KECS-CR-23-40

D'Amo v5.0

Certification Report

Certification No.: KECS-CISS-1246-2023

2023. 6. 15.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.06.15.	-	Certification report for D'Amo v5.0 - First documentation

This document is the certification report for D'Amo v5.0 of Penta Security Systems Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

The Korea Security Evaluation Laboratory (KSEL)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL1+ evaluation of D'Amo v5.0 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is database encryption software to prevent the unauthorized disclosure of confidential information by encrypting the database.

The TOE consists of D’Amo API Agent, D’Amo Plug-in Agent, D’Amo KMS, and the related guidance documents. The TOE includes a cryptographic module (CIS-CC V4.0) validated under the Korea Cryptographic Module Validation Program (KCMVP).

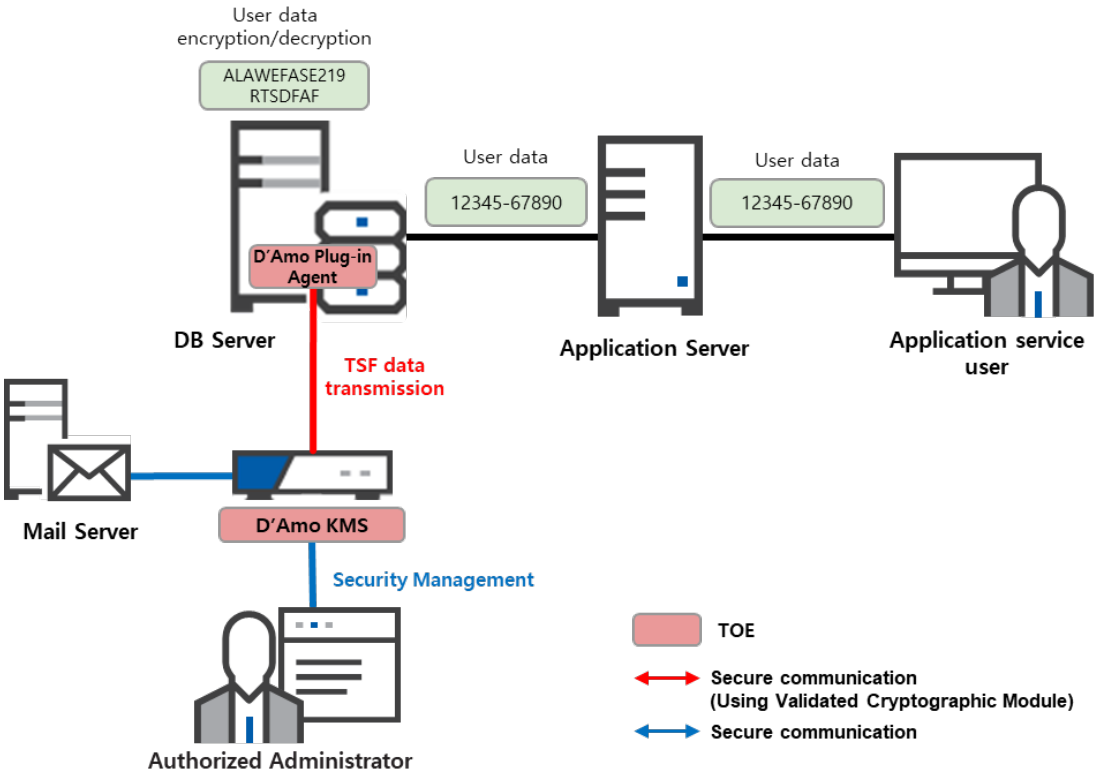
The TOE provides a variety of security features: security audit, cryptographic support, user data protection, identification and authentication including mutual authentication between TOE components, security management, protection of the TSF, and TOE access functions.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on May 23, 2023. This report grounds on the evaluation technical report (ETR) [3] KSEL had submitted and the Security Target (ST) [4].

The ST claims strict conformance to the Korean National Protection Profile for Database Encryption V1.1 (“PP” hereinafter) [5]. 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 augmented by ATE_FUN.1. 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 PP, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

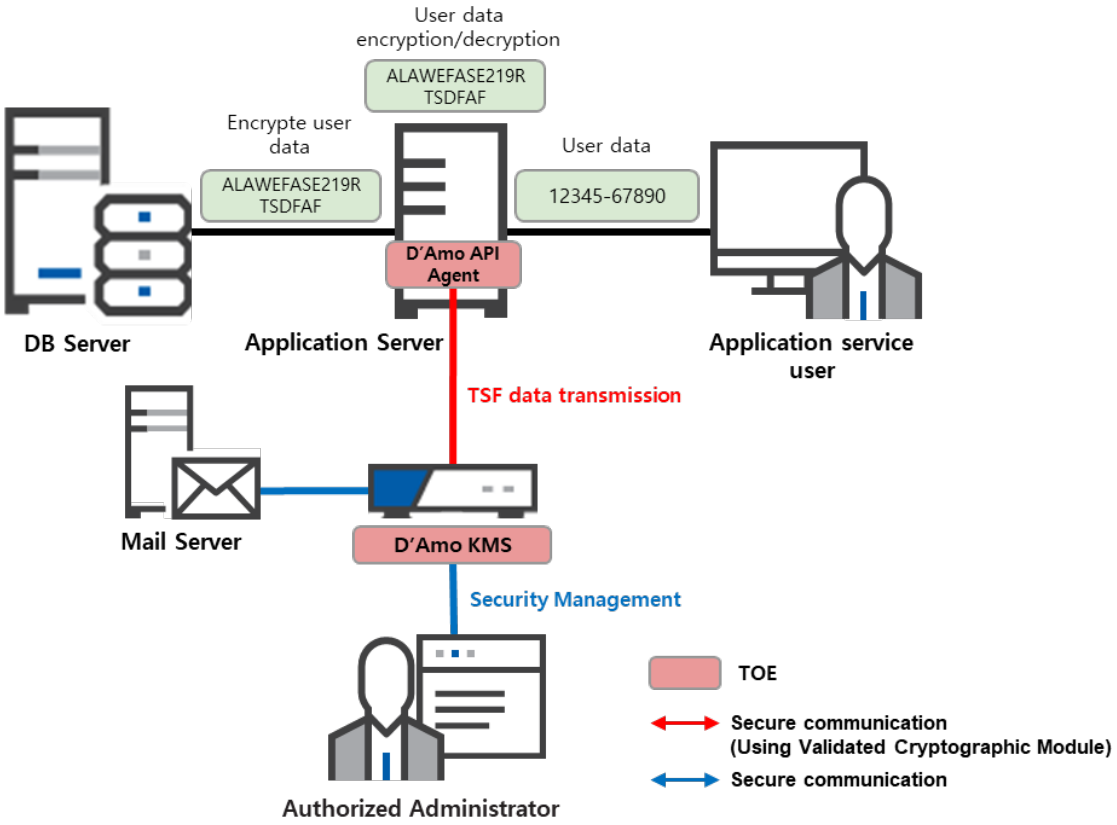
The TOE operational environment can be classified into plug-in type and API type.
[Figure 1] shows the operational environment of the plug-in type. The agent installed in the protected DB server encrypts the user data of the application server before storing it

in the DB according to the policy configured by the authorized administrator, and decrypts the encrypted user data before sending to the application server.



[Figure 1] TOE Operational Environment : Plug-in type (D'Amo Plug-in Agent, D'Amo KMS separate type)

[Figure 2] shows the operational environment of the API type. The application providing the application service, which is installed in the application server, is developed using the APIs provided by the D'Amo API Agent in order to use the cryptographic functions of the TOE. D'Amo API Agent 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'Amo API Agent, then sent to the database server. The encrypted user data received from the database server is decrypted by D'Amo API Agent, then sent to the application service user.



[Figure 2] TOE Operational Environment : API type (D'Amo API Agent, D'Amo KMS separate type)

The TOE implements secure communications between the TOE components to protect the transmitted data using the validated cryptographic module. The mail server that is an external IT entity of the TOE sends security alert mails to the authorized administrator.

The following tables show the hardware and software requirements necessary for installation and operation of the TOE.

Component		Specification
H/W	CPU	Intel-Pentium-Processor-G4600-3M-Cache-3.60 GHz or higher
	RAM	8 GB or higher
	HDD	50 GB or higher (Space required for TOE installation)
	NIC	10/100/1000 Mbps x 1EA or higher
S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-135)
	Java	java 1.8.0

[Table 1] Hardware and Software Requirements for D'Amo API Agent

Component		Specification
H/W	CPU	Intel-Pentium-Processor-G4600-3M-Cache-3.60 GHz or higher
	RAM	8 GB or higher
	HDD	50 GB or higher (Space required for TOE installation)
	NIC	10/100/1000 Mbps x 1EA or higher
S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-135) Oracle Linux 8.4 64bit (Kernel 5.4.17-2102.201.3.el8uek) Windows Server 2019 64bit
	DBMS	Tibero 6 * CUBRID 10.2 * Oracle 19.3 ** SQL Server 2019 Enterprise *** * Tibero and CUBRID are installed in Ubuntu. ** Oracle is installed in Oracle Linux *** SQL Server is installed in Windows Server
	Java	java 1.8.0

[Table 2] Hardware and Software Requirements for D'Amo Plug-in Agent

Component		Specification
H/W	CPU	Intel® Core™ I3-9100 Processor 3.6 GHz or higher
	RAM	16 GB or higher
	HDD	50 GB or higher (Space required for TOE installation)
	NIC	10/100/1000 Mbps x 1EA or higher
S/W	OS	Ubuntu 20.04 64bit (Kernel 5.4.0-144)
	Java	java 1.8.0
	DBMS	Postgresql 15.1
	3rd Party S/W	OpenSSL 1.1.1t Nginx 1.24.0 Node.js 18.12.1 libwrap0 7.6

[Table 3] Hardware and Software Requirements for D'Amo KMS

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 consists of D'Amo API Agent, D'Amo Plug-in Agent, D'Amo KMS, and the related guidance documents.

TOE	D'Amo v5.0	
Version	v5.0	
Detail version	v5.0.3	
TOE Components	D'Amo API Agent	D'Amo API Agent v5.0.2
	D'Amo Plug-in Agent	D'Amo Plug-in Agent for Tibero v5.0.2 D'Amo Plug-in Agent for CUBRID v5.0.2 D'Amo Plug-in Agent for Oracle v5.0.2 D'Amo Plug-in Agent for MSSQL v5.0.2
	D'Amo KMS	D'Amo KMS v5.0.3
Guidance Document	- D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo API Agent) - D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo Plug-in Agent) - D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo KMS)	

[Table 4] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (MSIT Notice No.2022-61, October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)

TOE	D'Amo v5.0
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	Penta Security System Inc.
Sponsor	Penta Security System Inc.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	May 23, 2023
Certification Body	IT Security Certification Center

[Table 5] Additional identification information

3. Security Policy

The TOE complies security policies pertaining to the following security functional requirements defined in the ST [4].

- Security Audit
- Cryptographic Support
- Identification and Authentication
- User Data Protection
- Protection of the TSF
- Security Management
- TOE Access

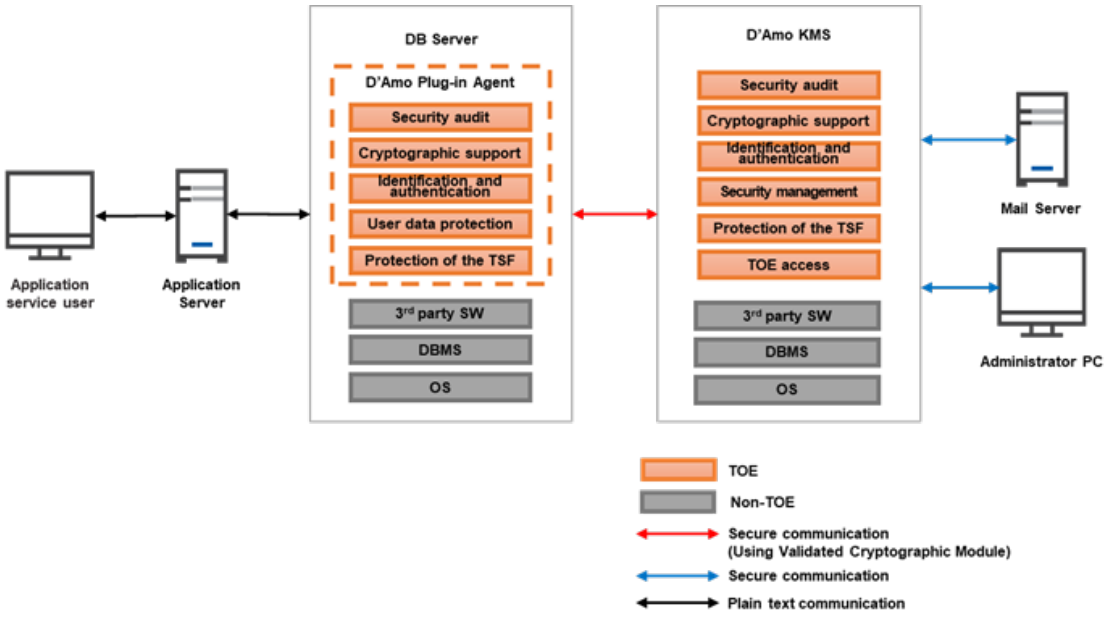
4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST [4]. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target.

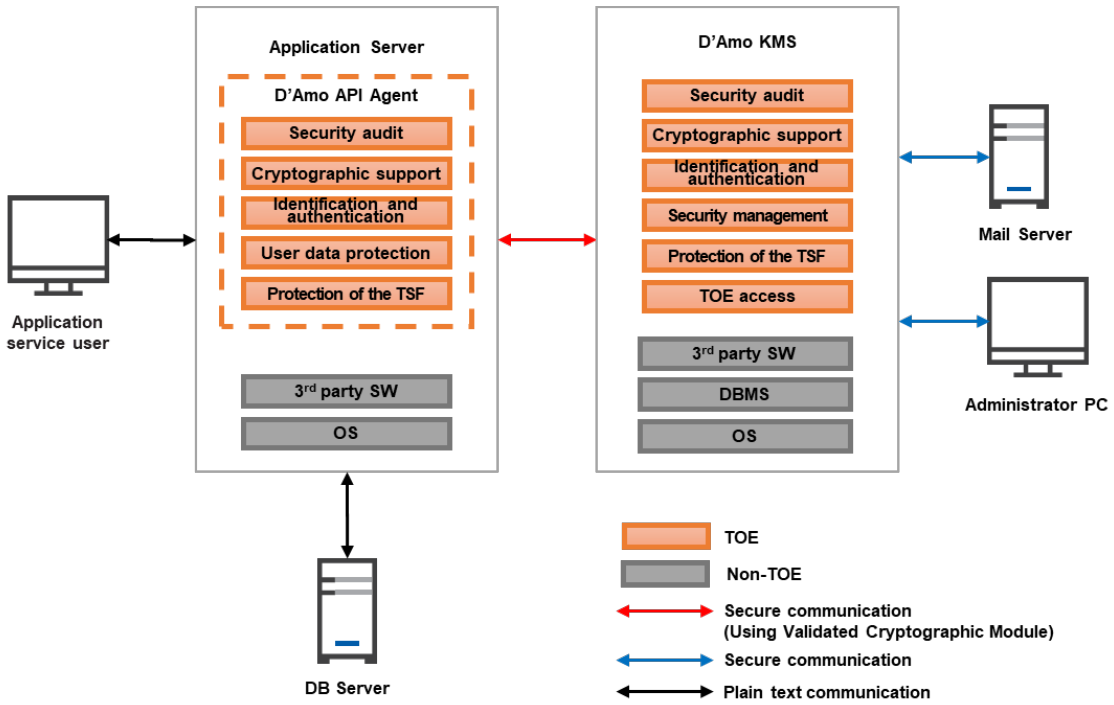
This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4]).

5. Architectural Information

TOE consists of the D'Amo API Agent, D'Amo Plug-in Agent, and D'Amo KMS. The TOE includes cryptographic modules (CIS-CC V4.0) validated under the KCMVP. [Figure 3] and [Figure 4] show the logical scope of the TOE.



[Figure 3] Logical scope of the TOE : Plug-in type (D'Amo Plug-in Agent, D'Amo KMS separate type)



[Figure 4] Logical scope of the TOE : API type (D'Amo API Agent, D'Amo KMS separate type)

6. Documentation

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

Identifier	Release	Date
D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo API Agent)	v1.1	May 4, 2023
D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo Plug-in Agent)	v1.1	May 4, 2023
D'Amo v5.0 Preparation procedure and user operation v1.1(D'Amo KMS)	v1.1	May 4, 2023

[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.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- 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 [3].

8. Evaluated Configuration

The TOE is D'Amo v5.0 (the version of the TOE is v5.0.3). See [Table 4] for detailed information on the TOE components. The TOE is installed from the CD-ROM distributed by Penta Security Systems Inc. The TOE is identified by TOE name and version number including release number. The TOE identification information is provided via GUI, API and Report.
And the guidance documents listed in this report chapter 6, [Table 6] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] 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 of EAL1+(ATE_FUN.1).

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 uniquely 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 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.

9.5 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, 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_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS

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 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 (D'Amo KMS) is implemented to provide a mechanism to prevent reuse of administrator's authentication information by using timestamp information during the administrator login process. Therefore, the administrator must set the time on the administrator's PC to match the Time on the server where D'Amo KMS installed before attempting to log in to D'Amo KMS for security management, and it should be noted that the login attempt is rejected if the timestamp value of the authentication information transmitted from the administrator's PC to D'Amo KMS is different by more than 3 seconds.
- The TOE is implemented to ignore audit data without saving it if the audit data storage is saturated. Therefore, when an authorized administrator receives an e-mail notification due to exceeding or saturation of the audit data storage

threshold, an audit log backup must be performed immediately to prevent audit data from being lost.

- The authorized administrator must ensure that the password used to generate the key encryption key (KEK) is different from the password used for administrator login, and must not use information that can be easily inferred by an attacker, such as personal information. To ensure the safety of the KEK, it is recommended to set and use the KEK at a level equivalent to the security strength of the administrator's password (set a rule combination of 3 or more of English letters/numbers/special characters and use 9 or more characters).
- The TOE purchaser can perform encryption/decryption of user data in the TOE operating environment (Application Server or Database Server) through additional development or modification using the D'Amo Agent. In this case, the TOE operating environment must be developed in compliance with the requirements provided by the TOE.
- SSL communication is implemented to perform secure communication between D'Amo KMS and mail server to send warning mails for security violation events. Authorized administrators should note that a public certificate must be used as the SSL certificate of the mail server that works with D'Amo KMS to send warning mails normally.

11. Security Target

The D'Amo v5.0 Security Target v1.2, May 4, 2023 [4] is included in this report by reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
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

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

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] D'Amo v5.0, Evaluation Technical Report V1.00, May 23, 2023

[4] D'Amo v5.0 Security Target v1.2, May 4, 2023

[5] Korean National Protection Profile for Database Encryption V1.1, December 11, 2019