KECS-CR-26-44

EdgeDB v4.2

Certification Report

Certification No.: KECS-CISS-1426-2026

2026. 11. 2.

IT Security Certification Center

Revision History			
No.	Date	Revised Pages	Description
00	2026.11.02.	-	Certification report for EdgeDB v4.2 - Initial issue

This document is the certification report for EdgeDB v4.2 of ITCEN PNS Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

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

Table of Contents

Certification Report **1**
1. **Executive Summary** **5**
2. **Identification** **6**
3. **Security Policy** **7**
4. **Assumptions and Clarification of Scope** **8**
   - 4.1 Assumptions 8
   - 4.2 Clarification of Scope 9
5. **Architectural Information** **9**
6. **Documentation** **13**
7. **TOE Testing** **14**
8. **Evaluated Configuration** **15**
9. **Results of the Evaluation** **15**
   - 9.1 Security Target Evaluation (ASE) 15
   - 9.2 Development Evaluation (ADV) 16
   - 9.3 Guidance Documents Evaluation (AGD) 17
   - 9.4 Life Cycle Support Evaluation (ALC) 17
   - 9.5 Test Evaluation (ATE) 17
   - 9.6 Vulnerability Assessment (AVA) 18
   - 9.7 Evaluation Result Summary 18
10. **Recommendations** **20**
11. **Evaluation Evidence** **21**
12. **Acronyms and Glossary** **21**
13. **Bibliography** **25**

1. Executive Summary

This report describes the evaluation result produced by the evaluation facility on the EdgeDB v4.2 developed by ITCEN PNS Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (hereinafter referred to as CC) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (hereinafter referred to as TOE) is database encryption software that encrypts and decrypts the user data in a column of a database to be protected. Also, the TOE shall provide a variety of security features: security audit, Cryptographic support, User data protection, identification and authentication including mutual authentication between TOE components, TOE access, TSF protection, and security management function.

The TOE operational environment classified into two: Plug-in method and API method. The TOE includes cryptographic module (EdgeCrypto v4.2, CM-299-2031.7) validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on October 28, 2026. This report is based on the evaluation technical report (ETR) [3] KSEL had submitted and the Security Target (ST) [4].

The ST claims conformance to the Korean National PP for Database Encryption V3.1 [5]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance components in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1 augmented by ATE_FUN.1. Therefore, the ST and the resulting TOE are CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and newly defined components in the Extended Component Definition chapter of the PP, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE are CC Part 2 extended.

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 consists of EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, EdgeDB Log Agent and related guidance documents.

TOE Name	EdgeDB v4.2	
TOE Version	v4.2.0.3	
TOE components	EdgeDB Key Agent	EdgeDB Key Agent v4.2.0.3 (EdgeDB_Key_Agent_4.2.0.3_Linux-x86_64.run)
	EdgeDB Log Agent	EdgeDB Log Agent v4.2.0.3 (EdgeDB_Log_Agent_4.2.0.3_Linux-x86_64.run)
	EdgeDB Key Server	EdgeDB Key Server v4.2.0.3 (EdgeDB_Key_Server_4.2.0.3_Linux-x86_64.run)
	EdgeDB Log Server	EdgeDB Log Server v4.2.0.3 (EdgeDB_Log_Server_4.2.0.3_Linux-x86_64.run)
Guidance documents	EdgeDB v4.2 Preparative Procedure (PRE) v1.4 (EdgeDB v4.2_Preparative Procedure(PRE)_v1.4.pdf) EdgeDB v4.2 Operational User Guidance (OPE) v1.2 (EdgeDB v4.2_Operational User Guidance(OPE)_v1.2.pdf) EdgeDB v4.2 Developer User's Guidance (DUG) v1.2 (EdgeDB v4.2_Developer User's Guidance(DUG)_v1.2.pdf)	

[Table 4] TOE identification

Scheme	Korea IT Security Evaluation and Certification Guidelines(Ministry of Science and ICT Guidance No.2022-61) Korea IT Security Evaluation and Certification Regulation(Ministry of Science and ICT·ITSCC, April 7, 2026)
TOE	EdgeDB v4.2
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Database Encryption V3.1
Developer	ITCEN PNS Co., Ltd.
Sponsor	ITCEN PNS Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	October 14, 2026
Certification Body	IT Security Certification Center

[Table 5] Additional identification information

3. **Security Policy**

The TOE complies security policies pertaining to the following security functional requirements defined in the ST [4].

- Security Audit
- Cryptographic support
- User data protection

- Identification and authentication
- Security Management
- Protection of the TSF
- TOE access
- Trusted path/channels

4. Assumptions and Clarification of Scope

4.1 Assumptions

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used:

- The place where the TOE is installed and operated shall be equipped with access control and protection facilities so that only authorized administrators can access it.
- The authorized administrator of the TOE is non-malicious, has been appropriately trained for the TOE management functions, and accurately fulfills their duties in accordance with administrator guidelines.
- Developers who use the TOE to link the encryption function to the application or DBMS shall comply with the requirements of the manual provided with the TOE to ensure that the security functions of the TOE are safely applied.
- The reliability and security of the operating system shall be ensured by reinforcing the latest vulnerabilities in the operating system on which the TOE is installed and operated.
- Communication between the web browser of the administrator PC and the web server, which is the operational environment of the TOE server, shall be secured.
- The TOE operational environment shall provide reliable time stamps to the TOE.
- Audit records stored in the DBMS installed on the same operating system as the TOE shall be protected by the DBMS from deletion or modification by unauthorized users.
- Upon completion of manual recovery, the tampered information of the TOE agent or

client shall be recovered.

4.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurance covered in the Security Target. All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

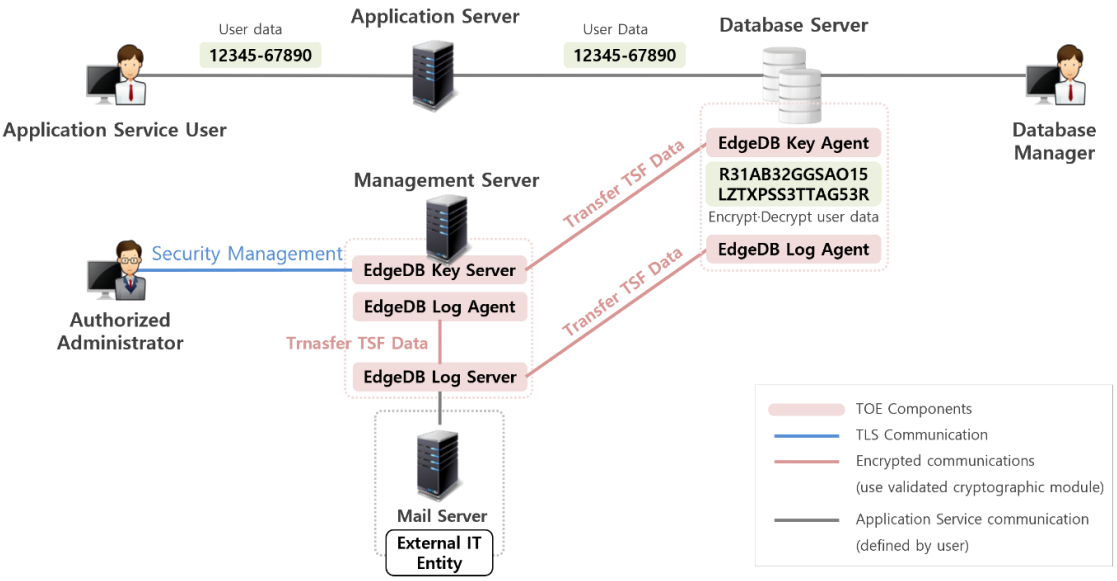
Note that:

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4])

5. Architectural Information

The TOE is database encryption software that encrypts and decrypts the user data in a column of a database to be protected. The physical boundary of the TOE consist of EdgeDB Key Server, EdgeDB Log Server, EdgeDB Key Agent, EdgeDB Log Agent, and the guidance documents.

The TOE supports two operational configurations : Plug-in method and API method. Both methods are composed of four components; EdgeDB Key Agent, EdgeDB Log Agent, EdgeDB Key Server, and EdgeDB Log Server. [Figure 1], [Figure 2] shows the operational environment of the TOE



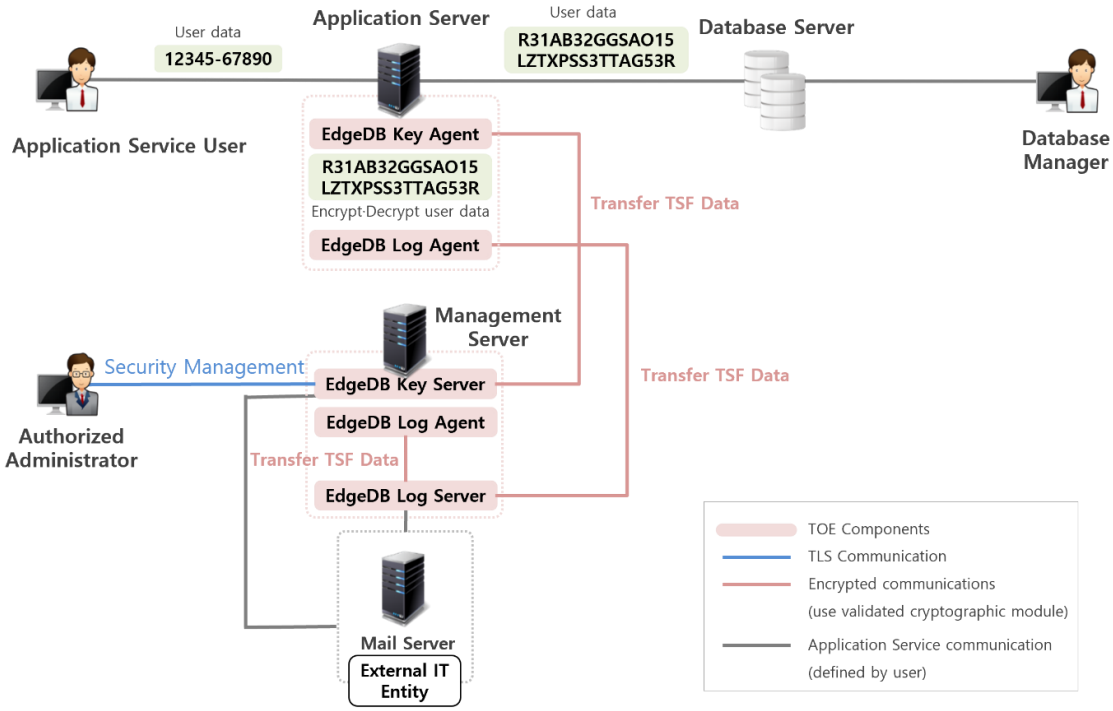
[Figure 1] TOE Operational Environment(Plug-in method)

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

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

TOE component to EdgeDB Log Server, and EdgeDB Log Server stores the logs collected through EdgeDB Log Agent in the DB.

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



[Figure 2] TOE Operational Environment(API method)

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

When the authorized chief administrator sets the TOE security policy through a web

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

[Table 1] shows the hardware and software requirements, and operating system to install the TOE.

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

Server		RAM	16GB or more
		HDD	At least 200MB required to install the TOE
		NIC	At least one 10/100/1000 Base-T Port
	SW	OS	Ubuntu 24.04.3 LTS (release 24.04) (Kernel Linux version 6.14.0-37-generic, x86_64)
		DBMS	MariaDB 11.4.9 x86_64
		JRE	jre 8u261 linux x64
		WAS	Apache-tomcat 9.0.122

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

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

Category	Contents
Software	Chrome 143.0.7499.193 64bit

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

6. Documentation

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

Identifier	Date
EdgeDB v4.2 Preparative Procedure (PRE) v1.4	September 30, 2026
EdgeDB v4.2 Operational User Guidance (OPE) v1.2	September 30, 2026
EdgeDB v4.2 Developer User's Guidance (DUG) v1.2	September 30, 2026

[Table 6] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator performed all the developer's tests, and conducted independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [4]. The evaluator considered the followings when devising a test subset:

- TOE security functionality: The TOE components are provided in the form of software and shall provide the encryption/decryption function for the user data by each column. The TOE can also provide a one-way encryption method in addition to the encryption/decryption method for each column.
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_FUN.1, and ATE_IND.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL1+(ATE_FUN.1), and the evaluator tried to balance time and effort of evaluator's activities between EAL1+ assurance components.

In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [3].

8. Evaluated Configuration

The TOE is software consisting of the following components:

- TOE : EdgeDB v4.2 (v4.2.0.3)
- TOE Components :

  EdgeDB Key Agent v4.2.0.3

  EdgeDB Log Agent v4.2.0.3

  EdgeDB Key Server v4.2.0.3

  EdgeDB Log Server v4.2.0.3

The TOE is identified by TOE name and version number. The TOE identification information is provided via the administrator page provided by EdgeDB Key Server.
And the guidance documents listed in this report chapter 6, [Table 6] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] 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 of EAL1+(ATE_FUN.1).

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 (ST reference, TOE reference, TOE overview and TOE description), and these four 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 Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore, the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The ST clearly and unambiguously defines the extended SFR component. 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 describes how the TOE meets each SFR, 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 Development Evaluation (ADV)

The functional specifications specify the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their purpose, method of use and all parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

Therefore, the functional specification (TSF interface description) which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

The verdict PASS is assigned to the assurance class ADV

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 the 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, Furthermore, the operational user guidance is clear and reasonable and contains no misleading information. 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 Life Cycle Support Evaluation (ALC)

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

The configuration list includes the TOE itself, the evaluation evidence required by the SARs, and the parts that comprise the TOE (required by the PP). Therefore, the verdict PASS is assigned to ALC_CMS.1.

The verdict PASS is assigned to the assurance class ALC.

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 penetrating 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_SPD.1	ASE_SPD.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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	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		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	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 7] 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:

- The TOE is implemented not to store audit data when the audit data storage is saturated. 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.

11. Evaluation Evidence

Identifier	Issue date
EdgeDB v4.2 Security Target(ST) v1.4	2026.09.30
EdgeDB v4.2 Functional Specification(FSP) v1.2	2026.09.30
EdgeDB v4.2 Preparative Procedures(PRE) v1.4	2026.09.30
EdgeDB v4.2 Operational Guidance(OPE) v1.2	2026.09.30
EdgeDB v4.2 Developer User Guidance(DUG) v1.2	2026.09.30
EdgeDB v4.2 Configuration Management Documentation (CMC_CMS) v1.2	2026.09.30
EdgeDB v4.2 Test Documentation(ATE) v1.2	2026.09.30

[Table 8] Evaluation Evidence

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
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 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.
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.
Auth Key Pair	Auth Priv Key and Auth Pub Key to perform mutual authentication.
Auth Priv Key	The private key of the key pair used to perform mutual authentication.
Auth Pub Key	The public key of the key pair used to perform mutual authentication.
Authentication Data	Information used to verify the claimed identity of a user.
Authorized Administrator	An authorized user who operates and manages the TOE securely (subdivided into Chief Administrator and General Administrator).
Chief Administrator	An authorized administrator who has the authority to add, modify, and delete the TOE's security functions and TSF data management.
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)	Security-related information that can compromise the security of the cryptographic module if disclosed or modified (e.g., secret keys/private keys, and authentication data such as passwords or personal

	identification numbers).
Database	A set of data organized according to a certain structure in order to receive, store, and provide data in response to the demands of multiple users so as to support multiple application duties at the same time. The database related to column-level encryption required by this PP refers to a relational database.
Database Server	The Database Server defined in this ST refers to the server on which the DBMS managing the protected DB is installed in the organization operating the TOE.
General Administrator	An authorized administrator who has only the authority to view the TOE's security functions and TSF data management.
Local Key	A cryptographic key that encrypts and decrypts TSF data existing on the Management Server on which EdgeDB Key Server and EdgeDB Log Server are installed and on the servers on which EdgeDB Key Agent and EdgeDB Log Agent are installed, among the TOE components.
Master Password	A password directly entered by the administrator to generate the Master Key through the PBKDF2-HMAC-SHA-256 algorithm.
Random bit generator (RBG)	A device or algorithm that outputs a binary string that is statistically independent and unbiased. An RBG used for cryptographic applications generally generates a bit string of 0s and 1s, and this string can be combined into random bit blocks. RBGs are classified into deterministic and non-deterministic types. A deterministic RBG consists of an algorithm that generates bit strings from an initial value called a seed

	key, and a non-deterministic RBG produces output that depends on an unpredictable physical source.
Session Key	A key used for encrypted communication between TOE components.
User data Key	A key for encrypting user data.
Zeroization	The procedure of overwriting with 0 twice for the length of the data so as not to leave residual data in the storage space of memory or files.

13. Bibliography

The evaluation facility has used the following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022

Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15

[2] Common Methodology for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-006, November 2022

Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 2025-10-15

[3] EdgeDB v4.2 Evaluation Technical Report V2.00, October 19, 2026

[4] EdgeDB v4.2 Security Target(ST) v1.4, September 30, 2026

[5] Korean National PP for Database Encryption V3.1, June 27, 2025