KECS-CR-20-30

D’Guard v3.0

Certification Report

Certification No.: KECS-CISS-1016-2020

2020. 05. 20

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.05.20	-	Certification report for D'Guard v3.0 - First documentation

This document is the certification report for D'Guard v3.0 for INEB Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the EAL1+ evaluation of D'Guard v3.0("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 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 types defined in this ST are grouped into the 'plug-in type' and 'API type', depending on the TOE operation type. The TOE supports both types. The plug-in type is a method that performs encryption on the DB Server and operates dependent on the database. Since TOE module(the plug-in type) is installed in the protected DB server to perform encryption/decryption, the DBMS is limited to Oracle 12.2. The API type performs encryption in the application server (hereinafter 'AP') and is classified into Java API and C API according to application work environment.

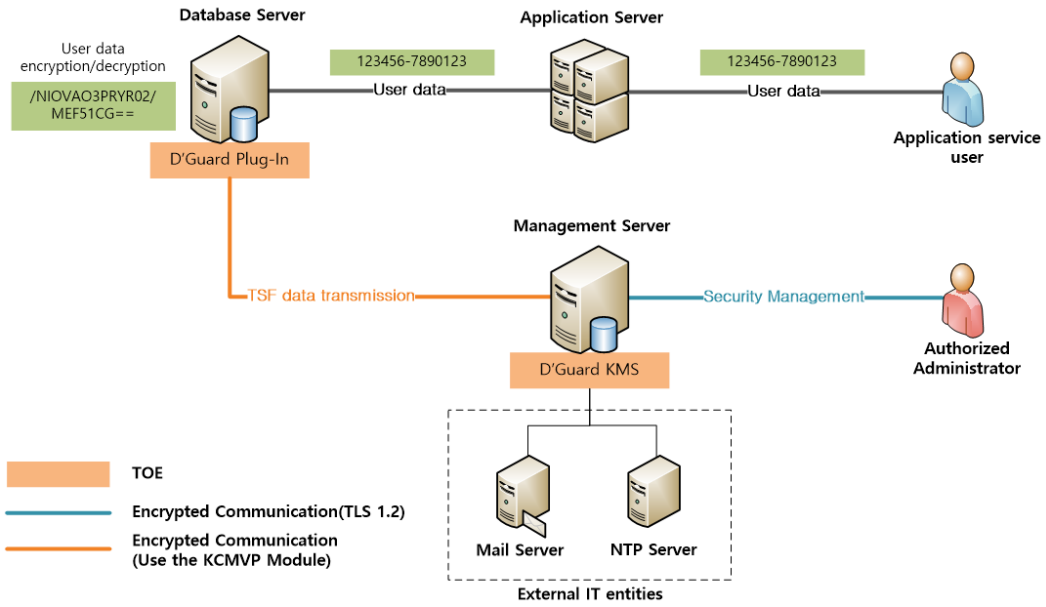
The TOE consists of D'Guard KMS, D'Guard Java API, D'Guard C API, and D'Guard Plug-In v3.0.4. Components of the TOE are the management server that manages policies and keys (hereinafter referred to as D'Guard KMS), agents that perform encryption in the C work environment (hereinafter referred to as D'Guard C API), and agents that perform encryption in the Java work environment (hereinafter referred to ad D'Guard Java API). And it consists of agent (D'Guard Plug-In) which performs encryption in DB Server. The D'Guard KMS provides services that perform key distribution roles, perform policy management roles and collect agent logs. The TOE administrator accesses the D'Guard KMS through a web browser and performs management roles. It also plays an administrative role in the console environment for initialization and operation.

The TOE includes cryptographic modules(MagicCrypto V2.0.0.0, INISAFE Crypto for C V5.3) validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on May 13, 2020. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6].

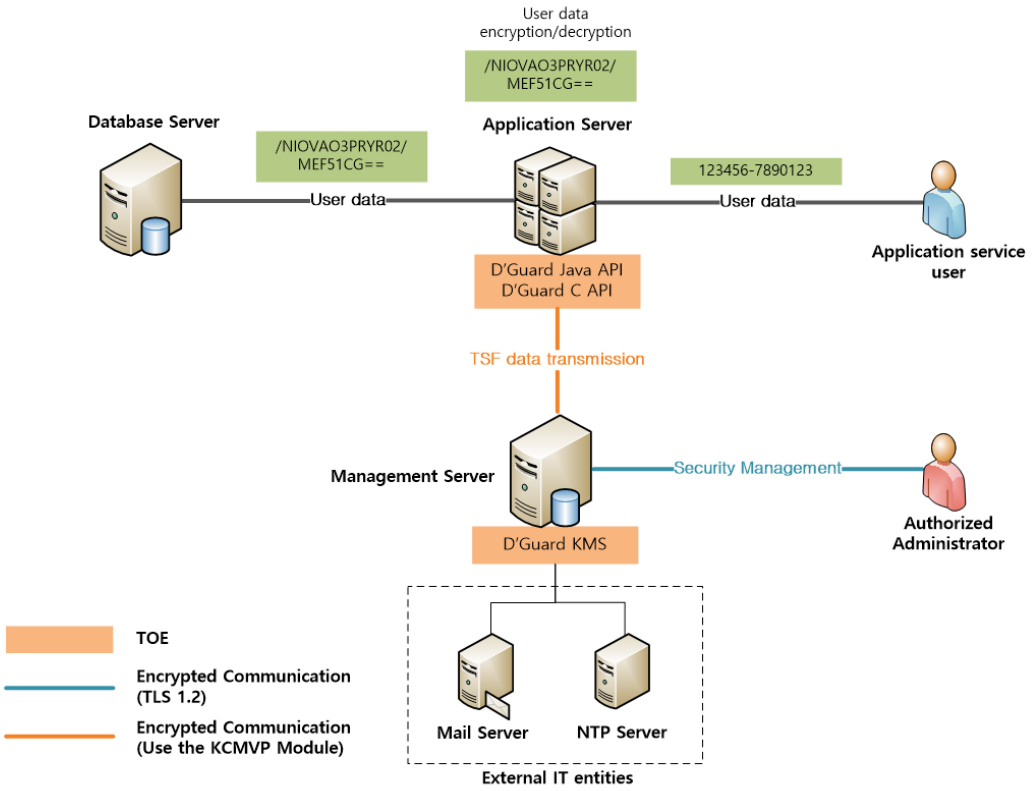
The ST claims strict conformance to the Korean National Protection Profile for Data Encryption V1.0 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. The ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (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] TOE Operational Environment. The operational environment of the TOE includes all the two types(API type, plug-in type) defined in the PP [3]. In the Plug-in type, the DBMS is limited to Oracle 12.2.



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

[Figure 2] shows the general operational environment of the API type. The application, which is installed in the application server and provides application services, is developed using the D'Guard Java API or D'Guard C API provided by API module in order to use the cryptographic function of the TOE. The D'Guard Java API or D'Guard C API module is installed in the application server and performs encryption/decryption of the user data in accordance with the policies configured by authorized administrator. The user data entered by the application service user is encrypted by D'Guard Java API or D'Guard C API module, which is installed in the application server, and sent to the database server. The encrypted user data received from the database server is decrypted by the D'Guard Java API or D'Guard C API module, which is installed in the application server, and sent to the application service user.



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

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

Category		Contents
D'Guard KMS	CPU	Intel i5 3.3 GHz or higher
	RAM	8GB or higher
	HDD	1GB or higher necessary for installing the TOE
	NIC	10/100/1000 X 1 port or higher
	OS	CentOS 7.7 (Linux kernel version: 3.10.0-1062)
	Required S/W	PostgreSQL 10.12
		Apache Tomcat 8.5.51
		JRE (Java Runtime Environment) 8.0
D'Guard Plug-In	CPU	IBM POWER 3.0 GHz or higher
	RAM	16GB or higher
	HDD	30MB or higher necessary for installing the TOE
	NIC	10/100/1000 X 1 port or higher
	OS	AIX 7.1 TL5 (64 bit)
	Required S/W	Oracle 12.2
D'Guard Java API	CPU	Intel i5 3.3 GHz or higher
	RAM	8GB or higher
	HDD	30MB or higher necessary for installing the TOE
	NIC	10/100/1000 X 1 port or higher
	OS	CentOS 7.7 (Linux Kernel 3.10.0-1062))
	Required S/W	JRE (Java Runtime Environment) 8.0
D'Guard C API	CPU	Intel i5 3.3 GHz or higher
	RAM	8GB or higher
	HDD	30MB or higher necessary for installing the TOE
	NIC	10/100/1000 X 1 port or higher
	OS	CentOS 7.7 (Linux Kernel 3.10.0-1062)

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator's PC to access D'Guard KMS.

Category		Contents
Software	Web Browser	Chrome 80.0 (64bit)

[Table 2] The minimum requirements for the administrator's PC

2. Identification

The TOE reference is identified as follows.

TOE	D'Guard v3.0
Detail Version	v3.0.4
TOE Components	D'Guard KMS v3.0.4 (D'Guard_KMS_v3.0.4.zip)
	D'Guard Plugin v3.0.4 (D'Guard_Plug-In_v3.0.4.zip)
	D'Guard C API v3.0.4 (D'Guard_C_API_v3.0.4.zip)
	D'Guard Java API v3.0.4 (D'Guard_Java_API_v3.0.4.zip)
Guidance Documents	D'Guard v3.0 KMS Document_v1.4 (D'Guard_v3.0_KMS_Document_v1.4.pdf) D'Guard v3.0 Java API Document_v1.4 (D'Guard_v3.0_Java_API_Document_v1.4.pdf) D'Guard v3.0 Plug-In Document v1.4 (D'Guard_v3.0_Plug-In_Document_v1.4.pdf) D'Guard v3.0 C API Document v1.4 (D'Guard_v3.0_C_API_Document_v1.4.pdf) D'Guard v3.0 Admin Document v1.3 (D'Guard_v3.0_Admin_Document_v1.3.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)[4]
TOE	D'Guard 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
Protection Profile	Korean National PP for Database Encryption V1.1, KECS-PP- 0820a-2017, December 11, 2019
EAL	EAL1+ (augmented by ATE_FUN.1)
Developer	INEB Inc.
Sponsor	INEB Inc.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	May 13, 2020
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST by security objectives and security requirements. The TOE provides following security features as follows. For more details refer to the ST [7].

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

TSF	Explanation
	key generation/distribution/destruction using MagicJCrypto V2.0.0.0, INISAFE Crypto for C V5.3
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(super administrator, security user) 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.
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 5] Security Functions

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

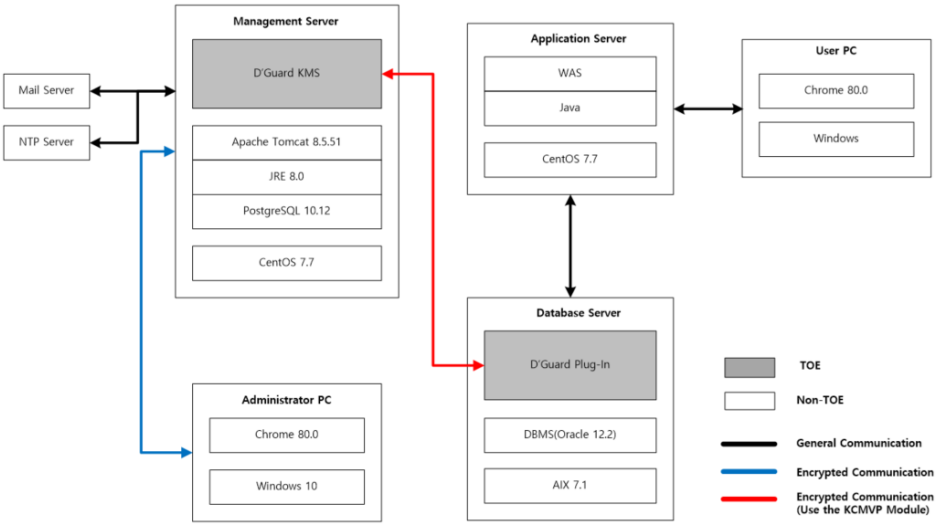
authentication function in operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

- 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.

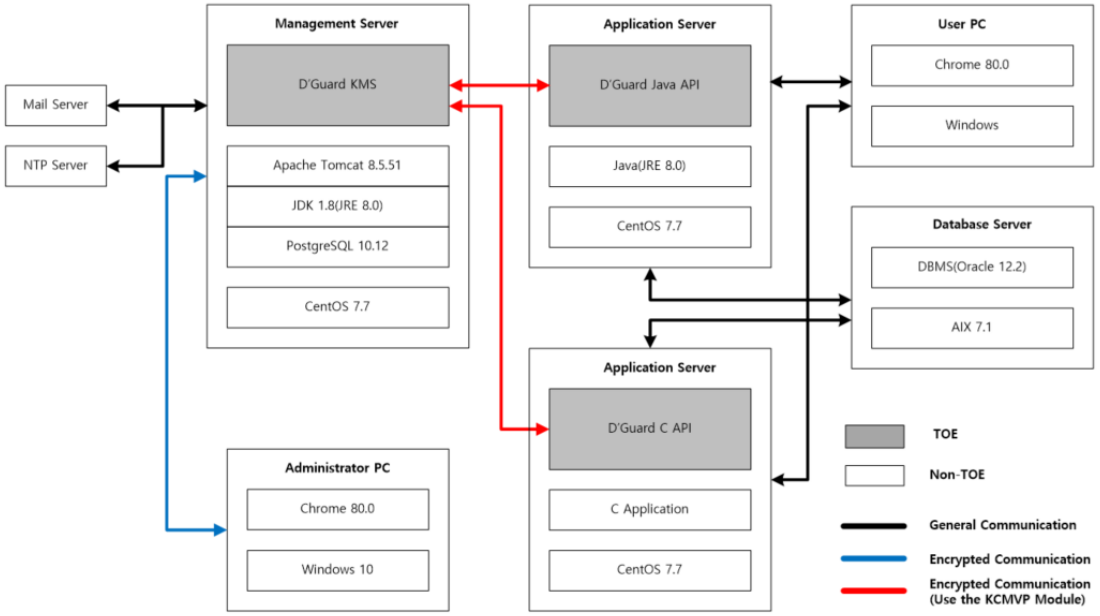
5. Architectural Information

5.1 Physical Scope of TOE

The physical scope and boundaries of the TOE are shown in the following figure.



[Figure 3] Physical scope of the TOE (Plug-In type)



[Figure 4] Physical scope of the TOE (API type)

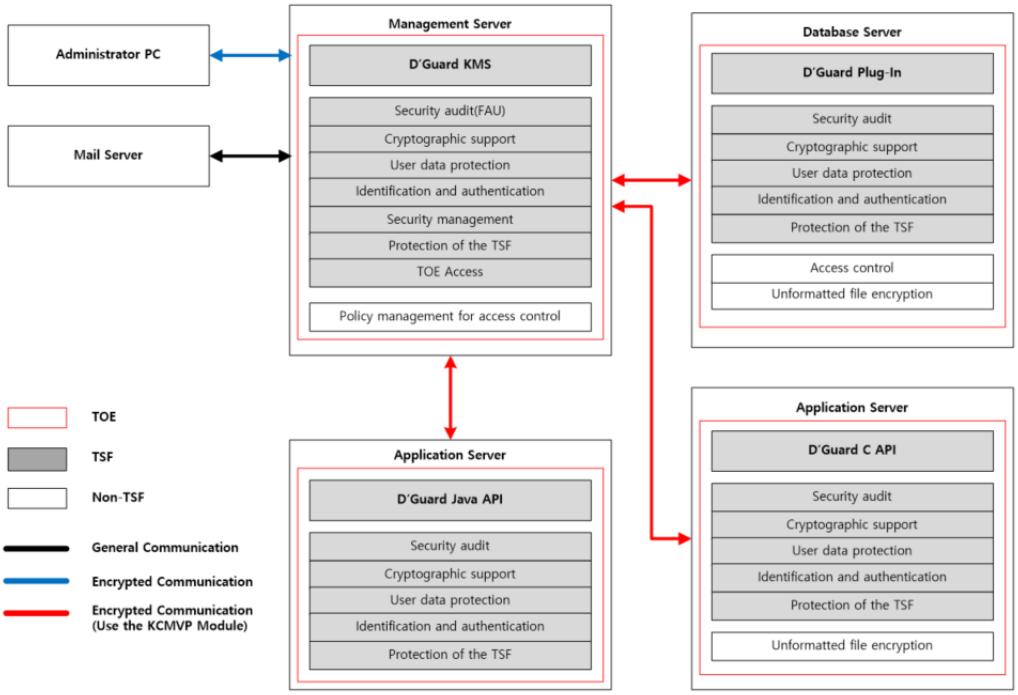
[Table 6] shows the physical scope of the TOE including softwares and documentations. The physical scope of the TOE is divided into the D'Guard KMS, D'Guard Plug-In, D'Guard Java API, D'Guard C API and documentation. Verified Cryptographic Module(MagicCrypto V2.0.0.0, INISAFE Crypto for C V5.3) is embedded in the TOE components. Hardware, operating system, DBMS, WAS, JRE which are operating environments of the TOE are excluded from the physical scope of the TOE.

Type	Identification	
S/W	TOE Component	D'Guard KMS v3.0.4 (D'Guard_kMS_v3.0.4.zip)
		D'Guard Java API v3.0.4 (D'Guard_Java_API_v3.0.4.zip)
		D'Guard C API v3.0.4 (D'Guard_C_API_v3.0.4.zip)
		D'Guard Plug-In v3.0.4 (D'Guard_Plug-In_v3.0.4.zip)
Doc (PDF)	Guidance document	D'Guard v3.0 KMS Document_v1.4 (D'Guard_v3.0_KMS_Document_v1.4.pdf)
		D'Guard v3.0 Java API Document_v1.4 (D'Guard_v3.0_Java_API_Document_v1.4.pdf)

		D'Guard v3.0 Plug-In Document v1.4 (D'Guard_v3.0_Plug-In_Document_v1.4.pdf)
		D'Guard v3.0 C API Document v1.4 (D'Guard_v3.0_C_API_Document_v1.4.pdf)
		D'Guard v3.0 Admin Document v1.3 (D'Guard_v3.0_Admin_Document_v1.3.pdf)

[Table 6] Physical scope of the TOE

5.2 Logical Scope of TOE



[Figure 5] Logical scope of the TOE

The TOE is software consisting of the following components:

D'Guard KMS provides security features such as administrator identification and authentication, password key management and security management for TOE and TSF data.

- D'Guard KMS provides a Web-based management interface to authorized administrators.

- D'Guard KMS provides an authorized administrator with a CLI-based management interface.

- The D'Guard KMS can send security policy and user data encryption keys to the D'Guard Plug-In, D'Guard Java API and D'Guard C API according to the security policy set by the administrator.

- D'Guard Plug-In, D'Guard Java API and D'Guard C API encrypt and decrypt user data in database column.

Note that all the four components perform the same functionalities of audit data generation, cryptographic key management, cryptographic operations, protection of TSF data, and mutual authentication between the components.

The following functions are excluded from the evaluation scope.

[D'Guard KMS]

Access control policy management

The D'Guard KMS provides access control policy management function by the authorized administrator when encrypting user data according to date, time, and day of the week based on database account, IP address, MAC address, and application. This function is a security function of the TOE that is excluded from evaluation. The access control policy management function according to the date, time, and day of the week is not a security requirement required by the National Database Encryption Protection Profile (PP), and does not perform/support the security function.

[D'Guard Plug-In]

Access control function

The D'Guard Plug-In performs access control policy management function by an authorized administrator when encrypting user data according to date, time, and day of the week based on database account, IP address, MAC address, and application. This function is a security function of the TOE that is excluded from evaluation. The access control policy management function according to the date, time, and day of the week is not a security requirement required by the National Database Encryption Protection Profile (PP), and does not perform/ support the security function.

Unstructured File Encryption

The TOE administrator provides a function to encrypt/decrypt user data or log files in the form of files using encryption programs (the Dgsam, the Dgfile). The unstructured file encryption function is not a security requirement required by the National Database Encryption Protection Profile (PP), and does not perform/support the security function.

[D'Guard C API]

Unstructured File Encryption

The TOE administrator provides the ability to encrypt and decrypt unstructured files containing user data using encryption programs (dgsam, dgfile). The unstructured file encryption function is not a security requirement required by the National Database Encryption Protection Profile (PP), and does not perform/support the security function.

For the detailed description on the architectural information, refer to the ST [6], chapter 1.4.

6. Documentation

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

Identifier	Release	Date
D'Guard v3.0 KMS Document v1.4 (D'Guard_v3.0_KMS_Document_v1.4.pdf)	V1.4	April. 7, 2020
D'Guard v3.0 Java API Document_v1.4 (D'Guard_v3.0_Java_API_Document_v1.4.pdf)	V1.4	April. 7, 2020
D'Guard v3.0 Plug-In Document v1.4 (D'Guard_v3.0_Plug-In_Document_v1.4.pdf)	V1.4	April. 7, 2020
D'Guard v3.0 C API Document v1.4 (D'Guard_v3.0_C_API_Document_v1.4.pdf)	V1.4	April. 7, 2020
D'Guard v3.0 Admin Document v1.3 (D'Guard_v3.0_Admin_Document_v1.3.pdf)	V1.3	April. 7, 2020

[Table 6] 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 D′Guard v3.0(3.0.4) and software consisting of the following components:

- D'Guard KMS v3.0.4
- D'Guard Plug-In v3.0.4

- D'Guard C API v3.0.4
- D'Guard Java API v3.0.4

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 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 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 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 specifies 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.

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 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	
		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_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.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.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	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 1] 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 administrator should install and operate the TOE and DBMS in a physically secure environment accessible only by the authorized administrator, and should not allow remote management from the outside.
- Developers who link the encryption function to the application or DBMS should ensure that the security functions of the TOE are applied safely in accordance with the requirements of the manual.
- The authorized administrator should manage the encryption key, security policy to prevent leakage and grant the policy appropriate to the application service user authority.
- The authorized administrator should periodically perform encryption key backup in case of loss of encryption key information.
- The authorized administrator should set only necessary policies, and delete unused policies to prevent potential vulnerabilities.
- It is necessary to maintain a secure state, such as periodically changing the administrator's password when operating the product.
- The authorized administrator shall maintain the secure state, such as applying the latest security patches to the operating system and DBMS, and removing

unnecessary services, when operating the product.

- The authorized administrator shall periodically check the free space of the audit data storage in preparation for the loss of the audit records and perform the backup of the audit records so that the audit records are not deleted.
- The authorized administrator must register the e-mail address of the administrator in the product so that warning e-mail can be normally sent out when a potential security violation event occurs after installation of the product.
- An authorized administrator should install and operate an IT security product (eg, an intrusion prevention system) in front of the DB to respond to network threats.

11. Security Target

The D'Guard v3.0 Security Target V1.5, May 12, 2020 [7] is included in this report by 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
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
Column	A set of data values of a particular simple type, one for each row of the table in a relational database
Database	A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this ST, refers to the relational database.
DBMS (Database Management System)	A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this ST, refers to the database management system based on the relational database model.
dgfile	A program that encrypts and decrypts all unstructured files
dgsam	This is a program that encrypts and decrypts the value of a specific item by separating the values of each item from the unstructured file by a separator or a fixed length.

13. Bibliography

The evaluation facility 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

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

[5] TTA-CCE-17-017 D'Guard v3.0 Evaluation Technical Report V1.3, May 13, 2020

[6] D'Guard v3.0 Security Target V1.5, May 12, 2020 (Sanitized Version)