KECS-CR-24-39

SafeDB V4.1

Certification Report

Certification No.: KECS-CISS-1317-2024

2024. 6. 28.

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2023. 6. 28.	-	Certification report for SafeDB V4.1 - First documentation

This document is the certification report for SafeDB V4.1 of INITECH Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

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 SafeDB V4.1(“TOE” hereinafter) 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 TOE is provided as software and provides the encryption/decryption function for the user data by each column of Database.

The TOE consists of SafeDB Policy Server that manages cryptographic operation policies and keys, SafeDB Manager that performs web security management, SafeDB Agent that is received security policy from SafeDB Policy Server and deploy the policy to SafeDB SDK and SafeDB Plug-In, SafeDB SDK which supports Java / C language, and SafeDB Plug-In applied to DBMS.

When the security administrator input policy information through the SafeDB Manager, the security policy is managed by the SafeDB Policy Server. The security policy is distributed as SafeDB Agent, and it is referenced in SafeDB SDK and SafeDB Plug-In cryptographic operation based on the received security policy.

The TOE is required to use the cryptographic algorithm validated in the Korea Cryptographic Module Validation Program (KCMVP).

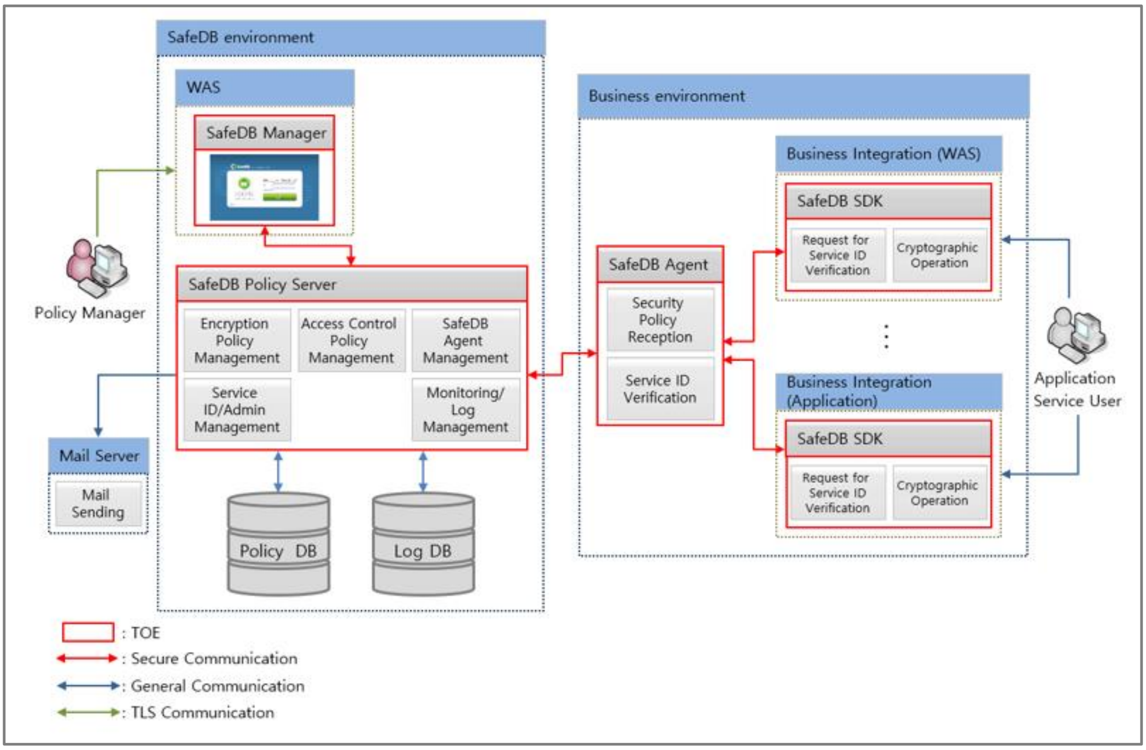
The TOE is used to encrypt the user data according to the policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information.

The TOE includes a variety of security features: security audit function that records the audit data for the critical events related to the security and management functions, identification and authentication function including verification of an administrator identity and authentication failures handling, TSF protection function such as protecting the data stored in the storage controlled by the TSF, TSF self-testing and integrity check. In addition, the TOE provides security management functions to define the administrator role and configure security functions, the TOE access function to manage the authorized administrator’s interacting session.

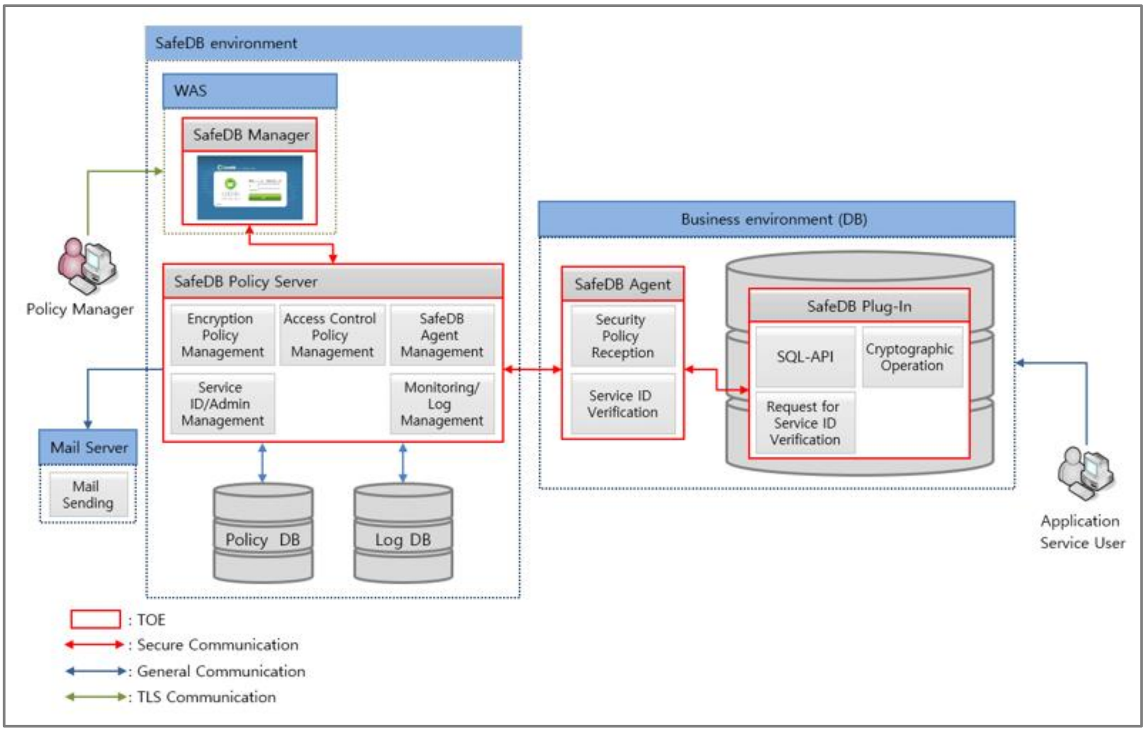
The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on June 25, 2024. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to the Korean National Protection Profile for Data Encryption V1.1 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. 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 operational environment of the TOE is shown in [Figure 1, 2] TOE Operational Environment. The operational environment of the TOE includes all the two types (API type, plug-in type) defined in the PP [3].



[Figure 1] Operational Environment of the TOE(API Type)



[Figure 2] Operational Environment of the TOE(Plug-In Type)

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 reference is identified as follows.

TOE	SafeDB V4.1
Version	V4.1.2
TOE Components	SafeDB Policy Server V4.1.2 SafeDB Manager V4.1.2 SafeDB Agent V4.1.2 SafeDB SDK for C V4.1.2 SafeDB SDK for Java V4.1.2 SafeDB Plug-In V4.1.2
Guidance Documents	CCP.C_SB41_Preparative Procedures (PRE)_V1.3.pdf CCP.C_SB41_Operational Guidance(OPE)_V1.2.pdf

[Table 1] TOE Identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

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, May 17, 2021) [4]
TOE	SafeDB V4.1
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (augmented by ATE_FUN.1)
Protection Profile	Korea National Protection Profile for Database Encryption V1.1, KECS-PP-0820a-2017, Dec. 11, 2019 [3]

Developer	INITECH Co., Ltd.
Sponsor	INITECH Co., Ltd.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	June 25, 2024
Certification Body	IT Security Certification Center

[Table 1] Additional Identification Information

3. Security Policy

The TOE provides following security features. For more details refer to the ST [6].

TSF	Explanation
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 operation such as encryption/decryption, and cryptographic key management such as key generation/distribution/destruction using INISAFE Crypto for C V5.4
User data protection	The TOE provides encryption / decryption function for each column of Database to protect user data.
Identification and Authentication	The TOE identifies and authenticates the administrators(Policy Manager, General Manager, Install Manager) based on ID/PW. Mutual authentication between TOE components.
Security Management	Only the authorized administrator who can access the management interface provided by TOE can performs security management of the TOE.
Protection of the TSF	The TOE provides secure communications amongst TOE components to protect confidentiality and integrity of the transmitted data between them. The TOE also protects TSF data against unauthorized exposure and modification through encryption.

TSF	Explanation
TOE Access	The TOE manages the authorized administrator's or end user's access to itself by terminating interactive sessions after defined time interval of their inactivity. The TSF restrict the maximum number of concurrent session, and management access session of the administrator based on Access IP, and same administrator right.

[Table 3] Security Features

4. Assumptions and Clarification of Scope

There are no explicit Assumptions in the Security Problem Definition in the Low Assurance ST. The followings are procedural method supported from operational environment in order to provide the TOE security functionality accurately.

- The place where TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
- The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.
- The developer who uses the TOE to interoperate with the user identification and authentication function in 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.
- The authorized administrator shall periodically checks a spare space of 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.
- 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.
- Security policies and audit records are stored in the trusted database. Without the request of the TOE, the database is not created, modified or deleted.
- The TOE shall accurately record the security related events using the reliable time stamp from the TOE operational environment.

- A secure path shall be ensured by the security policy of WAS in case of TOE administrator’s UI access and use via a web browser on an authorized administrator’s PC.

5. Architectural Information

The physical scope of the TOE consists of SafeDB Policy Server, SafeDB Manager, SafeDB Agent, SafeDB SDK for C, SafeDB SDK for Java, SafeDB Plug-In and guidance documents.

The major security functions of the TOE and logical scope of the TOE are shown in [Figure 1, 2] and chapter 3, [Table 3]

For the detailed description, refer to the ST [6].

6. Documentation

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

Identifier	Release	Date
CCP.C_SB41_Preparative Procedures (PRE)_V1.3	V1.3	June. 7, 2024
CCP.C_SB41_Operational Guidance(OPE)_V1.2	V1.2	June. 7, 2024

[Table 4] 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. 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 has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator 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: SafeDB V4.1(version detail: V4.1.2)

- SafeDB Policy Server V4.1.2
- SafeDB Manager V4.1.2
- SafeDB Agent V4.1.2
- SafeDB SDK for C V4.1.2
- SafeDB SDK for Java V4.1.2
- SafeDB Plug-In V4.1.2

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation results in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation results were 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 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.

9.3 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 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.

9.5 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 Results 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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
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 5] Evaluation Results 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 authorized administrator must install and operate the TOE and DBMS in a physically secure environment accessible only to authorized administrators and must not allow remote management from external sources.
- Developers integrating encryption functions with applications or DBMS using the TOE must adhere to the requirements of the documentation provided with the TOE

to ensure the secure application of the TOE's security features.

- During product operation, administrators must maintain a secure state by periodically changing the administrator's password.
- To maintain the reliability and security of the operating system where the TOE is installed and operated, the latest vulnerability mitigation measures must be applied.
- The authorized administrator must periodically check the free space of the audit data storage to prevent loss of audit records and perform backups to ensure audit records are not exhausted.
- After installing the product, the administrator must register their email address in the product to ensure that warning emails can be sent in the event of potential security violations. The email address must be accurately registered to confirm the functionality works correctly.
- The authorized administrator must set only the necessary policies and delete unused policies to prevent potential vulnerabilities.

11. Security Target

The SafeDB V4.1 Security Target V1.6 [6] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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 evaluation facility has used the 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] Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)

[5] TTA-CCE-22-002 SafeDB V4.1 Evaluation Technical Report V1.3, June 25, 2024

[6] SafeDB V4.1 Security Target V1.6, June 7, 2024