EdgeDB Log Server	PORT information	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	DBMS account information	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Network interface	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit Data (Temporary file)	Obfuscate with self-encoding
EdgeDB Log Agent	Server IP	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Server PORT	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Network interface	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Audit Data (Temporary file)	Obfuscate with self-encoding

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

	Auth Priv Key(Agent)	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.
	Local Key	Self-encoding cipher text by encryption it with ARIA-256-CBC algorithm.

[Table 6-17] Protection method for stored TSF data

Obfuscated and stored in memory using self-encoding values generated by each TOE component when stored in memory for the use of protected TSF data and cryptographic keys. If used, copy the values and maintain the existing obfuscated values, use them after disable obfuscation, and destroy them safely using the zeroing function immediately after use.

- ※ **SFR to be satisfied**
- FPT_PST.1(extended)


6.6.3. Testing of external entity

To confirm that the external entities required to operate the TOE are in normal operating status, the TOE run a suite of tests on external entity on the EdgeDB Key Server at the timing for testing external entity specified of [Table 6-18]. The testing items and objectives for each external entity subject to external entity test are as follows. (FPT_TEE.1)

External entity	Timing for testing external entity	Testing items	Response actions
Mail Server	Every time management function is used in the administrator page	Operating status	Display warning alert on the administrator page
Maria DB	Performed upon start-up	Operational status	Display warning alert on the administrator page
	Performed on a periodic basis after start-up	Operational status	Display warning alert on the administrator page

[Table 6-18] Testing Items for External Entity

- ※ **SFR to be satisfied**
- FPT_TEE.1(extended)

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

6.6.4. Self-testing


To demonstrate the correct operation of its components, namely EdgeDB Key Agent, EdgeDB Log Agent, EdgeDB Key Server, and EdgeDB Log Server, the TOE run a suite of self tests of the key security function processes during initiation of operation, or periodically during normal operation, and also self-tests validated cryptographic module. And, TSF verifying integrity of the validated cryptographic module, execution file, installation script, initiation script, stop script, library module, etc. Furthermore, an verifying integrity is performed on some TSF data from EdgeDB Key Server and on the local keys of all TOE components as specified of [Table 6-20].

If self-test for validated cryptographic module (at initiation) and integrity check of the Local Key fails, TOE sends relevant warning message in the CLI window and immediately halts the process. During normal operation term, self-testing cycle for EdgeDB Key Server, EdgeDB Key Agent, and EdgeDB Log Server is determined by the chief administrator from the administrator page.

In the event of violation in the results of periodic self-tests carried out during the normal operation term, email is sent to the authorized administrator designated by the chief administrator. The authorized administrator can perform an integrity check of TSF data stored in the internal DB by moving around the detailed query page of the management function from the administrator page. If the data integrity check fails, the administrator page outputs an integrity failure message and sends email to the authorized administrator designated by the chief administrator.

The following [Table 6-19] depicts the self-testing items by TOE components, and [Table 6-20] depicts the TSF data integrity verification items for TOE, and [Table 6-21] depicts the TSF integrity verification items for TOE components. The following self-test items and integrity verification items are performed the same regardless of the operating environment of the physical server where TOE is installed. (FPT_TST.1)


TOE components	Timing of self-testing	Testing items
EdgeDB Key Server	Performed upon start-up	validated cryptographic module
		Process
	Performed at the set time, at each self-test interval specified by the chief administrator	validated cryptographic module
		Process

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

EdgeDB Key Agent	Performed upon start-up	validated cryptographic module
		Process
EdgeDB Key Agent	Performed at the set time, at each self-test interval specified by the chief administrator	validated cryptographic module
		Process
EdgeDB Log Server	Performed upon start-up	validated cryptographic module
		Process
EdgeDB Log Server	Performed at the set time, at each self-test interval specified by the chief administrator	validated cryptographic module
		Process
EdgeDB Log Agent	Performed upon start-up	validated cryptographic module
		Process
EdgeDB Log Agent	Performed on a periodic basis after start-up	validated cryptographic module
	Performed at the set time, at each self-test interval specified by the chief administrator	Process

[Table 6-19] Self-testing Items for TOE

TOE Components	Timing of Integrity Verification	Verification items
EdgeDB Key Server	Performed upon start-up	TSF data (Local Key)
	Performed at the set time, at each self-test interval specified by the chief administrator	
	Performed when management functions and settings are looked up in detail from the administrator page	TSF data (Setting value)
EdgeDB Log Server	Performed upon start-up	TSF data (Local Key)
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Key Agent	Performed upon start-up after start-up	TSF data

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5


for Windows	Performed at the set time, at each self-test interval specified by the chief administrator	(Local Key)
EdgeDB Key Agent for Linux	Performed upon start-up	TSF data (Local Key)
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Log Agent for Windows	Performed upon start-up	TSF data (Local Key)
	Performed on a periodic basis	
EdgeDB Log Agent for Linux	Performed upon start-up	TSF data (Local Key)
	Performed on a periodic basis after start-up	

[Table 6-20] TSF Data Integrity Verification items for TOE Components

TOE Components	Timing of Integrity Verification	Verification items
EdgeDB Key Server	Performed upon start-up	EdgeDB Key Server Binary data
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Log Server	Performed upon start-up	EdgeDB Log Server Binary data
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Key Agent for Windows	Performed upon start-up	EdgeDB Key Agent Binary data
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Key Agent for Linux	Performed upon start-up	EdgeDB Key Agent Binary data
	Performed at the set time, at each self-test interval specified by the chief administrator	
EdgeDB Log Agent for Windows	Performed upon start-up	EdgeDB Log Agent Binary data
	Performed on a periodic basis after start-up	
EdgeDB Log Agent for Linux	Performed upon start-up	EdgeDB Log Agent Binary data
	Performed on a periodic basis after start-up	

[Table 6-21] TSF Integrity Verification items for TOE Components

- ※ **SFR to be satisfied**
 - FPT_TST.1

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

6.7. TOE Access

6.7.1. Limiting the Number of Access Sessions

The EdgeDB Key Server blocks simultaneous access to the same account by limiting the maximum number of concurrent access sessions to 1 for both the chief administrator, and general administrator. When a new connection is made to an account that is already connected, the existing connection session is terminated. The default setting for the maximum number of concurrent access by general administrators is 5, and the chief administrator can modify it to be between 5~100 sessions from server information settings window. If general administrators with different accounts access simultaneously and exceed the maximum number of concurrent sessions, any additional access by administrators is blocked. (FTA_MCS.2)

※ **SFR to be satisfied**

- FTA_MCS.2

6.7.2. Session Management and Configuration

The TOE restricts TOE access to the administrative interface EdgeDB Key Server from registered IP address only, and terminates the session 10 minutes after login by authorized administrator. (FTA_SSL.5(extended), FTA_TSE.1)

The IP address used for the first login after installing the TOE is automatically granted access, and the chief administrator can modify or add one access IP address at a time from the administrator settings window. Configuration of access IP address range is not permitted. (FTA_TSE.1)

※ **SFR to be satisfied**


- FTA_SSL.5(extended), FTA_TSE.1

6.8. Trusted path/channels

6.8.1. Trusted Channel between TSF

When sending security alert email, the EdgeDB Key Server and EdgeDB Log Server uses the Mail Server and TLS v1.2 to reset cryptographic communication. Cipher Suites used during the cryptographic communication supports the Cipher Suites specified of [Table 6-22]. (FTP_ITC.1)

Cipher Suites

	EdgeDB v4.0	
	Title	Version
	Security Target(ST) for Public	1.5

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256

[Table 6-22] List of Cipher Suites to select when communicating with mail server TLS v1.2

※ **SFR to be satisfied**

- FTP_ITC.1