KECS-CR-19-69

Hancom xDB V2.8

Certification Report

Certification No.: KECS-CISS-0976-2019

2019. 11. 15.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.11.15.	-	Certification report for Hancom xDB V2.8 - First documentation

This document is the certification report for Hancom xDB V2.8 of Hancom With Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Information Security Technology (KOIST)

Table of Contents

1. Executive Summary

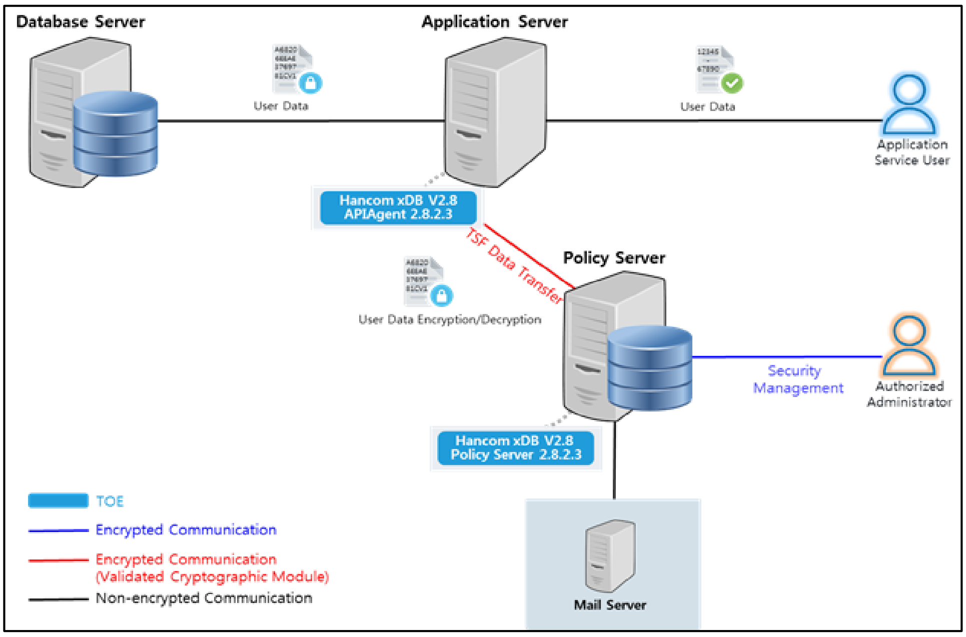
This report describes the certification result drawn by the certification body on the results of the evaluation of Hancom xDB V2.8 of Hancom With Inc. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and its 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 Hancom xDB V2.8 Policy Server, Hancom xDB V2.8 APIAgent, Hancom xDB V2.8 PluginAgent.

The Hancom xDB V2.8 Policy Server ("Policy Server" hereinafter) will be located in the environment that uses cryptographic services. Therefore, it is independent of the environment where data is stored. The Hancom xDB V2.8 APIAgent ("APIAgent" hereinafter) requests encryption and decryption policies from the Policy Server to perform encryption and decryption. The Hancom xDB V2.8PluginAgent ("PluginAgent" hereinafter) is a PluginAgent installed in the database server. it is in charge of receiving the user data delivered from the application server when encryption is in progress, performing DB encryption and decryption according to the policy of the Policy Server at the time of DBMS storage.The TOE includes cryptographic modules(XecureCrypto 2.0.1.1) validated under the Korea Cryptographic Module Validation Program (KCMVP).

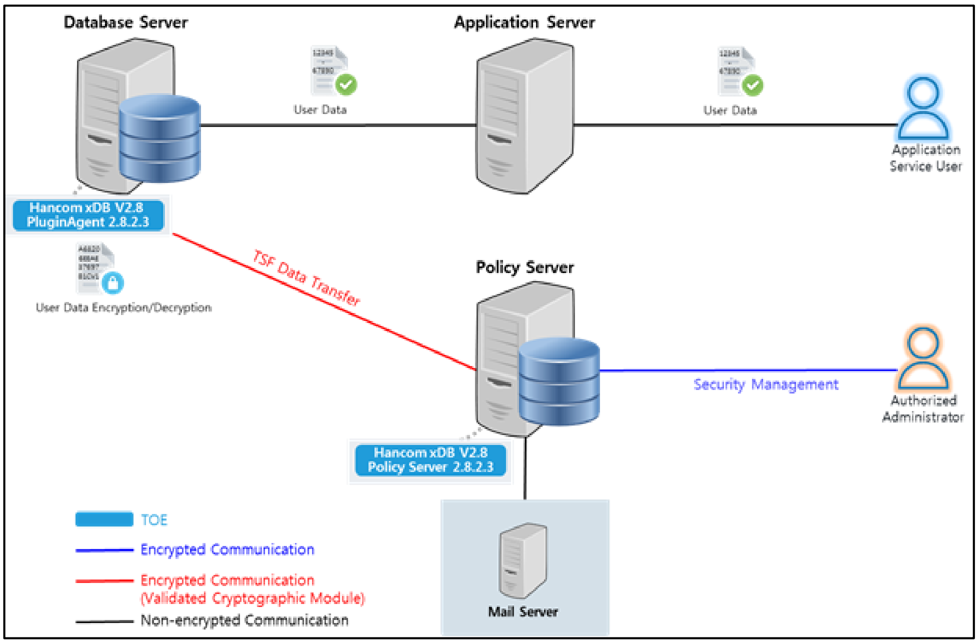
There are two types of the TOE operational environments: plug-in and API types. In the plug-in type, PluginAgent is installed in a database server, while APIAgent is installed in an application server

The evaluation of the TOE has been carried out by Korea Information Security Technology (KOIST) and completed on October 29, 2019. This report grounds on the evaluation technical report(ETR) KOIST 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 (API type)


Database Server
Application Server
User Data
User Data
Application Service User
Hancom xDB V2.8 PluginAgent 2.8.2.3
User Data Encryption/Decryption
TSF Data Transfer
Policy Server
Security Management
Authorized Administrator
Hancom xDB V2.8 Policy Server 2.8.2.3
TOE
Encrypted Communication
Encrypted Communication (Validated Cryptographic Module)
Non-encrypted Communication
Mail Server

[Figure 2] Operational environment of the TOE (Plug-in type)

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

TOE	OS	Division	Minimum Requirements
Hancom xDB V2.8 Policy Server	Linux	OS	CentOS 6.10 kernel 2.6.32 (64 bit)
		CPU	Xeon E3-1220 3.1 GHz or faster
		RAM	16 GB or more
		HDD	Disk space for TOE installation and operation: 100 GB or more
		NIC	1 port or more of 10/100/1000 Ethernet card
Hancom xDB V2.8 APIAgent	Linux	OS	CentOS 6.10 kernel 2.6.32 (64 bit)
		CPU	Xeon E3-1220 3.1 GHz or faster
		RAM	16 GB or more

		HDD	Disk space for TOE installation: 10 MB or more
		NIC	1 port or more of 10/100/1000 Ethernet card
Hancom xDB V2.8 PluginAgent	Linux	OS	CentOS 6.10 kernel 2.6.32 (64 bit)
		CPU	Xeon E3-1220 3.1 GHz or faster
		RAM	16 GB or more
		HDD	10 MB or more space required for TOE installation
		NIC	1 port or more of 10/100/1000 Ethernet card
	AIX	OS	AIX 5.3 64 bit
		CPU	PowerPC POWER64.2 GHz or faster
		RAM	16 GB or more
		HDD	10 MB or more space required for TOE installation
		NIC	1 port or more of 10/100/1000 Ethernet card
	HP-UX	OS	HP-UX 11.23 64 bit
		CPU	Intel Itanium(IA64) 1.4 GHz or faster
		RAM	16 GB or more
		HDD	10 MB or more space required for TOE installation
		NIC	1 port or more of 10/100/1000 Ethernet

			card

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator’s PC.

TOE	Division	Minimum Requirements
H/W	CPU	Intel ® Core™ i5-7500 3.4 GHz or faster
	Memory	4 GB or more
	HDD	1000 GB or more
	NIC	1 port or more of 10/100/1000 Ethernet card
S/W	OS	Windows 7 Professional SP1(x86/x64) Windows 10 Pro(x86/x64)
	Web Browser	Chrome 76.0

[Table 2] Hardware and software requirements for the TOE

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	Hanacom xDB V2.8 (Version: 2.8.2.3)	
TOE Component	Hancom xDB V2.8 Policy Server 2.8.2.3 (z_package.Hancom_xDB_V2.8_Policy_Server.2.8.2.3.tar.gz)	
	Hancom xDB V2.8 APIAgent2.8.2.3 (z_package.Hancom_xDB_V2.8_APIAgent.2.8.2.3.Linux.x86_64.64bit.tar.gz)	
	Hancom xDB V2.8 PluginAgent2.8.2.3 (z_package.Hancom_xDB_V2.8_PluginAgent.oracle.2.8.2.3.Linux.x86_64.64bit.tar.gz) (z_package.Hancom_xDB_V2.8_PluginAgent.oracle.2.8.2.3.AIX.5.3.tar.gz) (z_package.Hancom_xDB_V2.8_PluginAgent.oracle.2.8.2.3.HP-UX_IA.B.11.23.tar.gz)	
Manual	Preparative Procedure	Hancom xDB V2.8 Preparative Procedure (PRE) v1.9 (HancomxDB_V2.8_PreparativeProcedure(PRE)_v1.9.pdf)
	Operation Guide	Hancom xDB V2.8 Operation Guide (OPE) v1.8 (HancomxDBV2.8_OperationGuide(OPE)_v1.8.pdf)

[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 Scheme for IT Security (September 12 2017)

Protection Profile	Korean National Protection Profile for Database Encryption 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
Common Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017
EAL	EAL1+ (augmented by ATE_FUN.1)
Developer	Hancom With Inc.
Sponsor	Hancom With Inc.
Evaluation Facility	Korea Information Security Technology (KOIST)
Completion Date of Evaluation	October 29 2019
Certification Body	IT Security Certification Center (ITSCC)

[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:

1) Security Audit

The TOE creates and maintains audit records of auditable events such as the operation of security functions provided by the TOE and the history of security management.

2) Cryptographic Support

The TOE provides cryptographic key generation, distribution, destruction, and cryptographic operations to protect the transmitted data between TOE components and encrypt and decrypt user data. In addition, it provides a random number generation function for secure encryption key generation. The TOE uses the encryption target cryptographic algorithm of “XecureCrypto v2.0.1.1,” a validated cryptographic module whose security and implementation conformance are verified through the cryptographic module verification system (KCMVP) for the encryption of user data and TSF data to generate the encryption key.

3) User Data Protection

The TOE provides the function of encrypting and decrypting user data by column.

4) Identification & Authentication

To allow access to the security management functions provided by the TOE, the authorized administrator must be successfully identified and authenticated before allowing all actions related to the security functions

5) Security Management

The TOE provides the security management function for the authorized administrator to set up and manage the security policy and important data.

6) Protection of the TSF

When the TSF data is transmitted between the separated parts of the TOE using the cryptographic target algorithm of the validated cryptographic module “XecureCrypto v.2.0.1.1,” a validated cryptographic module whose safety and implementation conformity are verified through the cryptographic module verification system(KCMVP)

The TOE protects the passwords, encryption keys, critical security parameters, TOE configuration values (security policies, configuration parameters), and audit data of authorized administrators and DB encryption users stored in the TSF data repository from unauthorized exposures and modifications.

The TOE executes self-tests periodically at startup and during normal operation to verify the correct operation of the Policy Server, PluginAgent, and APIAgent.

7) TOE access

The TOE blocks the maximum number of concurrent sessions to 1 to disable concurrent login from the same account.

The TOE also blocks simultaneous access to the same authorization. The TOE terminates the session if there is no activity for 5 minutes after the authorized administrator logs in.

The TOE controls access to it so that only the registered IP (two default values or less) can access the security management interface.

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:

- Hancom xDB V2.8 Policy Server provides security features of identification and authentication of administrators, cryptographic key managements, and security management to the TOE and TSF data.
- Hancom xDB V2.8 APIAgent encrypt and decrypt the user data in a column of a database.
- Hancom xDB V2.8 PluginAgent encrypt and decrypt the user data in a column of a database.

Note that all the three 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 1.4.2.

6. Documentation

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

Idenfifier	Date
Hancom xDB_V2.8_Preparative Procedure(PRE)_v1.9.pdf	Sep. 25, 2019
Hancom xDB_V2.8_Operation guide(OPE)_v1.8.pdf	Sep. 25, 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 z 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 Hancom xDB V2.8 (version number V2.8.2.3). See table 3 for detailed information on the TOE components.

The TOE is installed from the CD-ROM distributed by Hancom With Inc. After installing the TOE, an administrator can identify the TOE version through 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	Requirements for evaluator actions	Verdict		
			Requirements for evaluator actions	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_OPE.1	AGD_OPE.1.1E	PASS	PASS	PASS
	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	
		AGD_PRE.1.2E	PASS		
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 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 administrator should install and operate the TOE and DBMS in a physically secure environment that is accessible only by the authorized administrator, and should not allow remote management from the outside.
- 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.
- 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 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 time information of each operating system where the TOE is installed should be synchronized to keep accurate time information.

11. Security Target

Hancom xDB V2.8 Security Target v1.10 [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
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 evaluation facility has used the following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

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] Hancom xDB V2.8 Evaluation Technical Report V1.10, October 29, 2019

[6] Hancom xDB V2.8 Security Target V1.10, October 21, 2019

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