KECS-CR-20-60

EdgeDB v4.0

Certification Report

Certification No.: KECS-CISS-1046-2020

2020. 10. 6.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.10.06.	-	Certification report for EdgeDB v4.0 - First documentation

This document is the certification report for EdgeDB v4.0 for SECUCEN Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory Co., Ltd. (KSEL)

Table of Contents

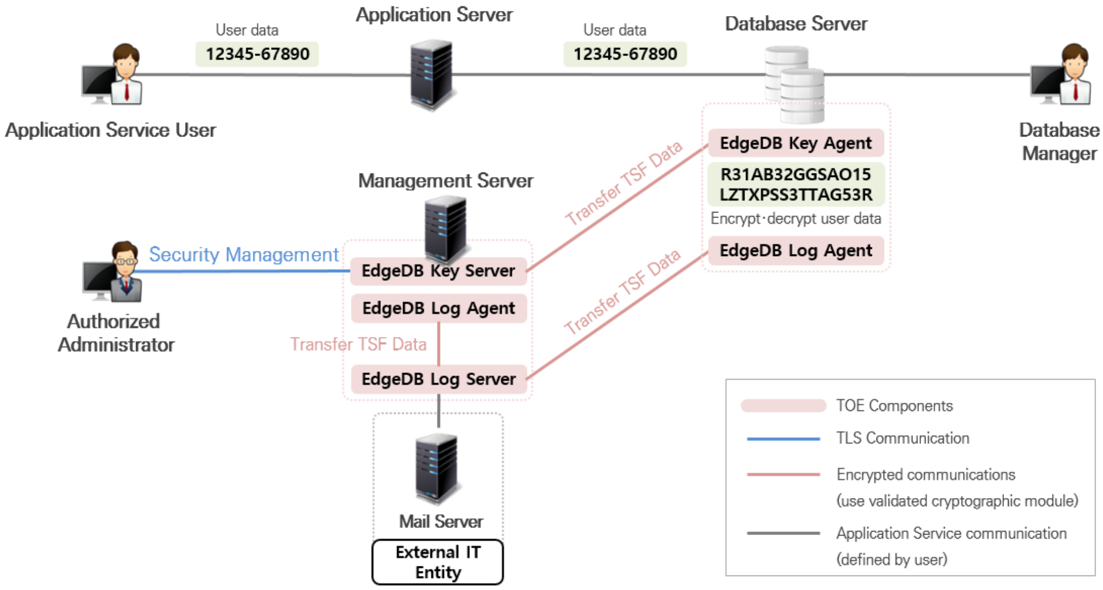
1. Executive Summary

This report describes the certification result drawn by the evaluation facility on the results of the EdgeDB v4.0 developed by SECUCEN Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is database encryption software. The TOE provides a variety of security features: security audit, cryptographic operation using cryptographic module (USCryptoLib V1.2) validated under the Korea Cryptographic Module Validation Program (KCMVP), identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function.The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory Co., Ltd. (KSEL) and completed on September 21, 2020.

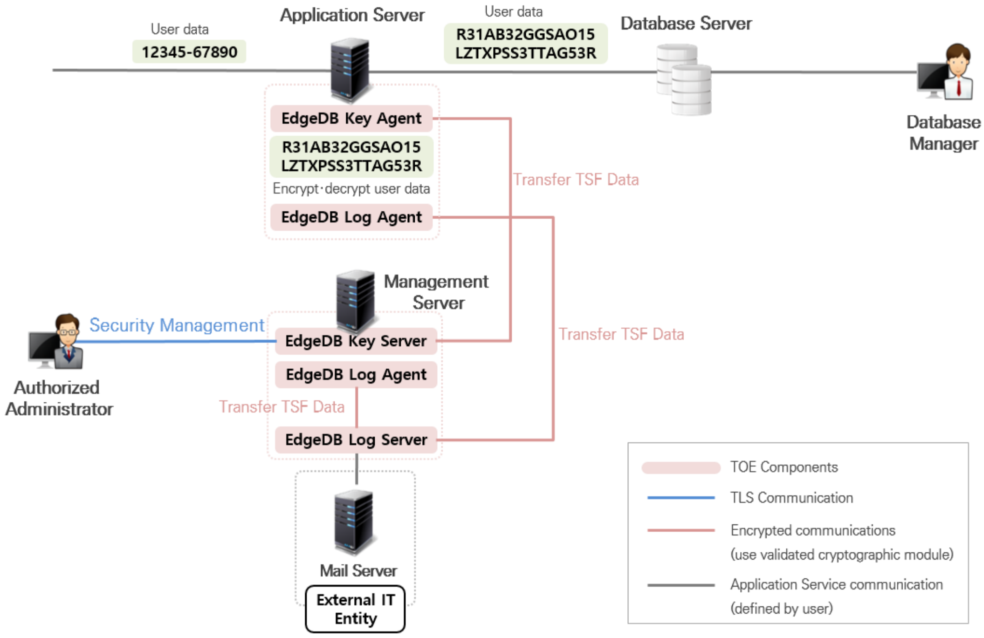
The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

The TOE consists of EdgeDB Key Server(EdgeDB Key Server v4.0.4.11), EdgeDB Log Server(EdgeDB Log Server v4.0.4.11), EdgeDB Key Agent(EdgeDB Key Agent v4.0.4.11 for Windows, EdgeDB Key Agent v4.0.4.11 for Linux), EdgeDB Log Agent(EdgeDB Log Agent v4.0.4.11 for Windows, EdgeDB Log Agent v4.0.4.11 for Linux) and related guidance documents. The TOE operational environment classified into two: plug-in type and API type. [Figure 1] show the Plug-in type operational environment. The authorized administrator can encrypt/decrypt the user data through the EdgeDB Key Server according to the scope of the encryption that is required by the organizational security policy. The EdgeDB Key Server is installed in the management server. The EdgeDB Key Agent, which is installed in the protected database server of the DB, encrypts the user data received from the application server before storing it in the DB according to the policy configured by the authorized administrator, and decrypts the encrypted user data sent from the database server to the application server. The EdgeDB Log Agent, which is installed in both database Server and management Server, sends the log to the EdgeDB Log Server, which is installed in the management server.



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

[Figure 2] show the API type operational environment. The application, which is installed in the application server and provides application services, is developed using the API provided by the EdgeDB Key Agent in order to use the cryptographic function of the TOE. The EdgeDB Key Agent is installed in the application server and the API of the EdgeDB Key Agent performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by the API, which is installed in the application server, and sent to the database server. The encrypted user data received from the database server is decrypted by the API of the EdgeDB Key Agent, and sent to the application service user. Communications among TOE components, which rely on a self-implemented protocol, carry out cryptographic communication, using an approved algorithm of the validated cryptographic module (USCryptoLib V1.2).



[Figure 2] TOE Operational Environment (API type)

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

Category			Contents
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
		VC++	Visual C++ Redistributable Packages for Visual Studio 2013 (12.0.30501) (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)
		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	10/100/1000 Base-T 1 Port or higher
	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

[Table 1] The requirements for hardware, software and operating system

[Table 2] shows the software requirements for the administrator's PC.

Category	Contents
SW	Chrome 80.0 64bit

[Table 2] SW Requirements for the administrator's PC

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is software consisting of the following software components and related guidance documents.

TOE	오류! 참조 원본을 찾을 수 없습니다.	
Version	v4.0.4.11	
TOE components	EdgeDB Key Agent	EdgeDB Key Agent v4.0.4.11 for Windows EdgeDB Key Agent v4.0.4.11 for Linux
	EdgeDB Log Agent	EdgeDB Log Agent v4.0.4.11 for Windows EdgeDB Log Agent v4.0.4.11 for Linux
	EdgeDB Key Server	EdgeDB Key Server v4.0.4.11
	EdgeDB Log Server	EdgeDB Log Server v4.0.4.11
Guidance documents	EdgeDB v4.0 Preparative Procedures(PRE) v1.9 EdgeDB v4.0 Operational User Guidance(OPE) v1.8 EdgeDB v4.0 Developer User's Guidance(DUG) v1.6	

[Table 3] TOE identification

Note that the TOE is delivered contained in a CD-ROM.

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	EdgeDB v4.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Protection Profile	Korean National Protection Profile for Database Encryption V1.1
Developer	SECUCEN Co., Ltd.

Sponsor	SECUCEN Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory Co., Ltd. (KSEL)
Completion Date of Evaluation	Sep. 21, 2020
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [4] for the TOE claims strict to the Korean National PP for Database Encryption V1.1 [3], and complies security policies defined in the PP by security requirements. Thus, the TOE provides security features defined in the PP as follows:

- Security audit: The TOE generates audit records of security relevant events such as the start-up/shutdown of the audit functions, integrity violation, self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic key management such as key generation, distribution, and destruction, and cryptographic operations such as encryption and decryption using the cryptographic modules (USCryptoLib V1.2) validated under the KCMVP.
- User data protection: The TOE provides encryption and decryption for the user data in a column of a database.
- Identification and authentication: The TOE identifies and authenticates the administrators using their ID/password and mutually authenticates TOE components.
- Security management: The TOE allows only an authorized administrator to access the management interface provided by the TOE.
- Protection of the TSF: The TOE implements secure communications between the TOE components to protect the transmitted data. The TOE encrypts the stored TSF data to protect them from unauthorized exposure and modification. The TOE performs self-tests on the TOE components, which includes the self-test on the validated cryptographic module.
- TOE access: The TOE manages authorized administrators' sessions based on access IP addresses and administrator rights, and terminates the sessions after predefined time interval of inactivity.

- Trusted path/channels : The TOE provide secure communication channel.

4. Assumptions and Clarification of Scope

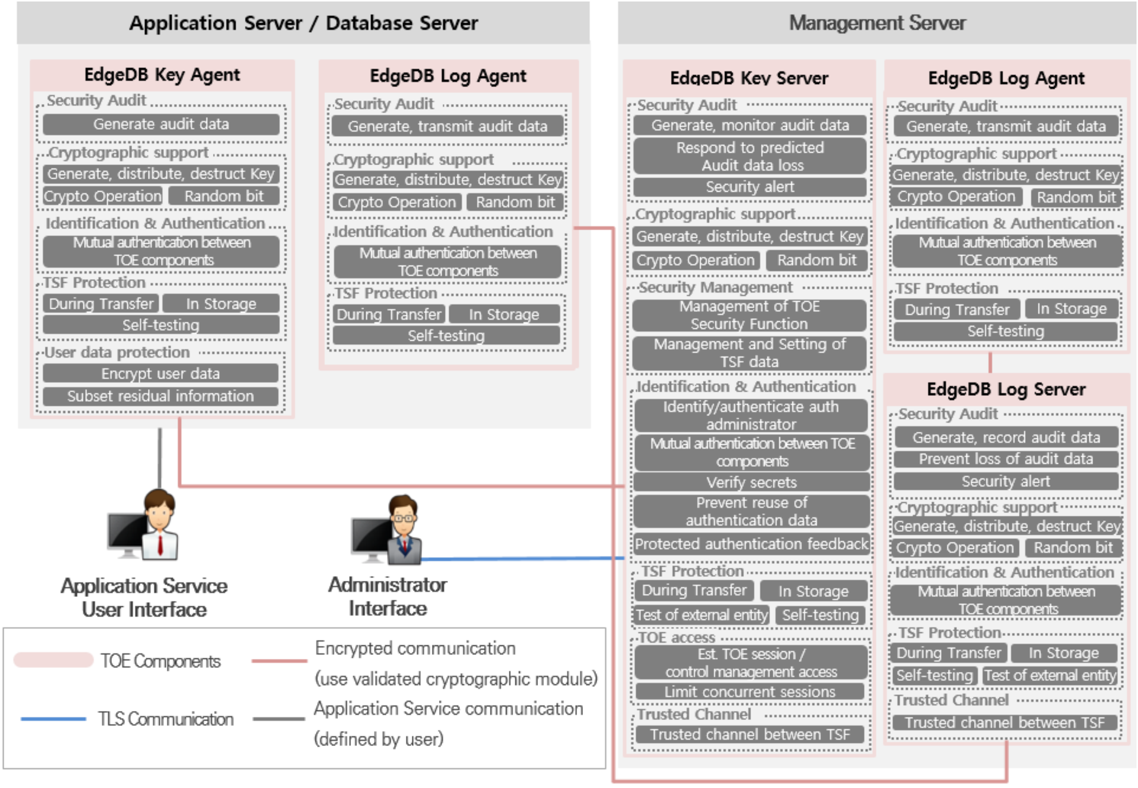
There is no explicit Security Problem Definition chapter, therefore no Assumptions secti on in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [3] in which the TOE will be used or is intended to be used (F or the detailed and precise definition of the security objectives of the operational enviro nment, refer to the ST [4], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:
TOE : EdgeDB v4.0 (v4.0.4.11)
TOE Components :

- EdgeDB Key Agent v4.0.4.11 for Windows,
- EdgeDB Key Agent v4.0.4.11 for Linux
- EdgeDB Log Agent v4.0.4.11 for Windows
- EdgeDB Log Agent v4.0.4.11 for Linux
- EdgeDB Key Server v4.0.4.11
- EdgeDB Log Server v4.0.4.11

In [Figure 2], The TOE components perform the same functionalities of audit data generation, cryptographic key management, cryptographic operations, protection of TSF data, and mutual authentication between the components. For the detailed description on the architectural information, refer to the ST [4].


Application Server / Database Server
EdgeDB Key Agent
Security Audit
Generate audit data
Cryptographic support
Generate, distribute, destruct Key
Crypto Operation
Random bit
Identification & Authentication
Mutual authentication between TOE components
TSF Protection
During Transfer
In Storage
Self-testing
User data protection
Encrypt user data
Subset residual information
EdgeDB Log Agent
Security Audit
Generate, transmit audit data
Cryptographic support
Generate, distribute, destruct Key
Crypto Operation
Random bit
Identification & Authentication
Mutual authentication between TOE components
TSF Protection
During Transfer
In Storage
Self-testing
Management Server
EdgeDB Key Server
Security Audit
Generate, monitor audit data
Respond to predicted Audit data loss
Security alert
Cryptographic support
Generate, distribute, destruct Key
Crypto Operation
Random bit
Security Management
Management of TOE Security Function
Management and Setting of TSF data
Identification & Authentication
Identify/authenticate auth administrator
Mutual authentication between TOE components
Verify secrets
Prevent reuse of authentication data
Protected authentication feedback
TSF Protection
During Transfer
In Storage
Test of external entity
Self-testing
TOE access
Est. TOE session / control management access
Limit concurrent sessions
Trusted Channel
Trusted channel between TSF
EdgeDB Log Agent
Security Audit
Generate, transmit audit data
Cryptographic support
Generate, distribute, destruct Key
Crypto Operation
Random bit
Identification & Authentication
Mutual authentication between TOE components
TSF Protection
During Transfer
In Storage
Self-testing
EdgeDB Log Server
Security Audit
Generate, record audit data
Prevent loss of audit data
Security alert
Cryptographic support
Generate, distribute, destruct Key
Crypto Operation
Random bit
Identification & Authentication
Mutual authentication between TOE components
TSF Protection
During Transfer
In Storage
Self-testing
Test of external entity
Trusted Channel
Trusted channel between TSF
Application Service User Interface
Administrator Interface
TOE Components
Encrypted communication (use validated cryptographic module)
TLS Communication
Application Service communication (defined by user)

[Figure 2] Logical scope of the TOE

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identification	Date
EdgeDB v4.0 Preparative Procedures(PRE) v1.9	September 3, 2020
EdgeDB v4.0 Operational User Guidance(OPE) v1.8	September 3, 2020
EdgeDB v4.0 Developer User’s Guidance(DUG) v1.6	July 10, 2020

[Table 5] Documentations

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator installed and prepared the TOE in accordance to the preparative procedures, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: EdgeDB v4.0 (v4.0.4.11)

- EdgeDB Key Agent v4.0.4.11 for Windows,
- EdgeDB Key Agent v4.0.4.11 for Linux
- EdgeDB Log Agent v4.0.4.11 for Windows
- EdgeDB Log Agent v4.0.4.11 for Linux
- EdgeDB Key Server v4.0.4.11

- EdgeDB Log Server v4.0.4.11

The TOE identification information is provided via CLI and Report. And the guidance documents listed in this report chapter 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.
The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.
The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.
The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.
The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.
Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.
The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The functional specification specifies a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore, the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore, the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ADV_FSP.1.2E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 6] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- When additional development to operate the TOE in the API type, user plaintext data may remain in the memory after encryption and decryption by the API of the TOE, so the memory area of the plaintext data must be overwritten with 0 twice or more so that it is safely deleted.
- The TOE is implemented not to store audit data when the audit data storage is exceeded. Therefore, if an authorized administrator receives e-mail notification due to exceeding the audit data storage threshold or limit, the audit log backup must be performed immediately so that audit data is not lost.
- Authorized administrators use a master password different from the administrator login password to generate a secure master key (KEK), and be careful not to use easily inferred information such as the use of personal information, and create a secure master key according to NIST 800-132. It is recommended to use at least 10 lengths for the master password to generate the secure master key.

11. Security Target

EdgeDB v4.0 Security Target v1.12 [4] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
Application Server	The application server 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.
Column	A set of data values of a particular simple type, one for each row of the table in a relational database

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

Self-test

Pre-operational or conditional test executed by the cryptographic module

Validated Cryptographic Module

A cryptographic module that is validated and given a validation number by validation authority

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April, 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017

[3] Korean National Protection Profile for Database Encryption V1.1, KECS-PP-0820a-2017, December 11, 2019

[4] EdgeDB v4.0 Security Target(ST) v1.12, September 15, 2020

[5] EdgeDB v4.0, Evaluation Technical Report V3.00, September 21, 2020