KECS-CR-25-29

eXSignOn V4.0

Certification Report

Certification No.: KECS-CISS-1366-2024

2025. 9. 12.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025.9.12.	-	Certification report for eXSignOn V4.0 - First documentation

This document is the certification report for eXSignOn V4.0 of Tomato System co,. LTD.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

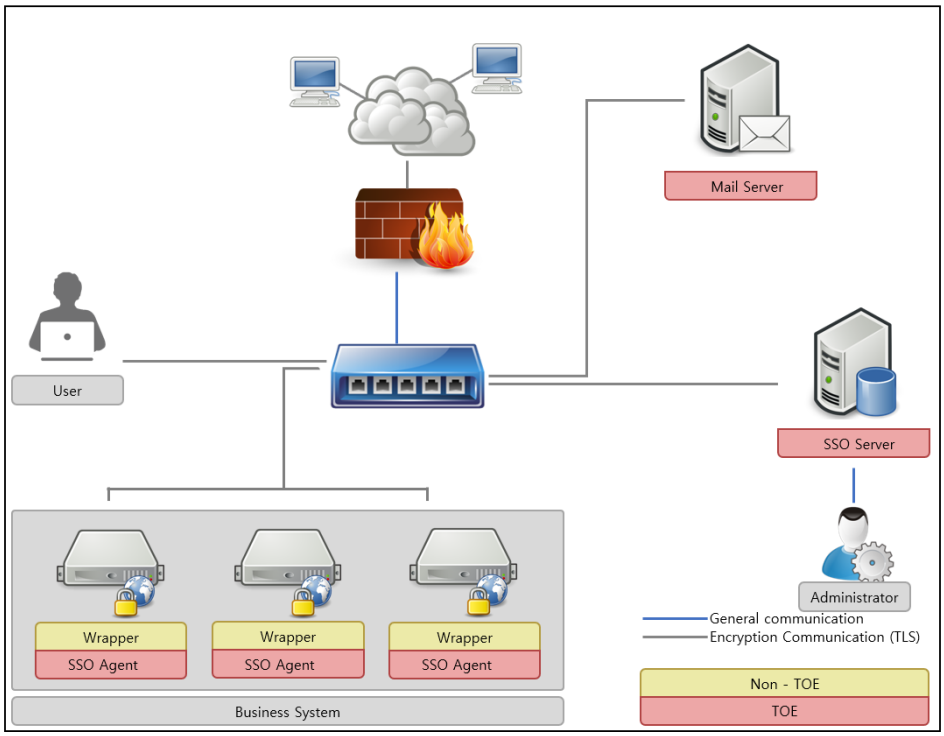
1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the eXSignOn V4.0 developed by Tomato System Co,. LTD. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.
The Target of Evaluation (“TOE” hereinafter) is 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 (KOSYAS) and completed on August 27, 2025. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [7] and the Security Target (ST) [4].
The ST claims conformance to the Korean National Protection Profile for Single Sign On V3.1[3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1+. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

The TOE is 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 behavior 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 Core i5 2.5GHz or higher
		Memory	16 GB or more
		HDD	Space required for installation of TOE : 50 GB or more
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	Windows Server 2022 (64bit)
		Java	OpenJDK 11.0.28 (64bit)
		WAS	Apache Tomcat 10.1.43 (64bit)
		DBMS	MariaDB 11.8.2 (64bit)
SSO Agent	HW	CPU	Intel Core i5 2.5GHz or higher
		Memory	8 GB or more
		HDD	Space required for installation of TOE : 10 GB or more
		NIC	Ethernet 100/1000 Mbps * 1 Port or more
	SW	OS	WindowsServer2019 (64bit), RHEL 9.0 (Linux 5.14.0) (64bit)
		Java	OpenJDK 11.0.28 (64bit)
		WAS	Apache Tomcat 10.1.43 (64bit)

[Table 1] TOE Hardware and Software specifications

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

Classification		Minimum Requirement
SW	Web Browser	Chrome 139.0

[Table 2] Administrator PC Requrements.

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	eXSignOn V4.0
Version	V4.0.005
TOE Components	eXSignOn Sever V4.0.005 eXSignOn Agent V4.0.005
Manuals	eXSignOn V4.0 operational guidance V1.8 eXSignOn V4.0 preparation procedure V1.8

[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	eXSignOn V4.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-07-002 Version 1.1, July 2024
Common Evaluation Methodology	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-07-002 Version 1.1, July 2024
EAL	EAL1+(ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign On V3.1
Developer	Tomato System Co., LTD.
Sponsor	Tomato System Co., LTD.
Evaluation Facility	Korea System Assurance, Inc. (KOSYAS)
Completion Date of Evaluation	August 27, 2025

[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
- Prtoection of the TSF
- TOE Access
- Trusted Path/Channels

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

4. Assumptions and Clarification of Scope

It is assumed that the following conditions exist in the TOE operational environment.

A.PHYSICAL_PROTECTION
The place where SSO agent and SSO server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.

A.TRUSTED_ADMIN
The authorized administrator of the TOE is non-malicious, has been appropriately trained for the TOE management functions, and accurately fulfills their duties in accordance with administrator guidelines.

A.OPERATION_SYSTEM_REINFORCEMENT
The reliability and security of the operating system shall be ensured by reinforcing the latest vulnerabilities in the operating system on which the TOE is installed and operated.

A.SECURE_DEVELOPMENT
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.

A.SECURE_DBMS
Audit records, including audit trail stored in the DBMS and other components interacting with the TOE, must be protected against unauthorized deletion or modification.

A.TRUSTED_TIMESTAMP
The TOE must use a trusted timestamp provided by the TOE's operational environment to accurately record security-related events.

A.MANUAL_RECOVERY
The TOE must support manual recovery procedures, such as user-involved reinstallation, to restore tampered information after the TOE agent experiences a failure or service disruption.

A.SECURE_ADMIN_ACCESS
The TOE shall use a secure channel (SSL) to ensure the confidentiality and integrity of communications between the administrator's PC web browser and the user web server.

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 (eXCryptoLib V1.0) 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	eXSignOn V4.0	-
TOE Detailed Version	V4.0.005	-

TOE components	SSO Server	eXSignOn Server V4.0.005 (TMTEXS_SERVER_V4.0.005.zip)	Software file (Distributed as a CD)
	SSO Agent	eXSignOn Agent V4.0.005 (TMTEXS_AGENT_V4.0.005.zip)	
Manuals		eXSignOn V4.0 operational guidance V1.8 (TMTEXS_OPE_V1.8.pdf)	PDF file (Distributed as a CD)
		eXSignOn V4.0 preparation procedure V1.8 (TMTEXS_PRE_V1.8.pdf)	

[Table 4] Physical scope of the TOE

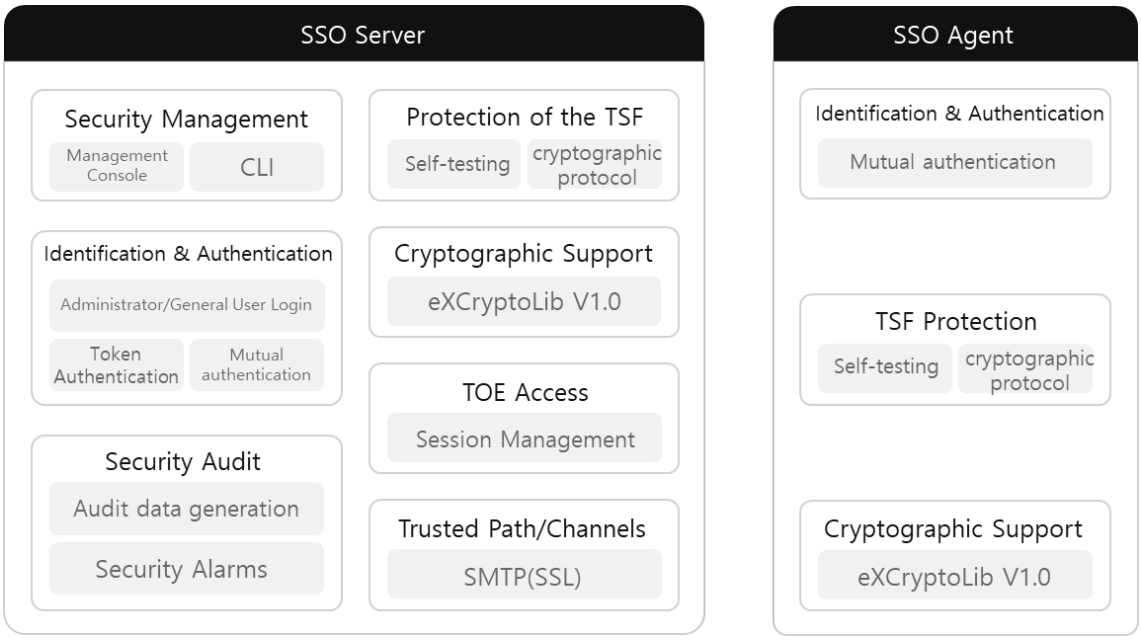
Validated cryptographic modules included the TOE are as follows in [Table 6].

category	content
Cryptographic Module Name	eXcryptoLib V1.0
Verification number	CM-268-2030.4
Verification Grade	VSL1
Developer	Tomato System
Verification date	April, 16, 2025

[Table 5] General Verification Cryptographic Module

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 1] TOE Logical scope

▣ Security Audit

The TOE provides functions for generating audit records of security-related events and detecting potential violations to track accountability for security-related actions. Audit records for all operations performed by users over time are stored, and the generated audit records are stored in the DBMS through the SSO server.

When the SSO server's disk capacity is saturated, an alert mail is sent to the authorized administrator in response to the loss of audit data, and a warning mail is sent to the authorized administrator in order to prevent the loss of audit data. If the loss prediction standard is exceeded, a saturation warning mail is sent, and if the saturation standard is exceeded, a saturation warning mail is sent.

▣ Cryptographic support

The TOE uses validated cryptographic algorithms within the validated cryptographic module (eXCryptoLib V1.0, CM-268-2030.4), whose security and implementation compliance have been confirmed through the Korea Cryptographic Module Validation

Program (KCMVP), to manage encryption keys, perform encryption operations, and generate random bits for SSO server–SSO agent communication.

Additionally, to protect transmitted data and stored TSF data (e.g., SSO server configuration files, SSO server preferences stored in DB and files, files that store DEK/IV/TSF data integrity verification keys (HMACs), and files that store DBMS access information), it uses ARIA/CCM (128-bit) mode to ensure both confidentiality and integrity. It also performs functions such as the issuance, verification, storage, and disposal of authentication tokens, as well as the use of random bit generators for cryptographic key management (e.g., key generation)

▣ Identification and authentication

The TOE performs secure encrypted communication between its components (SSO server and SSO agent) by implementing its own mutual authentication protocol. During mutual authentication, the following cryptographic algorithms are used:

- Generation of mutual authentication session keys and encrypted communication session keys: Hash_DRBG (random bit generator)

- Distribution (encryption/decryption) of session keys: RSAES (2048-bit)

- Authentication / encryption and decryption: ARIA/CCM (128-bit)

- SSO server identification information: SSO server domain

- SSO agent identification information: SSO agent domain and SPID

In addition, the SSO server performs user identification and authentication based on ID and password for both administrators and users, and user identification and authentication are required before any action is permitted. The password input field is masked with asterisks (*) to prevent it from being shown during input. Passwords must comply with the password policy defined by an authorized administrator. The TOE verifies the password used during an authentication attempt, does not provide feedback on failed authentication results, and prevents the reuse of authentication data.

To protect the TOE from improper authentication attempts, if the number of failed identification and authentication attempts exceeds the configured limit (default: 5 attempts, configurable from 1 to 5 attempts), the SSO server locks the account for the configured period of time (default: 5 minutes, configurable to 5/10/30/60 minutes).

Locked accounts are automatically unlocked after the configured time period has elapsed.

Authentication tokens used for user identification and authentication are generated using fixed values, the user ID, a timestamp, and random numbers produced by a random bit generator. To provide both confidentiality and integrity of the sensitive information contained in the token, the TOE uses a validated cryptographic module applying ARIA/CCM (128-bit) mode for token encryption. Upon logout, the contents of the authentication token are securely deleted from memory using a triple overwrite method with the value '0x00'.

▣ Security Management

The SSO server can manage security functions and TSF data through a administrator web interface. The security management functions provided by the SSO server are as follows:

1. Security function management: Administrators can manage TSF functions. The TOE provides security policy management and monitoring, as well as audit data review functions.
2. Data management: The TOE manages TSF data. TSF data enables functions for managing security policies and viewing audit data.
3. Password management: Provides authorized administrators with functions to manage password length and combination rules, and enforces the change of default administrator passwords for new administrators upon first login.
4. Security role management: Authorized administrators of the TOE are classified as super administrators, general administrators, and monitoring administrators. Super administrators can manage all security functions of the TOE and add, delete, and grant privileges to general administrators, while general administrators can access some security functions or monitoring features as configured by the super administrator. Monitoring administrators can only monitor audit data. Only one administrator with modification privileges for security functions (excluding monitoring administrators) can be logged in at the same time to prevent simultaneous modifications to security functions.

▣ Protection of the TSF

If a failure occurs in the entropy source (e.g., noise source health test failure), the TOE transitions to a critical error state and halts the operation of the validated cryptographic module to maintain a secure state. After mutual authentication between TOE components (SSO server and SSO agent) using its own protocol, the SSO server uses the distributed session key to perform encrypted communication with ARIA/CCM (128-bit), ensuring the confidentiality and integrity of transmitted TSF data. The SSO server also performs TSF self-tests, including integrity tests using the HMAC-SHA256 algorithm for libraries, configuration files, and cryptographic modules. TSF self-tests are performed during initial start-up, every 12 hours after start-up, and upon administrator request. If the TSF self-test fails, the SSO server notifies the authorized administrator of the failure details via email in order to provide TSF protection.

▣ TOE access

The SSO server limits the maximum number of concurrent administrators with privileges to change settings (super administrators and general administrators) to one. If another administrator logs in while an existing administrator is connected, the existing administrator's session is terminated. However, administrators with only monitoring privileges can log in concurrently. Administrator sessions are restrictively accessible to authorized personnel based on IP addresses. User sessions are restrictively accessible based on IP address, SSO agent ID, and SSO agent domain. If a user or administrator does not perform any activity for the configured session timeout period (default: 600 seconds, configurable from 60 to 600 seconds) after login, the session is terminated.

▣ Trusted Path/Channels

When the TOE communicates with external IT entities such as an Mail server(SMTP server), it provides a secure communication path/channel to protect transmitted data by using TLS v1.3 with the TLS_AES_256_GCM_SHA384 cipher suite and the ECDHE key exchange algorithm.

6. Documentation

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

Identification	Date
eXSignOn V4.0 operational guidance V1.8 (TMTEXS_OPE_V1.8.pdf)	August 6, 2025
eXSignOn V4.0 preparation procedure V1.8 (TMTEXS_PRE_V1.8.pdf)	August 6, 2025

[Table 6] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [5], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: 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: eXSignOn V4.0 (V4.0.005)
- eXSignOn Sever V4.0.005
- eXSignOn Agent V4.0.005

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 Problem Definition clearly defines the security problems that the TOE and operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.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 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_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 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 prvent audit data loss.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

11. Security Target

eXSignOn V4.0 Security Target V1.7 [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 V3.1, June 27, 2025

[4] eXSignOn V4.0 Security Target V1.7, June 6, 2025

[5] eXSignOn V4.0 Independent Testing Report(ATE_IND.1) V1.00, August 26, 2025

[6] eXSignOn V4.0 Penetration Testing Report (AVA_VAN.1) V1.00, August 26, 2025

[7] eXSignOn V4.0 Evaluation Technical Report V2.00, September 11, 2025