KECS-CR-19-14

SafeDB V4.0

Certification Report

Certification No.: KECS-CISS-0921-2019

2019. 3. 11.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.03.11.	-	Certification report for SafeDB V4.0 - First documentation

This document is the certification report for SafeDB V4.0 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 evaluation of SafeDB V4.0 of INITECH 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.

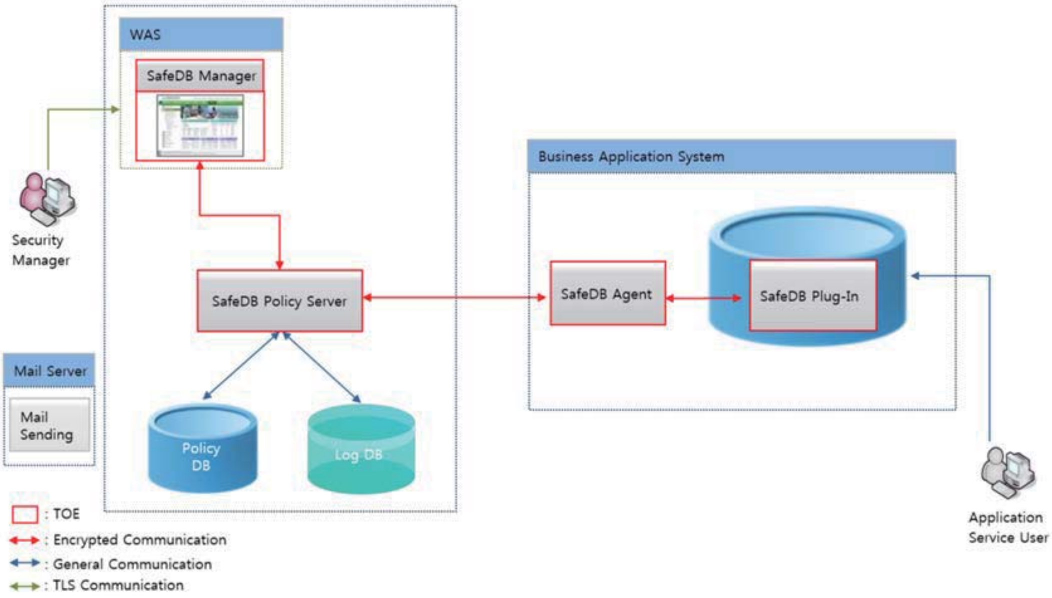
The Target of Evaluation (TOE) is database encryption software that encrypts and decrypts the user data in a column of a database to be protected. The TOE consists of SafeDB Policy Server, SafeDB Manager, SafeDB Agent, SafeDB Plug-In, SafeDB SDK for Java, and SafeDB SDK for C. SafeDB Policy Server allows authorized administrators to manage security functions and TSF data such as cryptographic operation policies and keys, SafeDB Manager provides management interfaces to authorized administrators, SafeDB Agent fetches security policies and data encryption keys from SafeDB Policy Server, and SafeDB Plug-In encrypts and decrypts the user data based on the policies. SafeDB SDK for Java and SafeDB SDK for C behave the same way as SafeDB Plug-In does. The TOE includes cryptographic modules (INISAFE Crypto for Java v4.1, INISAFE Crypto for C V5.3) validated under the Korea Cryptographic Module Validation Program (KCMVP).

There are two types of the TOE operational environments: plug-in and API types. In the plug-in type, SafeDB Plug-In is installed in a database server, while SafeDB SDK(SafeDB SDK for Java and SafeDB SDK for C) is installed in an application server in the API type.

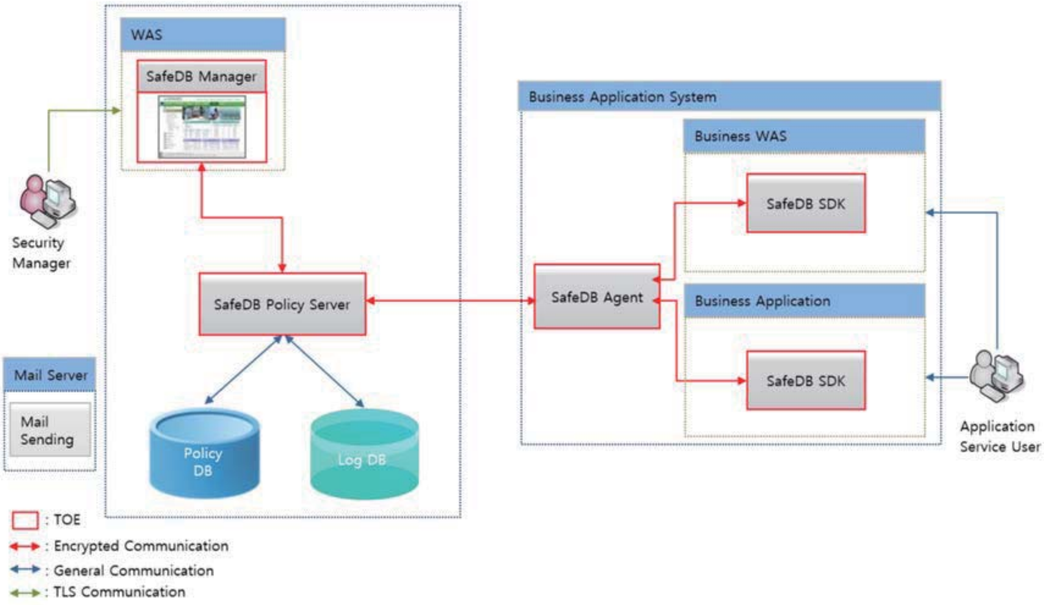
The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on March 8, 2019. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to the Korean National PP for Database Encryption V1.0 [7]. 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 the PP [7]. 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 newly defined components in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] and [Figure 2] show the operational environments of the TOE.



[Figure 1] Operational environment of the TOE (Plug-in type)



[Figure 2] Operational environment of the TOE (API type)

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Category		Contents
SafeDB Policy Server	CPU	Intel Core i5-5200U 2.20GHz or higher
	RAM	8GB or higher
	HDD	40MB or higher space for installation of SafeDB Policy Server
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit
	Required S/W	ElasticSearch v2.4.5 Apache Derby v10.14.2.0 JRE 8.0 (1.8.0_192)
SafeDB Manager	CPU	Intel Core i5-5200U 2.20GHz or higher
	RAM	8GB or higher
	HDD	70MB or higher space for installation of SafeDB Manager
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit
	Required S/W	JRE 8.0 (1.8.0_192) Apache Tomcat v8.5.37
SafeDB Agent	CPU	Intel Core i5-5200U 2.20GHz or higher
	RAM	8GB or higher
	HDD	10MB or higher space for installation of SafeDB Agent
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit
	Required S/W	JRE 8.0 (1.8.0_192)
SafeDB Plug-In	CPU	Intel Core i5-5200U 2.20GHz or higher
	RAM	8GB or higher
	HDD	10MB or higher space for installation of SafeDB Plug-In
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit
	Required S/W	Oracle 12c
SafeDB	CPU	Intel Core i5-5200U 2.20GHz or higher

SDK for Java	RAM	8GB or higher
	HDD	10MB or higher space for installation of SafeDB SDK for Java
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit
	Required S/W	JRE 8.0 (1.8.0_192)
SafeDB SDK for C	CPU	Intel Core i5-5200U 2.20GHz or higher
	RAM	8GB or higher
	HDD	10MB or higher space for installation of SafeDB SDK for C
	NIC	10/100/1000 X 1Port or higher
	OS	Windows Server 2008 R2 Enterprise SP1 64-bit

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator’s PC to access SafeDB Manager.

Category	Contents
CPU	Intel Core2 2.13 GHz or higher
RAM	2GB or higher
HDD	500GB or higher
NIC	10/100/1000 X 1Port or higher
OS	Windows 7 Professional SP1 (64-bit)
Required S/W	Internet Explorer 11 Chrome 65.0

[Table 2] The minimum 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	SafeDB V4.0	
Version	V4.0.3	
TOE Components	SafeDB Policy Server	SafeDB Policy Server V4.0.3 (SafeDB_PolicyServer_4.0.3.zip)
	SafeDB Manager	SafeDB Manager V4.0.3 (SafeDB_Manager_4.0.3.zip)
	SafeDB Agent	SafeDB Agent V4.0.3 (SafeDB_Agent_4.0.3.zip)
	SafeDB Plug-In	SafeDB Plug-In V4.0.3 (SafeDB_Plugin_4.0.3.zip)
	SafeDB SDK for Java	SafeDB SDK for Java V4.0.3 (SafeDB_SDK_Java_4.0.3.zip)
	SafeDB SDK for C	SafeDB SDK for C V4.0.3 (SafeDB_SDK_C_4.0.3.zip)
Guidance Document	CCP.C_SB40_Preparative Procedures (PRE)_V1.4.pdf CCP.C_SB40_Operational Guidance(OPE)_V1.4.pdf	

[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 Scheme for IT Security (September 12, 2017)
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 PP for Database Encryption V1.0, KECS-PP-

	0820-2017, August 18, 2017
Developer	INITECH Co., Ltd
Sponsor	INITECH Co., Ltd
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	March 8, 2019
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [6] for the TOE claims strict to the Korean National PP for Database Encryption V1.0 [7], and complies security policies defined in the PP [7] by security requirements. Thus, the TOE provides security features defined in the PP [7] 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 (INISAFE Crypto for Java v4.1, INISAFE Crypto for C V5.3) 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.

4. Assumptions and Clarification of Scope

There is no explicit Security Problem Definition chapter, therefore no Assumptions section in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [7] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [6], chapter 3.):

5. Architectural Information

The TOE is software consisting of the following components:

- SafeDB Policy Server provides security features of identification and authentication of administrators, cryptographic key managements, and security management to the TOE and TSF data.
- SafeDB Manager provides management interfaces to authorized administrators.
- SafeDB Agent provides CLI-based management interface to an authorized administrator.
- SafeDB Agent fetches security policies and data encryption key from SafeDB Policy Server, then provides those data to SafeDB Plug-In, SafeDB SDK for Java, and SafeDB SDK for C.
- SafeDB Plug-In, SafeDB SDK for Java, SafeDB SDK for C encrypt and decrypt the user data in a column of a database.

Note that all the five 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 [6], chapter 1.4.3.

6. Documentation

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

Identifier	Release	Date
CCP.C_SB40_Preparative Procedures (PRE)_V1.4	V1.4	Feb. 14, 2019
CCP.C_SB40_Operational Guidance(OPE)_V1.4	V1.4	Feb. 14, 2019

[Table 5] Documentation

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.: Identifier of each test case
- 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 SafeDB V4.0 (version number V4.0.3). See table 3 for detailed information on the TOE components.

The TOE is installed from the CD-ROM distributed by INITECH Co., Ltd. After installing the TOE, an administrator can identify the complete TOE reference using the product's Info check menu. The guidance documents listed in this report Chapter 6, [Table 5] 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 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 it is 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 uniquely identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration list includes the TOE and the evaluation evidence required by the SARs in the ST. Therefore, the verdict PASS is assigned to ALC_CMS.1.

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 developer has provided a high-level description of at least 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 TSF, 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, 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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.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.2	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 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:

- The authorized administrator should set only necessary policies, and delete unused policies to prevent potential vulnerabilities.
- It is necessary to maintain a secure state of the TOE by such as periodically changing the administrator's password.
- The authorized administrator shall maintain the secure state, by such as applying the latest security patches to the operating system and DBMS, and by

removing unnecessary services.

- The authorized administrator shall periodically check the free space of the audit data storage in preparation for the loss of the audit records and backup the audit records so that the audit records are not deleted.
- The authorized administrator must register their e-mail address in the product so that warning e-mail can be delivered to the administrator in case of the occurrence of any potential security violation event.
- An authorized administrator should install and operate an IT security product such as an intrusion prevention system in front of the database to protect from network threats.

11. Security Target

SafeDB V4.0 Security Target V1.6 [6] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
KCMVP	the Korea Cryptographic Module Validation Program
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

Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Encryption	The act that converting the plaintext into the ciphertext

	using the cryptographic key
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
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

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

[3] Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)

[5] TTA-CCE-17-013 SafeDB V4.0 Evaluation Technical Report V1.5, March 8, 2019

[6] SafeDB V4.0 Security Target V1.6, February 14, 2019

[7] Korean National PP for Database Encryption V1.0 (KECS-PP-0820-2017, August 18, 2017)