KECS-CR-25-31

Alpha DBGuard V2.1

Certification Report

Certification No.: KECS-CISS-1368-2025

2025. 9. 25.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025.9.25	-	Certification report for Alpha DBGuard V2.1 - First documentation

This document is the certification report for Alpha DBGuard V2.1 of Alphabit Co.,Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Information Security Technology (KOIST)

Table of Contents

1. Executive Summary

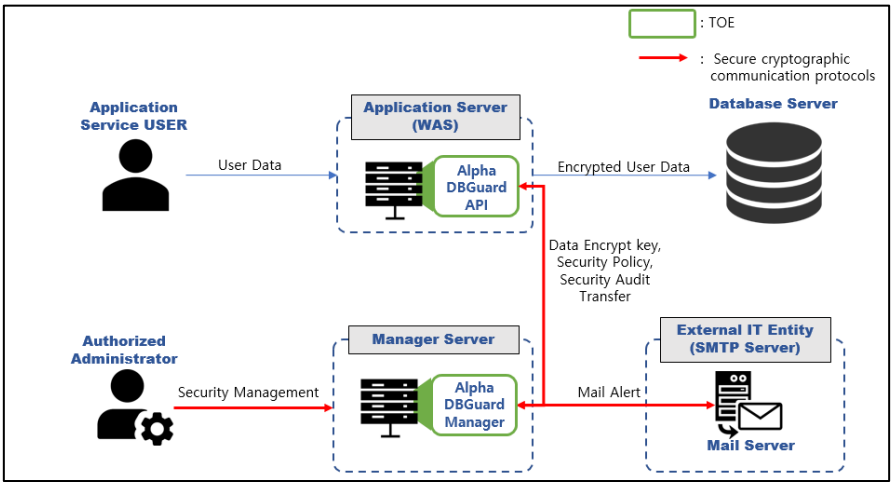
This report describes the certification result drawn by the certification body on the results of the EAL1+ evaluation of Alpha DBGuard V2.1 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is database encryption to prevent DBMS from unauthorized exposure of the information. The TOE also provides security features such as security audit, cryptographic key management and cryptographic operation using validated cryptographic module, user identification and authentication and mutual authentication between TOE components, security management, TSF data protection and self-protection, TOE access control.

The evaluation of the TOE has been carried out by Korea Information Security Technology (KOIST) and completed on 24 September 2025. This report grounds on the evaluation technical report (ETR) KOIST had submitted [6] and the security target (ST) [7][8].

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V3.1 [5]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. 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, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environments of the TOE.



[Figure 1] Operational environment of the TOE

[Table 1] shows the hardware and software requirements to install and operate the TOE.

TOE Component		Requirement	
Alpha DBGuard Manager	HW	CPU	Intel(R) Core(TM) i5-7200U Dual Core 2.5 GHz or faster
		Memory	8 GB or more
		HDD	Space required for TOE installation is 512 MB or more
		NIC	100/1000 Mbps x 1 EA or more
	SW	OS	Rocky Linux 9.6 (64bits) (kernel 5.14.0-570.23.1)
		3rd party SW	SpringBoot V2.7.18 H2DB V2.2.224 Oracle Java Runtime Environment v1.8.0_202
Alpha DBGuard API	HW	CPU	Intel(R) Core(TM) i5-7200U Dual Core 2.5 GHz or faster
		Memory	8 GB or more
		HDD	Space required for TOE installation is 512 MB or more
		NIC	100/1000 Mbps x 1 EA or more
	SW	OS	Rocky Linux 9.6 (64bits) (kernel 5.14.0-570.23.1)
		3rd party SW	Apache Tomcat 9.0.95 Oracle Java Runtime Environment v1.8.0_202

[Table 1] TOE Hardware and Software requirements

The 3rd party software included in the TOE are shown in [Table 2].

3rd party S/W	Description
AlphaCrypto V1.0	User Data Protection TSF Data Protection
Rt.jar	TSF Data Transfer

[Table 2] The 3rd party software included in TOE

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 identified as follows.

TOE	Alpha DBGuard V2.1
TOE Version	V2.1.0.3
TOE Components	Alpha DBGuard Manager V2.1.0.3 - Alpha_DBGuard_Manager_V2.1.0.3.tgz
	Alpha DBGuard API V2.1.0.3 - Alpha_DBGuard_API_V2.1.0.3.tgz
Guidance Document	Alpha_DBGuard_V2.1 Preparative Procedures and Operational Guidance V1.4 - Alpha_DBGuard_V2.1_PREOPE_V1.4.pdf

[Table 3] TOE identification

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
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 1.1, CCMB-2024-07-002, July, 2024
EAL	EAL1+ (augmented by ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Database Encryption V3.1, KECS-PP-1350-2025, June 27, 2025
Developer	Alphabit Co.,Ltd.

Sponsor	Alphabit Co.,Ltd.
Evaluation Facility	Korea Information Security Technology (KOIST)
Completion Date of Evaluation	September 24, 2025
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the ST [7][8].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the chapter 3.1 of ST [7][8]):

- The TOE must be in a physically safe environment, and protected from unauthorized physical accesses.
- The authorized administrators of the TOE should not be malicious, and should be properly trained and perform their duties accurately according to administrator guidelines.
- Developers integrating the encryption function of the TOE into an application or DBMS should comply with the requirements specified in the guidance

documents to ensure that the security function of the TOE is applied properly.

- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement work on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
- Reliable timestamp should be provided by the operational environment to accurately record security-related events.

Furthermore, some aspects of threats, and organizational security policies are not fulfilled by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the chapter 3.2 and 3.3 of ST [7][8].

The scope of this evaluation is limited to the functionality and assurance covered in ST [7][8]. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

5. Architectural Information

The TOE consists of Alpha DBGuard Manager, Alpha DBGuard API and Guidance document. In the TOE components, the validated cryptographic module (AlphaCrypto V1.0) is embedded for protection of user data and TSF data. The physical scope of the TOE and the information of validated cryptographic module are presented in [Table 5] and [Table 6], respectively.

Category	Name	Type	Delivery
TOE	Alpha DBGuard V2.1	-	-
TOE version	V2.1.0.3	-	-
TOE Component	Alpha DBGuard Manager V2.1.0.3 - Alpha_DBGuard_Manager_V2.1.0.3.tgz	SW	CD
	Alpha DBGuard API V2.1.0.3 - Alpha_DBGuard_API_V2.1.0.3.tgz	SW	
	Alpha_DBGuard_V2.1 Preparative Procedures and Operational Guidance V1.4 - Alpha_DBGuard_V2.1_PREOPE_V1.4.pdf	PDF	

[Table 5] Physical Scope of TOE

Category	Description
Cryptographic module name	AlphaCrypto V1.0
Validation No.	CM-265-2030.3
Developer	Alphabit Co.,Ltd.
Module type	S/W(library)
Validation date	07 Mar 2025
Expiration Date	07 Mar 2030

[Table 6] Validated Cryptographic Module

The logical scope of the TOE is defined as follows.

- Security Audit (FAU)

The TOE creates and maintains audit records of auditable events such as the operation of security functions provided by the TOE and the history of security management.

- Cryptographic support (FCS)

The TOE provides cryptographic key generation, distribution, destruction, and cryptographic operations to protect the transmitted data between TOE components and encrypt and decrypt user data. In addition, it provides a random number generation function for secure encryption key generation. The TOE uses the cryptographic algorithm of “AlphaCrypto V1.0”, which is a validated cryptographic module whose security and implementation conformance are verified through the cryptographic module verification program(KCMVP), for the encryption of user data and TSF data and the generation of the encryption key.

- User data protection (FDP)

The TOE provides column-level encryption and decryption of user data in DBMS.

- Identification and authentication (FIA)

The TOE performs the identification and authentication based on user ID and password. All TOE management functions cannot be used before the authorized administrator is successfully identified and authenticated. The TOE performs mutual authentication

among its components.

- Security Management (FMT)

The TOE defines a single administrative role and account for the administrator. The authorized administrator is the only user permitted to perform the management of TOE's security functionalities.

- Protection of the TSF (FPT)

When the TSF data is transmitted between the separated components of the TOE using the validated cryptographic module "AlphaCrypto V1.0" whose safety and implementation conformity are verified through the cryptographic module verification program(KCMVP).
The TOE protects the following data stored in the TSF data repository from unauthorized exposure and modification: passwords, encryption keys, critical security parameters, TOE configuration values (configuration parameters), and audit data.
The TOE performs self-tests at startup and periodically during normal operation to verify the correct operation of the Manager.

- TOE access (FTA)

The TOE limits maximum number of simultaneous sessions to one by permitting administrative access only from terminals with IP addresses designated for connection and restricting concurrent login from the same account.
Additionally, the TOE provides a session timeout mechanism that terminates the session if no activity is detected from the authorized administrator for a defined period (10 minutes) after successful login.

6. Documentation

The following documentations are evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
Alpha_DBGuard_V2.1_PREOPE_V1.4.pdf	V1.4	Sep. 19, 2025

[Table 7] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [9], based upon test cases devised by the evaluator. The evaluator 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.: Identifier of each test case
- Test Purpose: Includes the security functions 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 evaluator set up the test configuration and testing environment consistent with the ST [7].

In addition, the evaluator performed vulnerability analysis and penetration testing with test cases devised from the evaluator's independent search for potential vulnerabilities.

The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

8. Evaluated Configuration

The TOE is Alpha DBGuard V2.1(version number V2.1.0.3). See [Table 3] for details on the TOE components.

The TOE is installed from the CD-ROM distributed by Alphabit Co.,Ltd. After installing the TOE, an administrator can identify the TOE version through the product's menu.

The guidance documents listed in this report chapter 6, [Table 7] were evaluated with the TOE

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR [6] 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+.

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 Problem Definition clearly defines the security problems that the TOE and operational environment are intended to address. 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 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 specifications specify 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 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.
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	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	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	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	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 10] 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 developers integrating the encryption function of the TOE into an application or DBMS should comply with the requirements specified in the guidance documents to ensure that the security function of the TOE is applied properly.
- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.
- To maintain a safe state during TOE operation, follow the recommendations for safe operation before installing TOE according to the preparation procedure.
- The administrator should periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prevent audit data loss.
- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.
- The time information of each operating system where the TOE is installed should be synchronized to keep accurate time information.

11. Security Target

Alpha DBGuard V2.1 Security Target V1.3[7] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [8] according to the CCRA supporting document ST sanitizing for publication [11].

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

13. Bibliography

The certification body has used 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 1.1, CCMB-2024-07-002, July, 2024

[2] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, CCMB-2022-11-006, November, 2022
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, July, 2024

[3] Korea Evaluation and Certification Guidelines for IT Security (31 October 2022)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] Korean National Protection Profile for Database Encryption V3.1, KECS-PP-1350-2025, June 27, 2025

[6] Alpha DBGuard V2.1 Evaluation Technical Report V1.20, 24 September 2025

[7] Alpha DBGuard V2.1 Security Target V1.3, 19 September 2025 (Confidential Version)

[8] Alpha DBGuard V2.1 Security Target V1.3, 19 September 2025 (Sanitized Version)

[9] Alpha DBGuard V2.1 Independent Testing Report (ATE_IND.1) V1.20, 23 September 2025

[10] Alpha DBGuard V2.1 Penetration Testing Report (AVA_VAN.1) V1.20, 17 September 2025

[11] ST sanitizing for publication, CCDB-2006-04-004, April 2006