KECS-CR-23-26

Korean National Protection Profile for Database Encryption V3.0 Certification Report

Certification No.: KECS-PP-1232-2023

2023. 4. 27.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023. 4. 27.	-	Certification report for Korean National Protection Profile for Database Encryption V3.0 - First documentation

This document is the certification report for Korean National Protection Profile for Database Encryption V3.0 of National Security Research Institute (NSR).

The Certification Body

IT Security Certification Center (ITSCC)

The Evaluation Facility

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

Table of Contents

1. Executive Summary

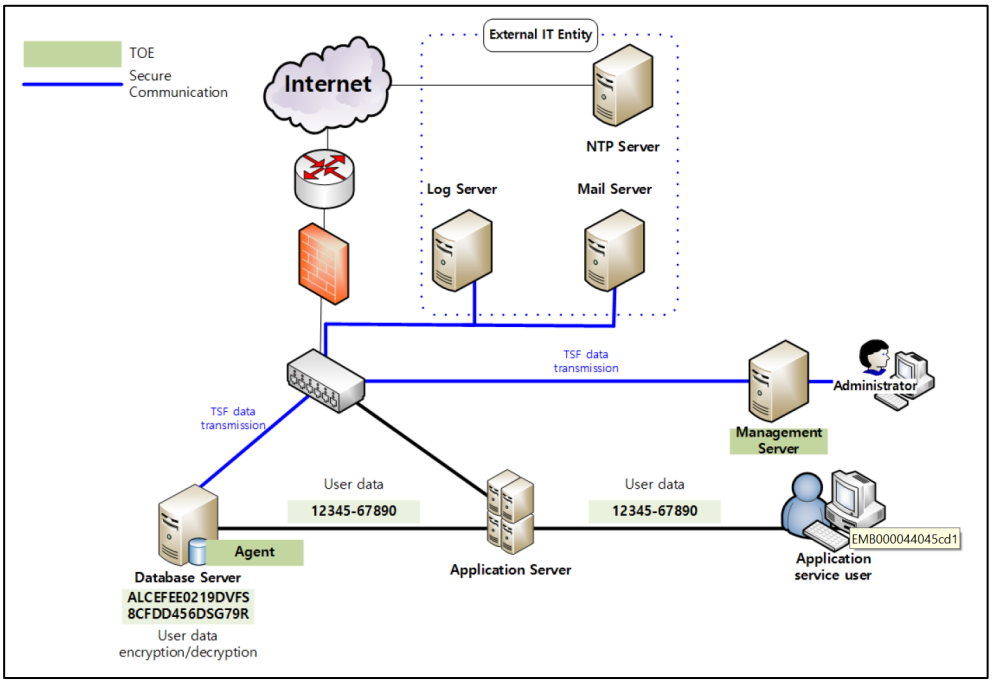
This report describes the certification result drawn by the certification body on the results of the APE evaluation of Korean National Protection Profile for Database Encryption V3.0 (“PP” hereinafter) [1] with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [2]. It describes the evaluation result and its soundness and conformity. The authors of the PP [1] are National Security Research Institute (NSR).

The Target of Evaluation (TOE) in the PP [1] is Database Encryption designed to prevent the unauthorized disclosure of confidential information by encrypting the database. Also, the TOE shall provide a variety of security features: security audit, the identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.. These TOE Security Functional Requirements (SFRs) are outlined in the PP [1].

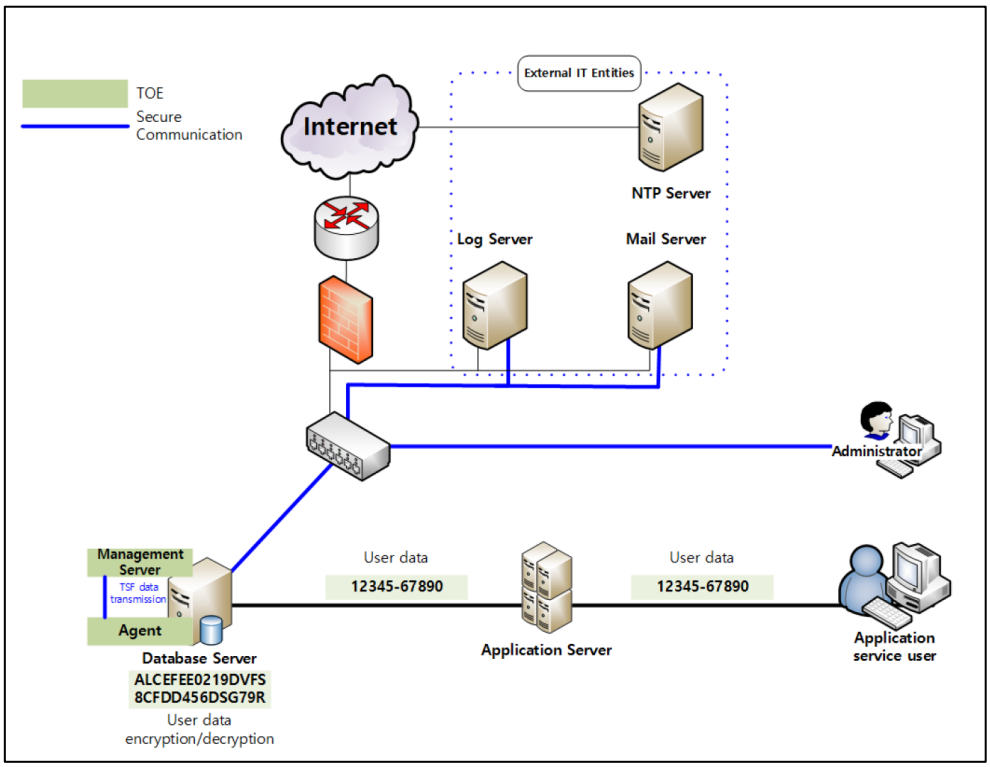
The evaluation of the PP [1] has been carried out by Korea Security Evaluation Laboratory Co., Ltd. (KSEL) and completed on 10 Nov 2022. This report grounds on the evaluation technical report (ETR) KSEL had submitted [6]. The evaluation of the PP [1] was performed in accordance with the APE (Protection Profile Evaluation) requirements in CC Part 3 and the Common Methodology for Information Technology Security Evaluation (“CEM” hereinafter) [3].

The PP [1] does not claim conformance to any other Protection Profile. All Security Assurance Requirements (SARs) in the PP [1] are based only upon assurance component in CC Part 3, and the assurance package is EAL1 augmented by ATE_FUN.1. Therefore the PP [1] is 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 [1]. Therefore the PP [1] is CC Part 2 extended. The PP [1] requires strict conformance.

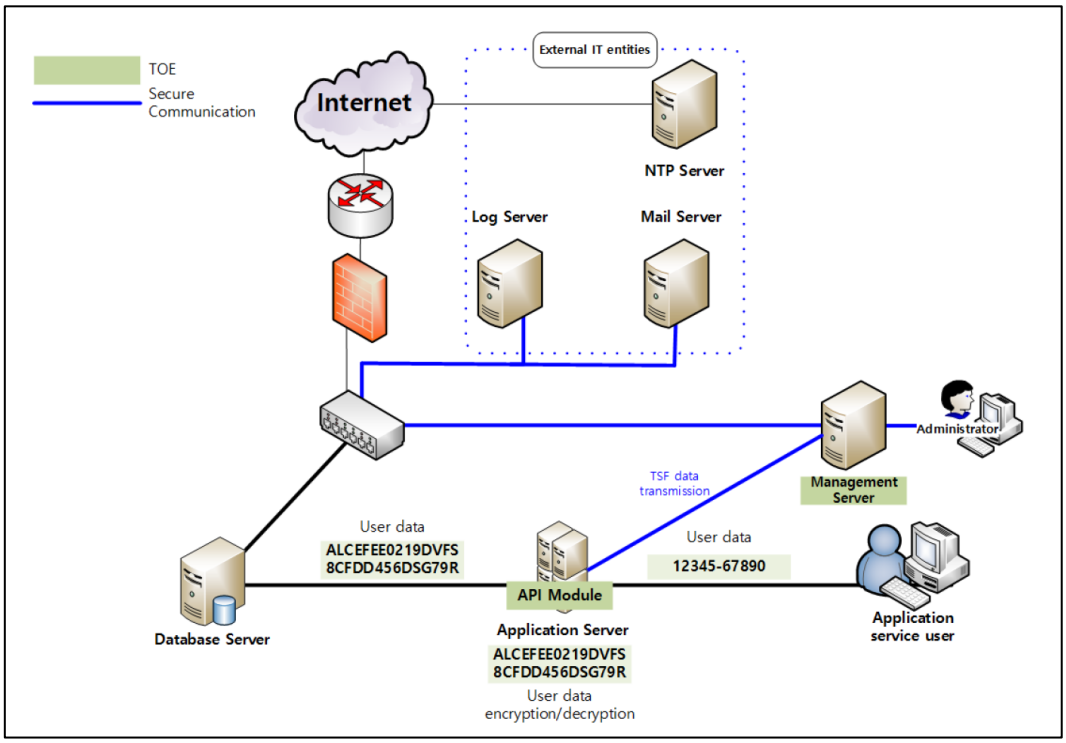
The operational environment of the Database Encryption is as shown in [Figure 1], [Figure 2], [Figure 3], and [Figure 4].



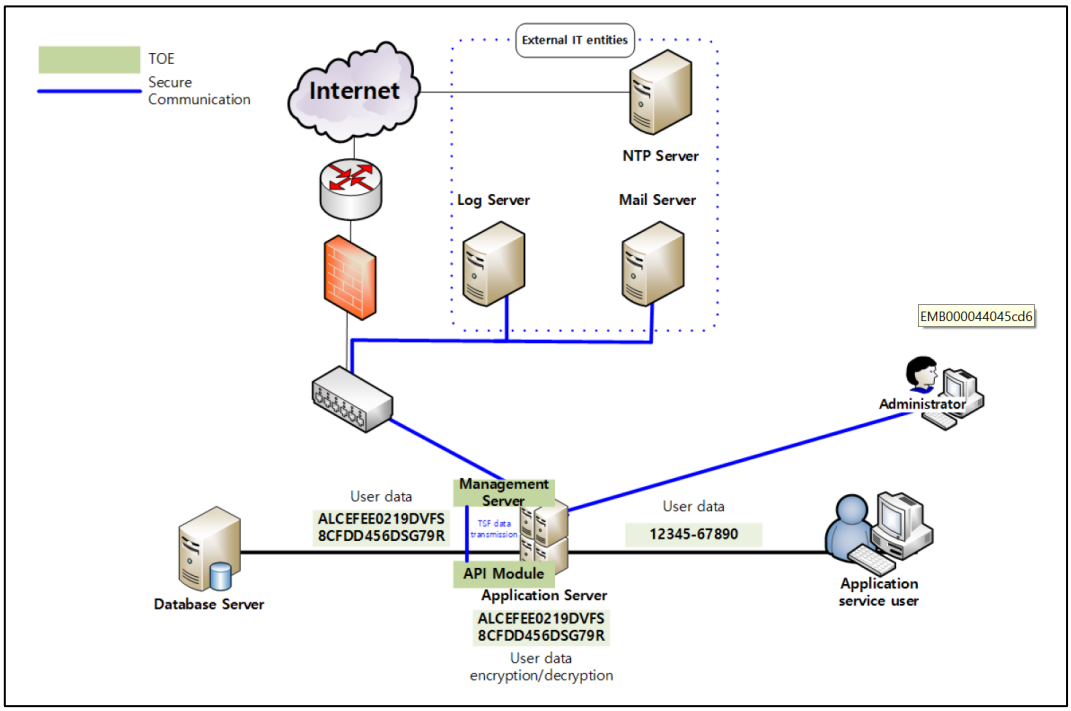
[Figure 1] Operational environment of Database Encryption (1)



[Figure 2] Operational environment of Database Encryption (2)



[Figure 3] Operational environment of Database Encryption (3)



[Figure 4] Operational environment of Database Encryption (4)

Certification Validity: The certificate is not an endorsement of the Protection Profile by ITSCC or by any other organization that recognizes or gives effect to this certificate, and no warranty of the Protection Profile by ITSCC or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

[Table 1] summarizes identification information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (31 October 2022) Korea Evaluation and Certification Scheme for IT Security (17 May 2021)
Name and Version of the Certified Protection Profile	Korean National Protection Profile for Database Encryption V3.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Common Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017
EAL	EAL1+ (augmented by ATE_FUN.1)
Developer	National Security Research Institute (NSR)
Sponsor	National Security Research Institute (NSR)
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	10 Nov 2022
Certification No.	KECS-PP-1232-2023
Certification Body	IT Security Certification Center (ITSCC)

[Table 1] Identification information

3. Security Policy

The PP [1] has reduced content of a low assurance PP, thus the PP [1] does not have any explicit security problem definition (i.e., threats, organisational security policies, and/or assumptions) and security objectives for the TOE. The TOE defined in the PP [1] provides security features in accordance with the SFRs. Refer to the PP [1] chapter 5 for details.

4. Assumptions and Clarification of Scope

The PP [1] has reduced content of a low assurance PP, thus the PP [1] does not have any explicit assumptions. The TOE defined in the PP [1] is the Database Encryption.

5. Results of the Evaluation

The PP [1] claims EAL1+ (ATE_FUN.1), thus has reduced content of a low assurance PP.

The evaluation facility provided the evaluation result in the ETR [6] which references a Single Evaluation Report for APE requirements and Observation Reports. The evaluation result was based on the CC [2] and CEM [3].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of APE.

5.1 Protection Profile Evaluation (APE)

The PP Introduction correctly identifies the PP, and the PP reference and the TOE overview are consistent with each other. Therefore the verdict PASS is assigned to APE_INT.1.

The Conformance Claim properly describes how the PP conforms to the CC and packages. Therefore the verdict PASS is assigned to APE_CCL.1.

The Security Objectives for the operational environment from the PP is clearly defined. Therefore the verdict PASS is assigned to APE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined,

and it is necessary. Therefore the verdict PASS is assigned to APE_ECD.1.
The Security Requirements is defined clearly and unambiguously, and it is internally consistent. Therefore the verdict PASS is assigned to APE_REQ.1.
Thus, the PP is sound and internally consistent, and suitable to be used as the basis for writing a low-assurance ST or another low-assurance PP.
The verdict PASS is assigned to the assurance class APE.

5.2 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
APE	APE_INT.1	APE_INT.1.1E	PASS	PASS	PASS
	APE_CCL.1	APE_CCL.1.1E	PASS	PASS	
	APE_OBJ.1	APE_OBJ.1.1E	PASS	PASS	
	APE_ECD.1	APE_ECD.1.1E	PASS	PASS	
		APE_ECD.1.2E	PASS		
	APE_REQ.1	APE_REQ.1.1E	PASS	PASS	

[Table 2] Evaluation Result Summary

6. Recommendations

The PP [1] defines the minimum security requirements for Database Encryption, and requires an ST or another PP claiming this PP [1] to fulfill the CC requirements for strict conformance, but only a low-assurance ST is allowed to make a conformance to the PP [1]. If the TOE defined in the ST which claims conformance to the PP [1] implements additional security features, then it is strongly recommended the ST author to define additional security functional requirements in accordance with the TOE implementation.

7. Acronyms and Glossary

CC Common Criteria

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

8. Bibliography

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

[1] Korean National Protection Profile for Database Encryption V3.0

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

- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components

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

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

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

[6] Korean National Protection Profile for Database Encryption V3.0 Evaluation Technical Report V1.00, 10 Nov 2022