KECS-CR-24-48

Magic SSO V4.5

Certification Report

Certification No.: KECS-CISS-1326-2024

2024. 08. 29.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.08.29.	-	Certification report for Magic SSO V4.5 - First documentation

This document is the certification report for Magic SSO V4.5 of Dream Security Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

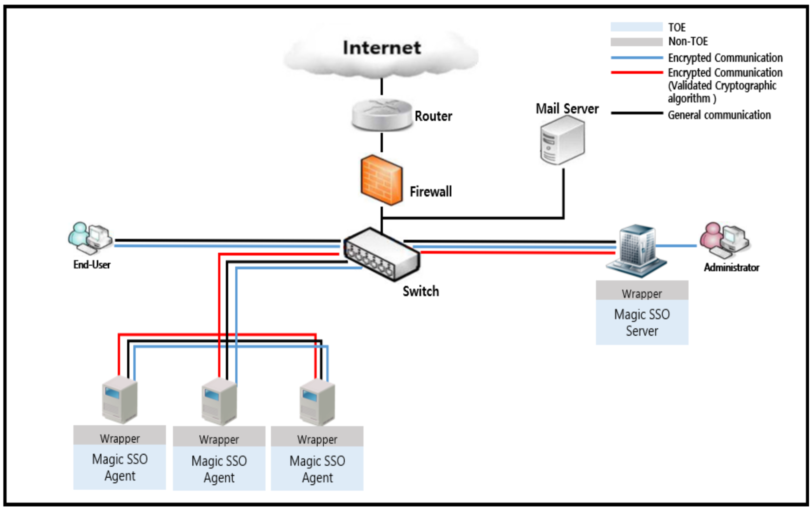
Korea System Assurance, Inc

Table of Contents

1. Executive Summary

This report describes the evaluation results drawn by the certification body on the results of the Magic SSO V4.5 developed by Dream Security Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter)[1]. It describes the evaluation results and its soundness and conformity.

The Target of Evaluation ("TOE" hereinafter) is used to enable the user to access various business systems and use the service through a single user login without additional login action. 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, Inc (KOSYAS) and completed on August 09, 2024. The ST claims conformance to the Korean National Protection Profile for Single Sign On V3.0[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 an 'integrated authentication' solution which allows an end-user to access to various business systems with a single log-in. The TOE provides the ID/PW based user log-in function and issues an authentication token when a user initially attempts to log in. The TOE issues a token during user log-in, and verify the issued token if accessing another business system after user log-in. The TOE provides the security audit function that records and manages critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and TSF protection function such as TSF self-testing. In addition, the TOE provides authentication failure handling, identification and authentication functions including mutual authentication between the TOE components, cryptographic support function such as cryptographic key management and cryptographic operation for issuing a token, security management function for management of security functions behaviour and configuration, and the TOE access function to manage the authorized administrator's interacting session. In addition, the token requires confidentiality and integrity protection, and the TOE executable file and configuration file requires integrity protection. [Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

The operational environment of the TOE is composed of the SSO server that is installed in the management server and the SSO Agent that is installed in the business system. The TOE is provided in software. The SSO Server is mounted on Web Application Server and operates as a single web application. The SSO Agent is installed in each business system web application server in the form of library file API. Wrapper is used for compatibility with various business systems and Wrapper is excluded from the scope of the TOE. The SSO Server performs the security management of the TOE via web browser which supports The confidentiality and integrity of data transmitted for communication between the web browser of the Administrator PC and the web server, which is the operating environment of the management server, must be guaranteed. The SSO server and Oracle, a relational database management system, are interlinked for the purpose of the management of authentication and policy information. A mail server is used as an external entity necessary for the operation of the TOE. The mail server is utilized to notify an authorized administrator via email in case of failed administrator authentication or possible audit data loss.

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

Component			Requirement
SSO Server	HW	CPU	Intel Dual Core 2 GHz or higher
		Memory	8 GB or more
		HDD	Space required for installation of TOE : 100 GB or more
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Ubuntu 20.04 (Kernel 5.15.0) 64 bit
		Java	OpenJDK 1.8.0_412
		WAS	Apache Tomcat 9.0.91
		DBMS	Oracle 11g(11.2.0.2.0)
SSO Agent	HW	CPU	Intel Dual Core 2 GHz or higher
		Memory	8 GB or more
		HDD	Space required for installation of TOE : 100 GB or more
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Ubuntu 20.04 (Kernel 5.15.0) 64 bit
		Java	OpenJDK 1.8.0_412
		WAS	Apache Tomcat 9.0.91

[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]

Component		Requirement
S/W	Web Browser	Chrome 126.0

[Table 2] Administrator PC Requirements

In addition, the external IT entities linked for TOE operation are shown in [Table 3]

Component	Requirement
Mail Server	Sends an e-mail about potential security violations to the authorized administrator on the designated receiving side from the SSO server.

[Table 3] External Entity

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	Magic SSO V4.5
Version	v4.5.0.1
TOE Components	Magic SSO V4.5 Server v4.5.0.1 Magic SSO V4.5 Agent v4.5.0.1
Guideline	Magic SSO V4.5 Operational Guidance v1.3 Magic SSO V4.5 Installation Guide v1.3

[Table 4] TOE identification

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guideline (Ministry of Science and ICT Guidance No. 2022-61, October 31, 2022) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	Magic SSO V4.5
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 Single Sign On V3.0
Developer	Dream Security Co., Ltd.
Sponsor	Dream Security Co., Ltd.
Evaluation Facility	Korea System Assurance, Inc (KOSYAS)
Completion Date of Evaluation	August 09, 2024

[Table 5] Additional identification information

3. Security Policy

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

- Security Audit
- Cryptographic Support
- 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 4])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the SSO Server, the SSO Agent, an operational guidance and an installation guide. Verified Cryptographic Module (MagicJCrypto V3.0.0) is embedded in the TOE components.

Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE.

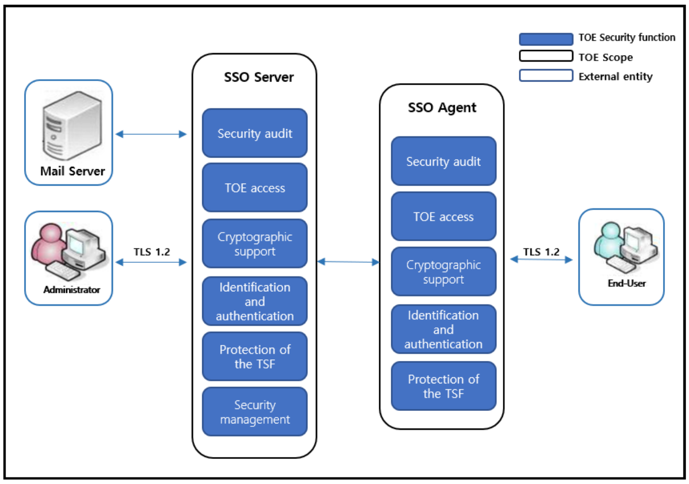
Category		Identification	Type
TOE	SSO	Magic SSO V4.5 Server v4.5.0.1	Software

components	Server	: magicsso-server-4.5.0.1.tar	(Distributed as a CD)
	SSO Agent	Magic SSO V4.5 Agent v4.5.0.1 : magicsso-agent-4.5.0.1.tar	
Guideline		Magic SSO V4.5 Operational Guidance v1.3 : Magic_SSO_V4.5-OPE-v1.3.pdf	PDF (Distributed as a CD)
		Magic SSO V4.5 Installation Guide v1.3 : Magic_SSO_V4.5-PRE-v1.3.pdf	

[Table 6] Physical scope of the TOE

2. Logical Scope of TOE

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



[Figure 2] Logical scope of the TOE

[Security Audit]

The SSO server generates audit data on security-relevant events in order to trace the responsibility for behaviors related to the security. Audit data generated by the SSO server record the date and time of an event, the type of an event, subject identity and an outcome (success or failure) of an event. All the audit data are stored in DBMS. An authorized administrator can review the audit data through the administrator screen and can search the audit data according to the date and time of an event, the type of an event and an outcome of an event. In addition to the super administrator, monitoring administrators authorized for audit viewing can view the audit data. In case the audit data storage reaches a certain threshold defined by the administrator, a warning email will be sent to the administrator. Also, in case the audit storage is full, audited events are ignored and a warning message is sent to the administrator via email. In addition, the following potential violations are analyzed, and a warning message is sent to the administrator via email.

The SSO agent generates audit data on security-relevant events in order to trace the responsibility for behaviors related to the security. Audit data generated by the SSO server record the date and time of an event, the type of an event, subject identity and an outcome (success or failure) of an event. All the audit data are transmitted to the SSO server.

[Cryptogrphic Support]

The TOE manages the security functions for generation, distribution and destruction of cryptographic key necessary for cryptographic operation, cryptographic operation and random number generation. For an algorithm applied here, MagicJCrypto V3.0.0, which is a validated cryptographic module, is used.

- Cryptographic key generation :
  - HASH_DRBG(SHA256, 256bit) : Symmetric key generation for Authentication Infomation and Authentication Token encryption/decryption
  - RSAES(2048bit) : Asymmetric key generate for data encryption/decryption
- Symmetric key operation(SEED-CBC, 128bit) : Cryptographic operation for Authentication Infomation and Authentication Token encryption/decryption
- Asymmetric key operation(RSAES, 2048bit) : Encrypt and distribute with public key when sending encryption key of authentication information
- Digital signature generation and verification (RSA-PSS, 2048bit) : Generation and verification of digital signature of authentication information
- HMAC(HMAC-SHA256) : Generation and verification of setting and module integrity data
- HASH(SHA-256) : HASH of administrator/end-user password

[Identification and authentication]

The TOE provides the function to identification and authentication the administrator who wants to use the security management function before every action and to protect the authentication feedback when entering the authentication data. In case administrator authentication attempts fail consecutively for a specified number of times defined by an administrator (default value: 5 times), the authentication function becomes inactivated and access is denied for a specified period of time for authentication delay defined by an administrator (default value: 5 minutes). It also blocks attempts to reuse authentication information for administrator logging in to TOE. An administrator password shall be generated in accordance with the password rules. Once identification and authentication are completed, the administrator can manage the security functions.

The TOE identification and authentication to SSO Agent for end-user to use single sign on function. It provides a function to protect authentication feedback when entering authentication data and provides secure identification and authentication function according to authentication lock processing function in case of consecutive authentication failure. It also blocks attempts to reuse authentication information for end-users logging in to SSO Agent.

When generating the authentication token used by the TOE, the authentication token is generated using the one-time authentication data (using the time stamp) through validated cryptographic module, the authentication token is overwritten with data 0x30 when the authentication token is destroyed.

TOE internal mutual authentication is performed through the protocol implemented by Dreamsecurity Co., Ltd.

[Security Management]

The SSO server provides the function that enables an authorized administrator to manage security roles, policies, end user information and audit information through the security management interface.

An authorized administrator can change an administrator’s or an end user’s password through the security management interface and verifies the validity of the password values in accordance with the password policy when creating or changing an end user’s or an authorized administrator’s password.

When an authorized administrator accesses the security management interface for the first time, it shall be enforced that the administrator changes the password. An audit administrator shall change the password upon access after the password is reset by an authorized administrator.

- Security Role Management: The function of the administrator role management is provided. The administrator role is classified into super administrator and monitoring administrator. A super administrator is authorized for policy management, end user information management and audit information management while a monitoring administrator is authorized for the monitoring of the TOE and audit information viewing.
- Security Policy Management: The function of the authentication policy management is provided. It performs the setting of the password validity and prevention of duplicated logins, and the establishment of end user authentication policies to define a session inactivity period. It establishes a threshold of the audit storage capacity and the audit information regarding the verification interval of the module implemented by Dreamsecurity Co., Ltd. It sets up mail information including mail server address and mail alarm information.
- End User Information Management: It provides the function of handling unlocking of an end user account that has been locked.
- Audit Information Management: It provides the function of viewing audit information based on a search period, types of audit events and outcomes.

[Protection of the TSF]

The TOE offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the cryptographic module.

For the protection of the TSF data, the information on end user/administrator’s authentication, TOE integrity verification, SSO server and SSO agent and so forth is encrypted, stored and managed in the DBMS. Authentication tokens are loaded in SSO server sessions in an end user’s browser and are destroyed immediately after the use.

The SSO server runs self tests during the initial start-up and periodically during normal operation to check the process status in order to ensure that it is in a safe condition and the security function works normally. It also performs integrity monitoring of TSF data and TSF executable files subject to the integrity verification.

[TOE Access]

The maximum number of concurrent sessions of management access by an administrator that belong to the same administrator is limited to one. The TOE blocks new access if an administrator makes management access in one terminal and then tries to log in with the same account or the same privilege in a different terminal. An access session by an administrator/end user is terminated after a specified time period of end user inactivity (default value: 10 minutes). As to management access by an administrator, any access by IPs, other than access IPs configurable by an administrator (default value: 2 IPs), is denied.

6. Documentation

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

Identification	Date
Magic SSO V4.5 Operational Guidance v1.3 : Magic_SSO_V4.5-OPE-v1.3.pdf	July 19, 2024
Magic SSO V4.5 Installation Guide v1.3 : Magic_SSO_V4.5-PRE-v1.3.pdf	July 19, 2024

[Table 7] 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.: 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 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: Magic SSO V4.5 (v4.5.0.1)

- Magic SSO V4.5 Server v4.5.0.1
- Magic SSO V4.5 Agent v4.5.0.1

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

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 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 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 Results 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	

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

[Table 8] 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 check 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.

- 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

Magic SSO V4.5 Security Target v1.3 [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 Programming Interface (API)

A set of system libraries existing between the application layer and the platform system, enables the easy development of the application running on the platform

Authentication Data
Information used to verify a user's claimed identity

Authentication token
Authentication data that authorized end-users use to access the business system

Authorized Administrator
Authorized user to securely operate and manage the TOE

Authorized User
The TOE user who may, in accordance with the SFRs, perform an operation

Business System
An application server that authorized end-users access through ‘SSO’

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

end-user
Users of the TOE who want to use the business system, not the administrators of the TOE

External Entity
An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.

Monitoring administrator
As An authorized user who operates and manages the TOE securely, Only the audit log can be viewed among the security management functions

Super Administrator
As an authorized user who operates and manages the TOE securely, it can perform all security management functions

Validated Cryptographic Module
A cryptographic module that is validated and given a validation number by validation authority

Wrapper

Interfaces for interconnection between the TOE and various types of business systems or authentication systems

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 Single Sign On V3.0, April 27, 2023

[4] Magic SSO V4.5 Security Target v1.3, July 19, 2024

[5] Magic SSO V4.5 Independent Testing Report(ATE_IND.1) V2.00, August 27, 2024

[6] Magic SSO V4.5 Penetration Testing Report (AVA_VAN.1) V2.00, August 27, 2024