KECS-CR-19-32

D'Amo v4.0

Certification Report

Certification No.: KECS-CISS-0939-2019

2019. 6. 25.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.06.25.	-	Certification report for D'Amo v4.0 - First documentation

This document is the certification report for D'Amo v4.0 of Penta Security System Inc.

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 **10**
3. Security Policy **11**
4. Assumptions and Clarification of Scope **11**
5. Architectural Information **12**
6. Documentation **122**
7. TOE Testing **133**
8. Evaluated Configuration **134**
9. Results of the Evaluation **144**
9.1 Security Target Evaluation (ASE) 144
9.2 Development Evaluation (ADV) 155
9.3 Guidance Documents Evaluation (AGD) 155
9.4 Life Cycle Support Evaluation (ALC) 16
9.5 Test Evaluation (ATE) 166
9.6 Vulnerability Assessment (AVA) 17
9.7 Evaluation Result Summary 17
10. Recommendations **188**
11. Security Target **19**
12. Acronyms and Glossary **19**
13. Bibliography **21**

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the D'Amo v4.0 developed by Penta Security Systems 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.

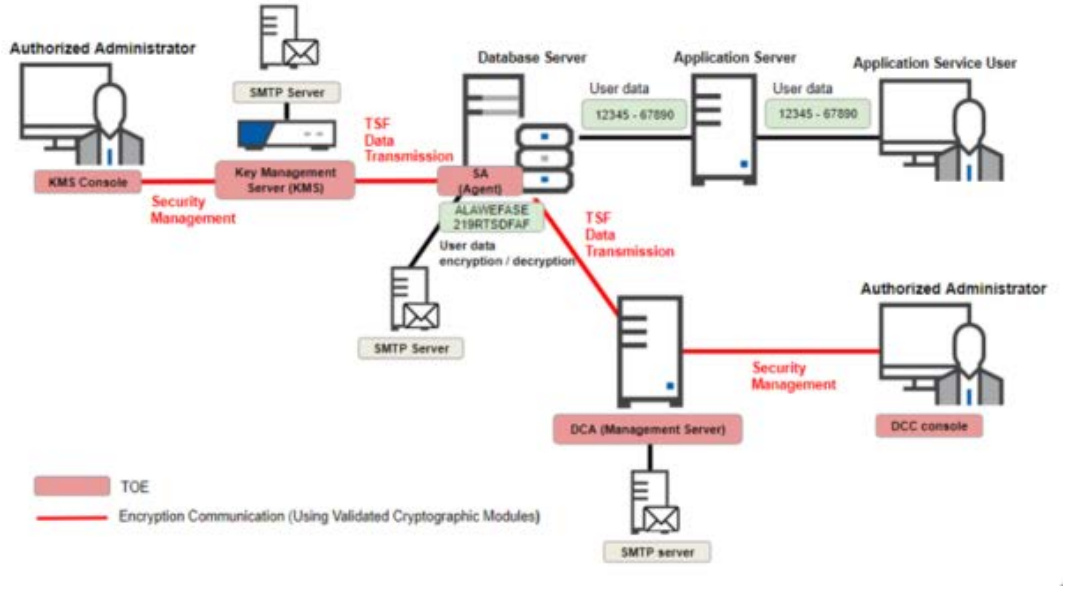
The Target of Evaluation ("TOE" hereinafter) is database encryption product to prevent unauthorized exposure of the information from DBMS. Also, the TOE shall provide a variety of security features: security audit, the user identification and authentication including mutual authentication between TOE 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 June 11, 2019. The ST claims conformance to the Korean National PP for Database Encryption V1.0[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 an agent (hereinafter 'SA'), management server (hereinafter 'DCA'), management console (hereinafter 'DCC console'), key management server (hereinafter 'KMS'), and key management server management console (hereinafter 'KMS console'). The Type of TOE is 'Plug-in' type.

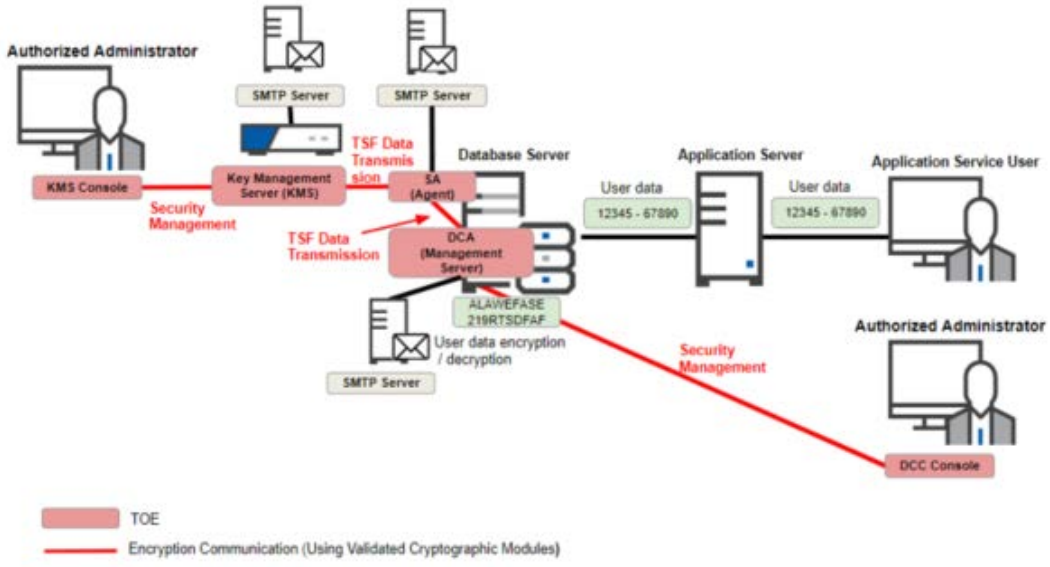
The operating environment of the TOE is divided into 'Agent and management server separated type' and 'Agent and management server integrated type' according to the installation location of management server and agent.

[Figure 1] represents the operating environment of 'agent and management server separated type'. This is installed together with SA in the protected DB, and DCA, DCC Console, and KMS are physically separated and installed.



[Figure 1] TOE operational environment : Agent and Management server separated type

[Figure 2] represents the operating environment of 'agent and management server integrated type'. This is installed SA and DCA together in the protected DB, and the DCC Console and KMS are physically separated and installed.



[Figure 2] TOE operation environment: Agent and management server integrated type

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

Type			Minimum requirements	Remarks
DCC Console	H/W	CPU	Intel Core i5 1.60 GHz or higher	
		RAM	4 GB or higher	
		HDD	20 GB or higher (space for TOE installation)	
		NIC	10/100/1000 Mbps x 1EA or higher	
	S/W	OS	- Windows 7 Pro 32bit - Windows Server 2008 R2 Enterprise 32bit - Windows 10 Pro K 32bit	Supported operation systems of the DCC Console
		3rd Party S/W	.NET Framework 4.6.1	Third-party software required to run DCC Console
DCA	H/W	CPU	- Intel Pentium CPU G4600 3.60 GHz or higher	

Type			Minimum requirements	Remarks
			- PowerPC_POWER3 450 MHz or higher	
		RAM	8 GB or higher	
		HDD	20 GB or higher (space for TOE installation)	
		NIC	10/100/1000 Mbps x 1EA or higher	
	S/W	OS	- Windows Server 2012 Standard 64bit - Windows Server 2008 R2 Enterprise 64bit - Windows 10 Pro K 64bit - CentOS release 6.10 (Linux Kernel 2.6, 64bit) - AIX 5.3 64bit	supported operating systems of DCA
SA	H/W	CPU	- Intel Pentium CPU G4600 3.60 GHz or higher - PowerPC_POWER3 450 MHz or higher	
		RAM	8 GB or higher	
		HDD	60 GB or higher (space for TOE installation)	
		NIC	10/100/1000 Mbps x 1EA or higher	
	S/W	OS	- Windows Server 2012 Standard 64bit - Windows Server 2008 R2 Enterprise 64bit - Windows 10 Pro K 64bit - CentOS release 6.10 (Kernel 2.6, 64bit) - AIX 5.3 64bit	supported operating systems of SA
		3rd Party S/W	- Oracle 10g Enterprise - Oracle 11g Enterprise - Oracle 12c Enterprise - SQL Server 2008 R2 Enterprise - SQL Server 2012 Enterprise	DB where SA is installed

Type			Minimum requirements	Remarks
			- SQL Server 2014 Enterprise	
KMS	H/W	CPU	Intel Pentium CPU G4600 3.60 GHz or higher	
		RAM	8 GB or higher	
		HDD	200 GB or higher (space for TOE installation)	
		NIC	10/100/1000 Mbps * 1 EA or higher	
	S/W	OS	Debian Linux OS 8.5 (Kernel 3.16)	Supported operating systems of KMS
		3rd Party S/W	MariaDB 10.0.25	Third-party software required to run KMS
KMS Console	H/W	CPU	Intel Core i5 1.60 GHz or higher	
		RAM	4 GB or higher	
		HDD	20 GB or higher (space for TOE installation)	
		NIC	10/100/1000 Mbps * 1 EA or higher	
	S/W	OS	Windows 10 Pro K 32bit	Supported operating systems of KMS Console
		3rd Party S/W	.NET Framework 4.5	Third-party software required to run KMS Console

[Table 1] Non-TOE Rrequired by the TOE

In addition, external IT entities linked to the TOE operation are as follows.

Mail Server: TOE interoperates with SMTP server when sending alarm mail

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	D'Amo v4.0
Version	D'Amo v4.0.10
TOE Components	D'Amo DP-ORA v4.0.4, D'Amo DP-MSQ v4.0.4 D'Amo DCA v4.0.6 D'Amo DCC Console v4.0.10 D'Amo KMS v4.0.10 D'Amo KMS Console v4.0.10
Guidelines	D'Amo_v4.0 Preparative Procedures, Operational Guide v1.8(DCC Console) D'Amo_v4.0 Preparative Procedures, Operational Guide v1.8(DP-MSQ) D'Amo_v4.0 Preparative Procedures, Operational Guide v1.8(DP-ORA) D'Amo_v4.0 Preparative Procedures, Operational Guide v1.8(KMS)

[Table 2] TOE identification

[Table 3] 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	D'Amo v4.0
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 V1.0 (August 18, 2017)
Developer	Penta Systems Inc.
Sponsor	Penta Systems Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	June 11, 2019

[Table 3] 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
- Protection of the TSF
- TOE Access

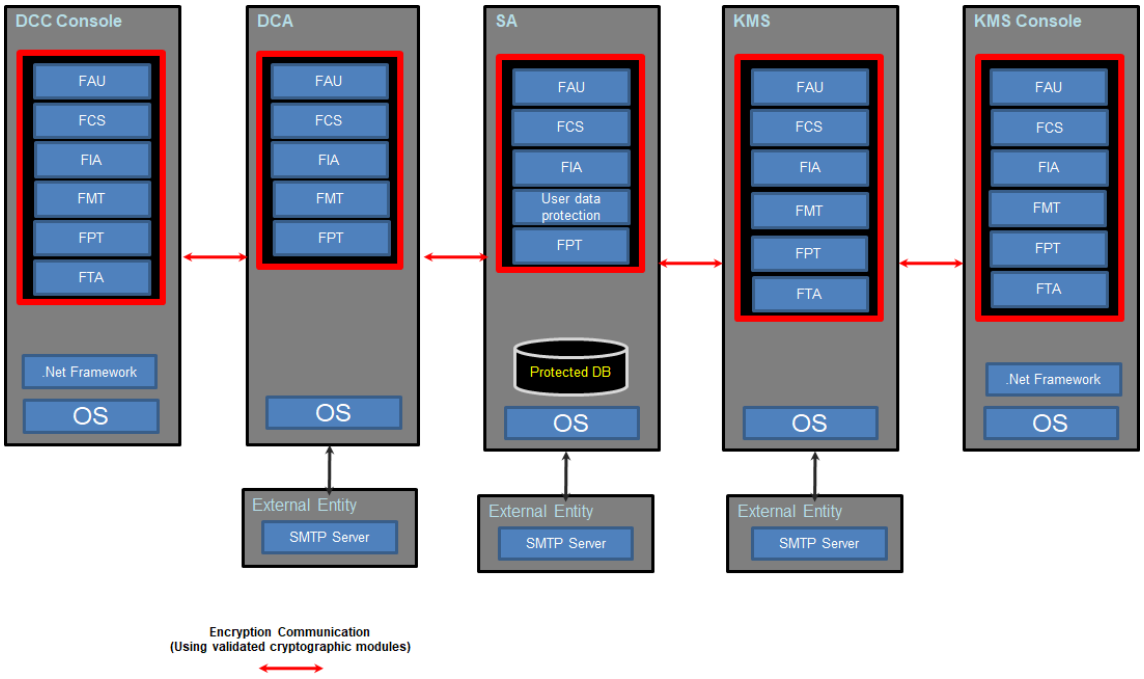
Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4]

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 2])

5. Architectural Information

TOE provides security functions such as security audit, cryptographic support, user data protection, identification and authentication, security management, TSF protection, and TOE Access as shown in [Figure 3].



[Figure 3] TOE Logical scope and boundary

6. Documentation

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

Identifier	Date
D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DCC Console).pdf D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DP-MSQ).pdf D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(DP-ORA).pdf D'Amo_v4.0_Preparative Procedures, Operational Guide_v1.8(KMS).pdf	May 09, 2018

[Table 4] 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: D'Amo v4.0
Version: D'Amo v4.0.10

- D'Amo DP-ORA v4.0.4, D'Amo DP-MSQ v4.0.4
- D'Amo DCA v4.0.6
- D'Amo DCC Console v4.0.10
- D'Amo KMS v4.0.10
- D'Amo KMS Console v4.0.10

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 7 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+).Security Target Evaluation (ASE).

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 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.

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 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 itself, the evaluation evidence required by the SARs, and the parts that comprise the TOE (required by the PP). Therefore, the verdict PASS is assigned to ALC_CMS.1.

The verdict PASS is assigned to the assurance class ALC.

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		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS

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

[Table 5] 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 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 prevent audit data loss.
- It is recommended the DBMS developer person who fully understands the preparation procedure and user operation manual install and operate the security function

11. Security Target

D'Amo v4.0 Security Target v1.11 [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

column

A set of data values of a particular simple type, one for each row of the table in a relational database

Database(DB)

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.

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

Database Management System(DBMS)

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.

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

DCC Console (D'Amo Control Center console)

The entity of the DCC subsystem, GUI-type console that provides security management function to authorized administrator

DCA (D'Amo Control Agent)

The process of passing the commands entered in the DCC Console to the SA, which can be executed in Windows, Linux, and Unix environments.

SA (Security Agent)

The component that executes the command that is input from the DCC Console.

KMS (Security Gateway - Key Management System)

As the key management server, it generates and manages KEK and DEK.

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, 2012

[3] Korean National Protection Profile for Database Encryption V1.0, August 18, 2017

[4] D'Amo v4.0 Security Target v1.11, June 11, 2019

[5] D'Amo v4.0 Independent Testing Report(ATE_IND.1) V2.00, June 11, 2019

[6] D'Amo v4.0 Penetration Testing Report (AVA_VAN.1) V1.00, May 14, 2019