KECS-CR-22-40

Spiceware DBE v2.0

Certification Report

Certification No.: KECS-CISS-1182-2022

2022. 9. 2.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2022.09.02.	-	Certification report for Spiceware DBE v2.0 - First documentation

This document is the certification report for Spiceware DBE v2.0 of Spiceware Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the evaluation of Spiceware DBE v2.0 of Spiceware 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.

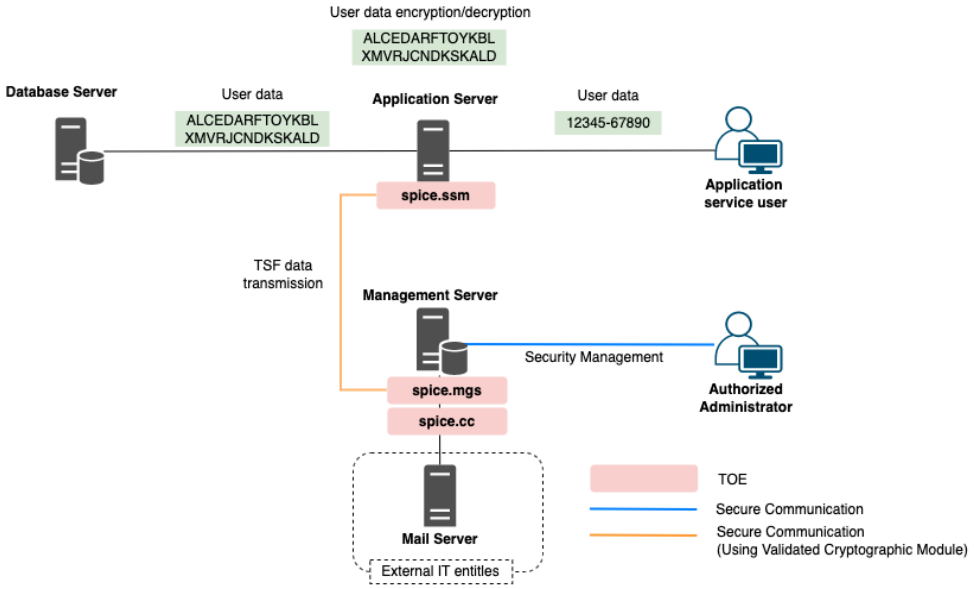
The Target of Evaluation (TOE) is database encryption software to prevent the unauthorized disclosure of confidential information by encrypting the database. The TOE consists of spice.ssm, spice.cc, and spice.mgs. The component spice.cc allows an authorized administrator (‘Master’) to manage security functions and TSF data such as cryptographic operation policies and keys. The component spice.ssm is an agent that encrypts and decrypts the user data based on the policies. The TOE includes cryptographic modules (AhnLab Cryptographic Module V1.0) validated under the Korea Cryptographic Module Validation Program (KCMVP). The operational environment of the TOE is API type, where the agent spice.ssm is installed on an application server, and the components spice.cc and spice.mgs are installed on a management server.

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on 26 August 2022. This report grounds on the evaluation technical report (ETR) KTC had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1 [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] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

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

Category		Contents
spice.ssm	CPU	Intel Core i5 CPU @2.7 GHz or higher
	RAM	16GB or higher
	HDD	30GB or higher space for installation of spice.ssm
	NIC	10/100/1000 X 1Port or more
	OS	Ubuntu 16.04 (64bit, Kernel 4.17)
	Required S/W	Amazon corretto 8.342.07.3
spice.cc, spice.mgs	CPU	Intel Core i5 CPU @2.7 GHz or higher
	RAM	32GB or higher
	HDD	30GB or higher space for installation of spice.cc and spice.mgs
	NIC	10/100/1000 X 1Port or more
	OS	Ubuntu 16.04 (64bit, Kernel 4.17)
	Required S/W	Tomcat 9.0.65 Amazon corretto 8.342.07.3 MySQL 5.7.38 Elasticsearch 7.13.4

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator's PC to access spice.cc.

Category	Contents
Web Browser	Chrome 97.0 (64bit)
OTP Generator	Authenticator 6.3.3 (by authenticator.cc)

[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	Spiceware DBE v2.0	
Version	v2.0.5	
TOE Components	spice.ssm	spice.ssm-2.0.1 (spice.ssm-2.0.1.tar.gz)
	spice.cc	spice.cc-2.0.3 (spice.cc-2.0.3.tar.gz)
	spice.mgs	spice.mgs-2.0.1 (spice.mgs-2.0.1.tar.gz)
Guidance Document	Spiceware DBE v2.0 Operational User Guidance v1.4 (Spiceware DBE v2.0-Operational User Guidance_v1.4.pdf) Spiceware DBE v2.0 API Guide v1.0 (Spiceware DBE v2.0-API Guide_v1.0.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 (May 17, 2021)
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 Protection Profile for Database Encryption V1.1, KECS-PP-0820a-2017, 11 December 2019
Developer	Spiceware Co., Ltd.
Sponsor	Spiceware Co., Ltd.
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	26 August 2022
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE provides security features defined in the PP [7] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up and shutdown of the audit functions, integrity violation and self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic operation such as encryption/decryption and hash, cryptographic key management such as key generation/distribution/destruction, and random bit generation using cryptographic modules (AhnLab Cryptographic Module V1.0) 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 ID/password, and mutually authenticate TOE components when they communicate each other.
- Security management: Security management of the TOE is restricted to only the authorized administrator who can access the management interface provided by 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 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. The TOE 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:

- spice.cc allows authorized administrators to manage security functions and TSF data such as cryptographic operation policies and keys
- spice.mgs transmits the policies to the agent spice.ssm.
- spice.ssm encrypts and decrypts the user data based on the policies.

Note that all the three components perform the 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 1.4.2.

6. Documentation

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

Identifier	Release	Date
Spiceware DBE v2.0 Operational User Guidance v1.4	v1.4	August 24, 2022
Spiceware DBE v2.0 API Guide v1.0	v1.0	January 21, 2022

[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 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

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, performed all tests provided by developer, 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 Spiceware DBE v2.0 (version number v2.0.5). See table 3 for detailed information on the TOE components.
The TOE is installed from the CD-ROM distributed by Spiceware Co., Ltd. After installing the TOE, an administrator can identify the complete TOE reference using the product version menu. And 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 the PP 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 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 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 provided by the developer specify 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, the identified potential vulnerabilities, 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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	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		
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		
	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 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:

- Developers who make the encryption/decryption functions of the TOE interact with other applications or DBMSs should ensure that the functions are securely applied according to the guidance document provided with the TOE.

- When operating the product, the administrator's password should be changed periodically to keep its security.
- The TOE shall be located in a physically secure environment to which only the authorized administrator is allowed to access and the protective facilities are provided.
- When the audit storage space is fulled, audit data may be lost, so periodic monitoring and periodic backup are required.
- The administrator shall maintain a safe state by applying, for example, the latest security patches, eliminating unnecessary service, and changing of the default ID/password of the operating system and DBMS in the operational environment of the TOE.

11. Security Target

Spiceware DBE v2.0 Security Target v1.4 [6] is included in this report for reference.

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
Encryption	The act that converting the plaintext into the ciphertext using the cryptographic key
Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Application Server	A server in which applications developed to provide

	specific application services in the organization operating the TOE are installed and operated
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority
Column	A set of data values of a particular simple type, one for each row of the table in a relational database
DBMS	A software system composed to configure and apply the database.

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 (24 August 2017)

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

[5] CC2021-00011 Evaluation Technical Report V2.0, 26 August 2022

[6] Spiceware DBE v2.0 Security Target v1.4, 24 August 2022

[7] Korean National Protection Profile for Database Encryption V1.1 (KECS-PP-0820a-2017, December 11, 2019)