KECS-CR-21-14

HEDES v1.0

Certification Report

Certification No.: KECS-CISS-1084-2021

2021. 3. 17.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2021.03.17.	-	Certification report for HEDES v1.0 - First documentation

This document is the certification report for HEDES v1.0 of HumaneSystem Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

Certification Report 1

1. Executive Summary 5

2. Identification 8

3. Security Policy 9

4. Assumptions and Clarification of Scope 9

5. Architectural Information 10

    1. Physical Scope of TOE 10

    2. Logical Scope of TOE 10

6. Documentation 14

7. TOE Testing 14

8. Evaluated Configuration 15

9. Results of the Evaluation 15

    1. Security Target Evaluation (ASE) 15

    2. Development Evaluation (ADV) 16

    3. Guidance Documents Evaluation (AGD) 16

    4. Life Cycle Support Evaluation (ALC) 17

    5. Test Evaluation (ATE) 17

    6. Vulnerability Assessment (AVA) 17

    7. Evaluation Result Summary 18

10. Recommendations 19

11. Security Target 20

12. Acronyms and Glossary 20

13. Bibliography 22

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the HEDES v1.0 developed by HumaneSystem 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" hereinafter) is database encryption software to prevent unauthorized exposure of the information from DBMS. Also, the TOE shall provide a variety of security features: security audit, cryptographic operation using cryptographic module, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc..

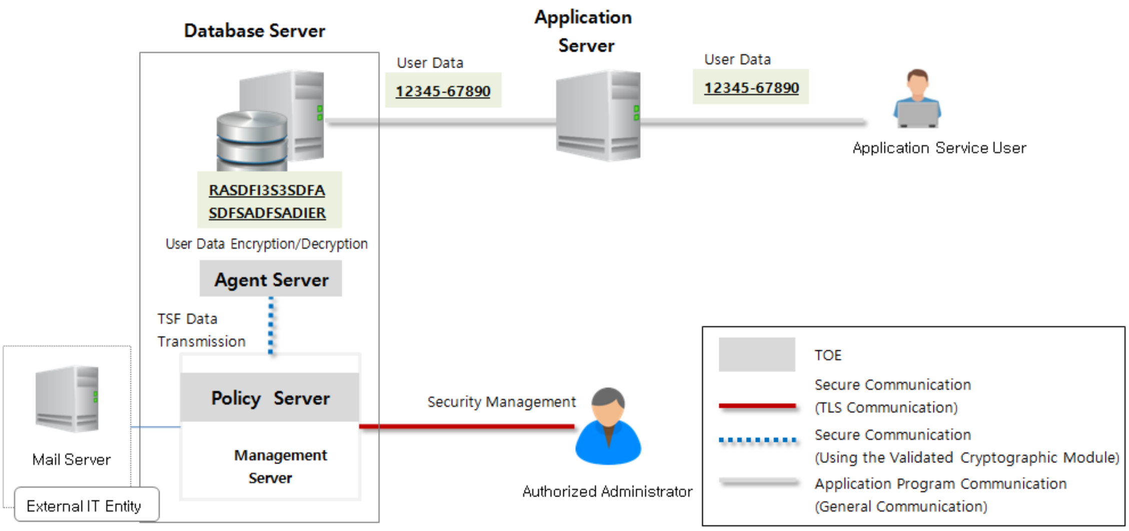
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on February 22, 2021.

The ST claims conformance to the Korean National Protection Profile for Database Encrytion V1.1[3]. 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 Evaluation Assurance Level EAL1+. 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 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 TOE is comprised of the Policy Server and Agent Server, and can be installed 'Plug-in' type. [Figure 1] shows the operational environment of the TOE.

[Figure 1] shows a typical operational environment of the plug-in type.

The plug-in operational environment is composed of the Policy Server and Agent Server. First, the Policy Server manages the information on policies established by the authorized administrator and manages the keys and the audit records. It also encrypts the information on a distributed key and loads it on the shared memory. Second, the Agent Server is installed inside the Database Server where the DB under the protection is located, and encrypts the user data received from the Application Server before they are stored in the DB. In addition, it decrypts the encrypted user data to be transmitted from the Database Server to the Application Server.



[Figure 1] Plug-in type operational environment of the TOE

(Agent, management server integrated type)

The application service user requests the encryption or decryption of the user data through the Application Server in accordance with the scope of the encryption as required by the security policy. The requested data are encrypted by the Agent Server and stored in the DB. The authorized administrator accesses the Policy Server to perform the security management of the encrypted data stored in the DB.

The cryptographic algorithm subject to the validation in the validated cryptographic module is used for the communication between the TOE components for the purpose of secure communication. In case the administrator accesses the Policy Server through a web browser, a secure path (TLS V1.2) is generated to carry out the communication.

As other external entities necessary for the operation of the TOE, there is email server to send alerts by email to the authorized administrator.

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

Classification			Minimum Requirement
HEDES Policy Server / HEDES Agent Server	HW	CPU	Intel Xeon CPU E3-1220 @ 3.10Ghz (4 Core) or higher
		Memory	16 GB or higher
		HDD	Space required for installation of TOE : 300 GB or higher
		NIC	10/100/1000 Mbps * 1 EA or higher
	SW	OS	CentOS 7.9 (kernel v3.10, 64 bit)
		JAVA	JAVA JRE 1.8.0_281
		DBMS	MySQL 5.7
		WAS	Jetty 9.4.36

[Table 1] TOE Hardware and Software specifications

Administrator uses the pc that can operate web browser to use the security management. Administrator pc minimum requirements are shown in [Table 2]

Classification	Minimum Requirement

SW	Web Browser	Google Chrome 88

[Table 2] Administrator PC Requirements.

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		HEDES v1.0
TOE Build Version		20210129-001
TOE Components	**Policy Server**	HEDES Policy Server v1.0-20210129-001
	Agent Server	HEDES Agent Server v1.0-20210129-001
Guidance		HEDES v1.0 Preparative Procedure v1.3 HEDES v1.0 Operational User Guidance v1.3

[Table 3] TOE identification

[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 Regulation for IT Security (September 12, 2017)
TOE	HEDES v1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)

Protection Profile	Korean National Protection Profile for Database Encryption V1.1
Developer	HumaneSystem Co., Ltd.
Sponsor	HumaneSystem Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	February 22, 2021

[Table 4] Additional identification information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User data protection
- Identification and Authentication
- Security Management
- Prtoection of the TSF
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4]

4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 3])

5. Architectural Information

1. Physical Scope of TOE

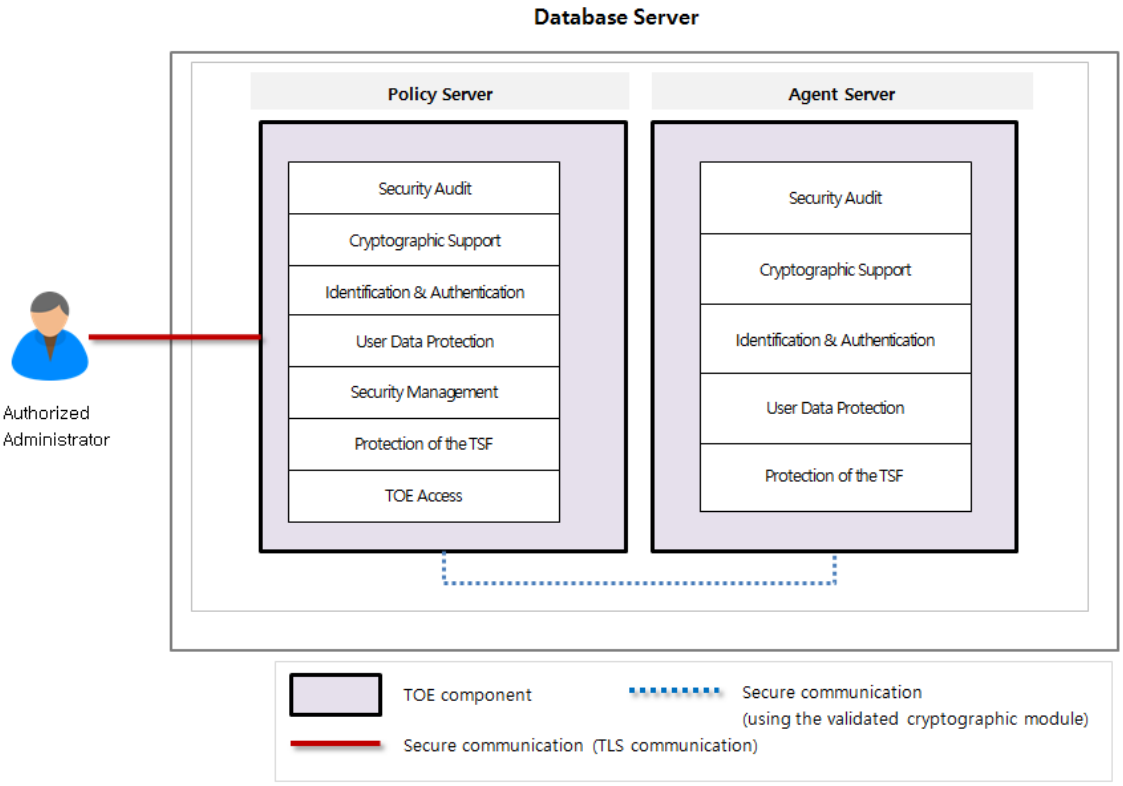
The physical scope of the TOE consists of the HEDES Policy Server, HEDES Agent Server and preparative procedure, operation guide. Verified Cryptographic Module(MagicCrypto V2.2.0) is embedded in the TOE components. Hardware, operating system, DBMS, WAS, JRE which are operating environments of the TOE are excluded from the physical scope of the TOE.

Classification		Identification	Type
TOE component	Policy Server	HEDES Policy Server v1.0-20210129-001 (hedes_policy_server_1.0_002.tar)	Software (Distributed as a CD)
	Agent Server	HEDES Agent Server v1.0-20210129-001 (hedes_agent_server_1.0_002.tar)	
Guidance		HEDES v1.0 Preparative Procedure v1.3 (hds_pre_004.pdf)	PDF (Distributed as a CD)
		HEDES v1.0 Operational User Guidance v1.3 (hds_ope_004.pdf)	

[Table 5] Physical scope of TOE

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 2] below.



[Figure 2] TOE Logical scope

▣ Security Audit

The TOE provides the authorized administrator with the function to search and view audit information, and also provides audit information such as date, time, IP, event type, event subject, details, etc. It generates audit records in case of auditable events, and sends an alarm email to the authorized administrator upon the detection of a potential security violation. It also stores all the generated audit data in an audit trail storage (DBMS) and securely manage them. The TOE prevents the unauthorized deletion of audit data, and provides the function to protect the audit trail storage by overwriting the oldest stored audit data if the audit trail storage is full.

▣ Cryptographic support

The TOE generates and destructs all cryptographic keys used for the operation of the product through MagicCrypto V2.2.0, the validated cryptographic module whose security and implementation conformance have been validated by the cryptographic module validation scheme. It performs cryptographic operations according to the cryptographic policy that defines cryptographic algorithms. In addition, the cryptographic key is generated and exchanged through MagicCrypto V2.2.0, which is the validated cryptographic module, for the encrypted communication between TOE components.

To generate the cryptographic key is generated, a cryptographic key is generated using a random bit through a random bit generator (HASH_DRBG 256) of the validated cryptographic module, and to encrypt user data of the DBMS to be protected is encrypted, the encryption algorithm (SEED 128(CBC), ARIA 256(CBC), SHA-512). In addition, a hash algorithm (SHA-512), symmetric key encryption (SEED 128(CBC), ARIA 256(CBC)) are used for protction of TSF data. For mutual authentication of the TOE, mutual authentication is secured through public key encryption methods (RSAES 2048, RSA-PSS 2048, ECDH 256), and when the encryption key is destroyed, it is overwritten with '0' to perform destruction.

▣ User data protection

To protect user data stored in the DBMS under the protection, it is encrypted and stored using a verified encryption module. Encryption/decryption is performed through block encryption algorithms (ARIA 256(CBC)) and (SEED 128(CBC)) according to the security policy set by the authorized administrator. Additionally, SHA-512 is provided for the one-way encryption algorithm.

The TOE provides the function of the encryption/decryption of user data at the column level . In addition, The same ciphertext is not generated for the same plaintext when encrypting the user data. After the encryption/decryption is completed, the memory area is initialized with “0” value and the used memory area is deallocated so that the user data are unrecoverable in the memory.

▣ Identification and authentication

The TOE provides identification and authentication functions for administrators who perform security management functions, and provides functions to protect authentication feedback when entering authentication data. In addition, the acceptance criteria are verified through password combination rules. In addition, it provides an authentication lock processing function in case of consecutive authentication failures. The TOE provides a function to block an attempt to reuse authentication information for an administrator.

The TOE performs the mutual authentication through the protocol developed by HumaneSystem Co., Ltd. for the purpose of the secure communication among the TOE components.

▣ Security Management

The TOE provides the authorized administrator with the security management function such as policy management, administrator management and environment configuration. The authorized administrator performs the security management through the security management interface. In addition, the administrator ID and password are designated during the installation. When the authorized administrator accesses the security management interface, the TOE enforces the authorized administrator to change the password if the password expiration date arrives (expiration period: 100 days). There is only one type of privilege of the authorized administrator, which is the top administrator.

▣ Protection of the TSF

The TOE protects the TSF data stored in containers controlled by the TSF, and the TSF data transmitted between TOE components. It also checks major security function processes, etc. by conducting TSF self tests. The TOE runs a suite of self tests during initial start-up and periodically during normal operation (1 hour interval), and verifies the integrity of TOE configuration files and major processes during initial start-up and periodically during normal operation. Then, if the integrity was compromised, it sends an alarm email to the administrator.

The TOE manages the information on administrator authentication, TOE integrity verification and so forth by storing them in the DBMS in a secure manner in order to protect the TSF data.

▣ TOE access

The TOE restricts the number of the administrator’s management access sessions whose access is allowed to perform the security management function to one. If the same account makes new access, it terminates the existing session and generates audit data. Also, if the administrator remains inactive for 10 minutes, it terminates the existing session and requires the administrator to be reauthenticated.

In the case of the administrator, access sessions are restricted according to the rule for allowing access IP. The TOE allows the management sessions made only from a device (2 or less) whose IP was designated and allowed to access, and generates audit data on the result of the limitation of sessions by the security management interface.

6. Documentation

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

Identification	Date
HEDES v1.0 Preparative Procedure v1.3 (hds_pre_004.pdf)	January 29, 2021
HEDES v1.0 Operational User Guidance v1.3 (hds_ope_004.pdf)	January 29, 2021

[Table 6] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [5], based upon test cases devised by the evaluator. The evaluator 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. 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 evaluator set up the test configuration and testing environment consistent with the

ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [6].

8. Evaluated Configuration

The TOE is software consisting of the following components:
TOE: HEDES v1.0 (20210129-001)
- HEDES Policy Server v1.0-20210129-001
- HEDES Agent Server v1.0-20210129-001

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 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation. (EAL1+).

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.

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.

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.

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.

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.

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.

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		
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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 7] 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 TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.

- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.

- The administrator should periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prvent audit data loss.

- The developer who uses the TOE to interoperate with the user identification and authentication function in the 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.

11. Security Target

HEDES v1.0 Security Target V1.4 [4] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

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

(2) Glossary

Application Server
The application server defined in this PP refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DB to the database server.

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 PP, refers to the relational database.

Database Server

The database server defined in this PP refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

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 PP, refers to the database management system based on the relational database model.

Data Encryption Key (DEK)

Key that encrypts and decrypts the data

Decryption

The act that restoring the ciphertext into the plaintext using the decryption key

Encryption

The act that converts the plaintext into the ciphertext using the encryption key

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Management access

The access to the TOE by using the HTTPS, SSH, TLS, etc to manage the TOE by administrator, remotely

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Secret Key
A cryptographic key which is used in an symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

HEDES Agent Server
A software module that processes the encryption or decryption of the data of a user according to the encryption/decryption policy of the Policy Server

HEDES policy server
A software module for the authorized administrator to manage the establishment of the encryption/decryption policy

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, December 11, 2019

[4] HEDES v1.0 Security Target V1.4, January 29, 2021

[5] HEDES v1.0 Independent Testing Report(ATE_IND.1) V1.00, February 19, 2021

[6] HEDES v1.0 Penetration Testing Report (AVA_VAN.1) V1.00, February 19, 2021