KECS-CR-26-13

Rathon-SSO v4.0

Certification Report

Certification No.: KECS-CISS-1395-2026

2026. 4. 3.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2026.4.3.	-	Certification report for Rathon-SSO v4.0 - First documentation

This document is the certification report for Rathon-SSO v4.0 of RathonTech 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 Rathon-SSO v4.0 developed by RathonTech 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 provides 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 March 24, 2026. 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 PP 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.

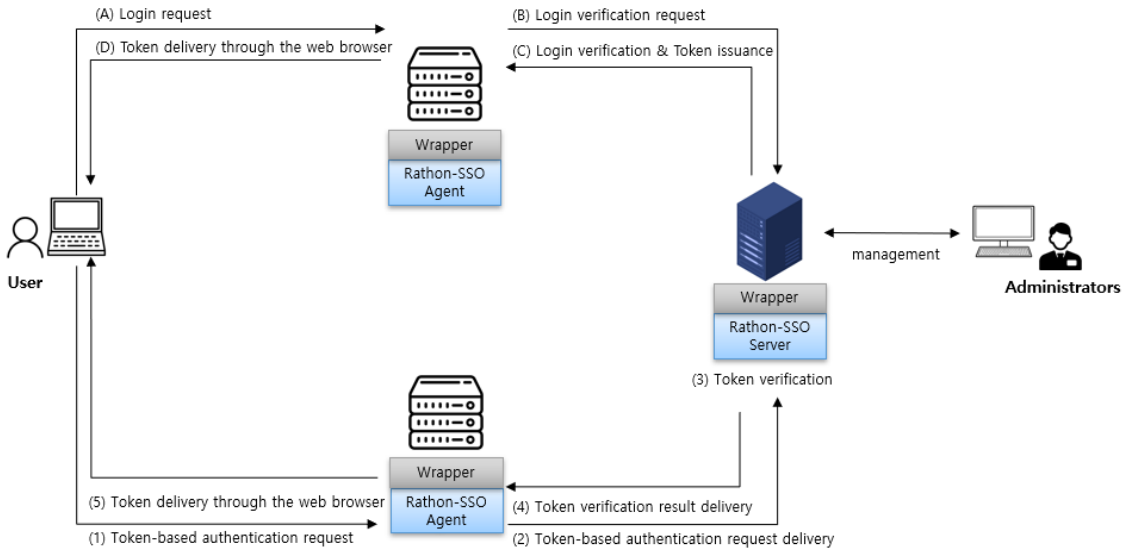
The TOE components are provided in the form of software. The TOE components consist of the Rathon-SSO Agent (hereinafter referred to as the ‘SSO agent’) and the Rathon-SSO Server (hereinafter referred to as the ‘SSO server’). The TOE is composed of a server that performs functions such as user login processing, authentication token management, and policy configuration, and an agent that is installed in each business system to perform functions such as authentication token issuance and authentication token verification requests.
In addition, the agent is provided in the form of an ‘API type’ composed of library files.

The general user identification and authentication procedure of the TOE is as shown

in “[Figure 1] User identification and authentication procedure”, and the detailed execution procedure is divided into an initial authentication phase based on ID/password and an authentication token-based business system authentication phase.

The user identification and authentication process is divided into an initial authentication phase using ID/password-based authentication and an authentication token-based authentication phase in which the user accesses business systems using the authentication token issued during the initial authentication process.
First, the execution procedure of the initial authentication phase is as follows. The user requests login using an ID/password, and the SSO agent that receives the login request message sends a login verification request to the SSO server to check whether the user is legitimate. Upon receiving the login verification request, the SSO server performs login verification directly using the user information stored in the DBMS. If the login verification result is valid, the SSO server issues an authentication token. The SSO agent delivers the token issued by the SSO server to the user.

The authentication token-based authentication phase is performed only when an authentication token has been normally issued through the initial authentication phase. When the user uses business system services, the issued authentication token is delivered to the SSO agent installed in the corresponding business system, and the SSO agent that receives the token verifies the validity of the authentication token through interaction with the SSO server.

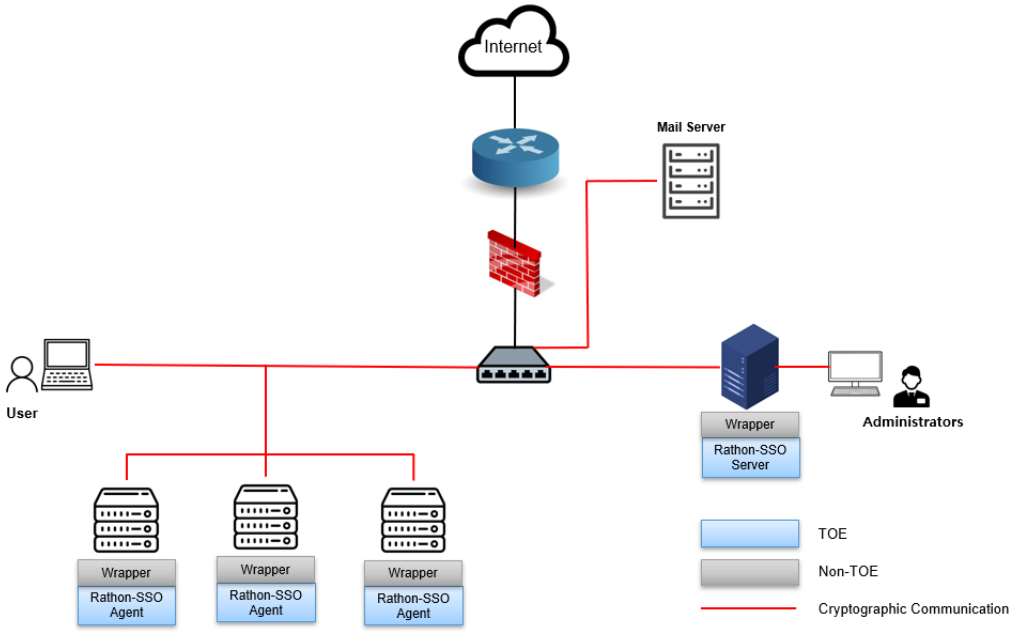


[Figure 1] User Identification and Authentication Procedure

In addition, the subjects responsible for authentication token issuance, storage, and verification are as follows.

- Subject responsible for authentication token issuance: Rathon-SSO Server
- Authentication token storage location: user PC web browser, Rathon-SSO Server
- Subject responsible for authentication token verification: Rathon-SSO Server

The TOE operational environment is as shown in “[Figure 2] TOE Operational Environment”. The TOE operational environment consists of an SSO server and an SSO agent.
TOE operational environment consists of an SSO server and an SSO agent.
The SSO server provides user login verification directly using user information stored in the DBMS, authentication token management, and policy configuration. The SSO agent performs user login verification requests to the SSO server and authentication token issuance and verification request functions, and operates by being installed in each business system. In addition, the SSO agent is provided in an ‘API type’ composed of library files.



[Figure 2] TOE Operational Environment

Authorized administrators access the SSO server through a web browser to perform security management. In the TOE operational environment, a wrapper may be used

to ensure compatibility with business systems, and the wrapper is excluded from the TOE scope.
Encrypted communication is performed in the communication sections between TOE components, and encrypted communication using TLS v1.3 or higher is also be performed when communication between the mail server and TOE components is required.
As external entities required for operating the TOE, a mail server is used to notify authorized administrators in cases such as administrator authentication failure or predicted 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	AMD Ryzen 5 5600G with Radeon Graphics 4.464 GHz or higher
		Memory	16 GB or higher
		HDD	Required storage space for TOE installation: 500 GB or more
		NIC	100/1000 Mbps * 1 EA or higher
	SW	OS	Ubuntu 24.04.3 (kernel 6.8.0, 64 bit)
		DBMS	PostgreSQL 17.7
		WAS	Apache Tomcat 11.0.18
SSO Agent	HW	CPU	AMD Ryzen 5 5600G with Radeon Graphics 4.464 GHz or higher
		Memory	16 GB or higher
		HDD	Required storage space for TOE installation: 500 GB or more
		NIC	100/1000 Mbps * 1 EA or higher
	SW	OS	Ubuntu 24.04.3 (kernel 6.8.0, 64 bit)
		WAS	Apache Tomcat 11.0.18

[Table 1] TOE Hardware and Software specifications

The minimum requirements for the administrator system for security management are shown in [Table 2]

Classification		Minimum Requirement
SW	Web Browser	Chrome 145.0(64bit)

[Table 2] Administrator PC Requrements.

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

Component	Requirement
Mail Server	It is used to send information mail to administrator in case of potential security threat of the TOE

[Table 3] External Entity

Validated cryptographic modules included the TOE are as follows.

Category	Description
Cryptographic Module	RTJCrypto V1.0
Validation No.	CM-281-2030.10
Developer	RathonTech Co., Ltd.
Module type	S/W(library)
Validation Date	October 24, 2025
Effective Expiration Date	October 24, 2030

[Table 4] Validated Cryptographic Module

The 3rd party S/W Included in TOE is as follws.

Component	3rd party S/W	Description
SSO Server	JRE 21.0.10+7	TSF Data Transfer
SSO Agent	JRE 21.0.10+7	TSF Data Transfer

[Table 5] The 3rd party S/W included in TOE

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE	Rathon-SSO v4.0
Version	V4.0.1
TOE Components	Rathon-SSO Server v4.0.1 Rathon-SSO Agent v4.0.1
Manuals	Rathon-SSO Preparation Procedures v1.1 Rathon-SSO Operating Manual v1.1

[Table 6] 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	Rathon-SSO v4.0
Common Criteria	Part 1: Introduction and general model, CC:2022 R1(CCMB-2022-11-001, 2022.11.) Part 2: Security functional components, CC:2022 R1(CCMB-2022-11-002, 2022.11.) Part 3: Security assurance components, CC:2022 R1(CCMB-2022-11-003, 2022.11.) Part 4: Framework for the specification of evaluation methods and activities, CC:2022 R1(CCMB-2022-11-004, 2022.11.) Part 5: Pre-defined packages of security requirements, CC:2022 R1(CCMB-2022-11-005, 2022.11.)
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), Version 1.2, CCMB-2025-001,

	October 2025
EAL	EAL1+(ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign On V3.1
Developer	RathonTech Co., LTD.
Sponsor	RathonTech Co., LTD.
Evaluation Facility	Korea System Assurance, Inc. (KOSYAS)
Completion Date of Evaluation	March 16, 2026

[Table 7] 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

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 6])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the Rathon-SSO Server, Rathon-SSO Agent and Manual. Verified Cryptographic Module(RTJCrypto V1.0) is embedded in the TOE components.

Hardware and OS where the TOE is installed are not included in the scope of the TOE.

Category		Type	Delivery
TOE	Rathon-SSO v4.0	-	-
TOE Version	v4.0.1	-	-
TOE Component	Rathon-SSO Server v4.0.1 : Rathon-SSO_Server-v4.0.1.war	S/W	CD
	Rathon-SSO Agent v4.0.1 : Rathon-SSO_Agent-v4.0.1.war		
Manual	Rathon-SSO Preparation Procedure v1.1 : Rathon-SSO_Preparation_Procedure_v1.1.pdf	PDF	
	Rathon-SSO Operating Manual v1.1 : Rathon-SSO_Operating_Manual_v1.1.pdf		

[Table 6] Physical scope of TOE

Validated cryptographic modules included the TOE are as follows in [Table 9].

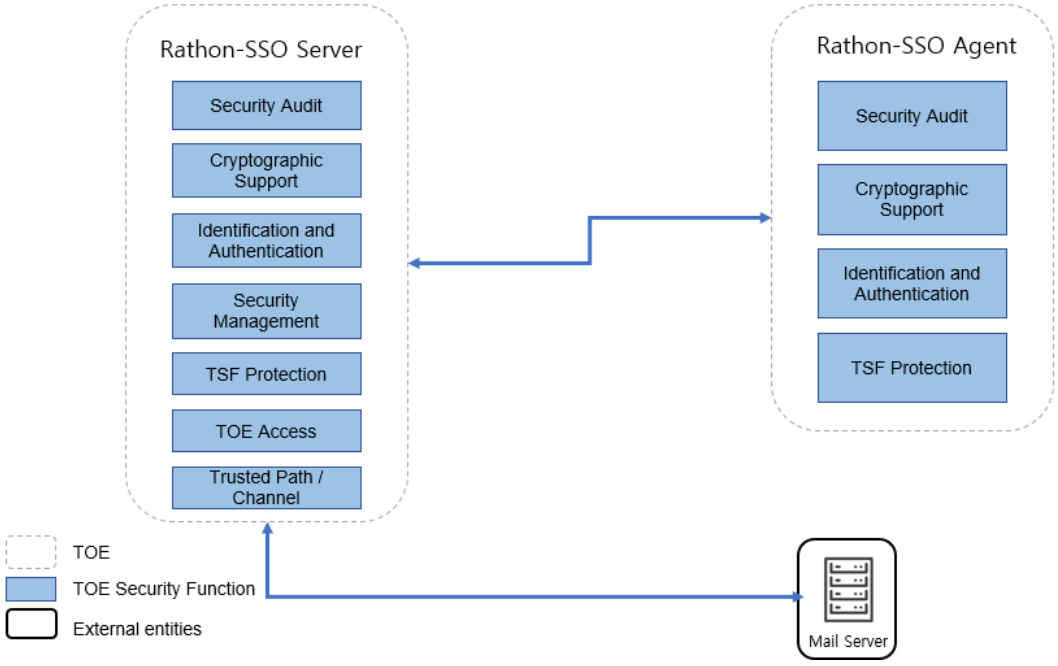
Category	Description
Cryptographic Module	RTJCrypto V1.0
Validation No.	CM-281-2030.10
Developer	RathonTech Co., Ltd.
Module type	S/W (library)

Validation Date	October 24, 2025
Effective Expiration Date	October 24, 2030

[Table 9] Validated 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 SSO server generates audit data for accountability of security-related events. The audit data generated by the SSO server records the date and time of the event, event type, identity of the subject, and event result (success or failure). All audit data is stored in the DBMS.

Authorized administrators can view audit data through the administrator interface and search audit data by applying descending order based on the date and time of the event using the event date AND event type as criteria.

When the audit data storage capacity reaches a predefined fixed threshold, a warning

email is sent to the administrator. In addition, when the audit data storage becomes full, audit events are not recorded and a warning message is sent to the administrator via email.

Additionally, when the following potential violations are detected, a warning message is sent to the administrator via email.

List of potential violations are follow:

- When administrator authentication attempts fail consecutively for the defined number of times (fixed value: 5 times),
- When general user authentication attempts fail consecutively for the defined number of times (fixed value: 5 times),
- When a validated cryptographic module self-test fails within the SSO server,
- When integrity verification fails within the SSO server,
- When a process test fails within the SSO server,
- When a validated cryptographic module self-test fails within the SSO agent,
- When integrity verification fails within the SSO agent,
- When a process test fails within the SSO agent,
- When the audit data repository threshold (fixed value: 80%) is exceeded,
- When the audit data repository reaches saturation (fixed value: 90%)

The SSO agent transmits audit data to the SSO server for recording when audit events occur, such as success or failure of user identification and authentication, or integrity verification of the SSO agent.

▣ Cryptographic support

The TOE uses a validated cryptographic module (RTJCrypto V1.0, CM-281-2030.10), whose security and implementation conformance have been verified through the Korea Cryptographic Module Validation Program (KCMVP), to manage cryptographic keys, perform cryptographic operations, and generate random bits for communication between

the SSO server and the SSO agent.

The TOE securely generates cryptographic keys based on the validated random number generation mechanism compliant with standards, ‘Hash_DRBG(SHA-384)’. The generated cryptographic keys include an integrity verification key (256 bit), a data encryption key (256 bit), an authentication token encryption key (128 bit), and a session key (128 bit). In addition, public/private key pairs (RSAES and RSA-PSS, 3072 bit) of the SSO server and SSO agent are respectively generated and used for session key protection and digital signatures, and the KEK for DEK protection is securely generated through a PBKDF2 (SHA-256)-based key derivation function.

Cryptographic operations are performed using validated cryptographic algorithms compliant with standards for KEK key derivation for DEK encryption (PBKDF2, SHA-256), TOE component integrity verification (HMAC, SHA-256), one-way encryption of user passwords (SHA-256), DEK, TSF data encryption(ARIA-CBC, 256 bit) and authentication token encryption(ARIA-CBC, 128 bit), transmission section security (RSAES, SHA-256), and mutual authentication between the SSO server and the SSO agent (RSA-PSS, SHA-256).

All cryptographic keys used in the SSO server and SSO agent are securely generated, managed, and destroyed, and upon destruction, the key values are overwritten with ‘0’ three times for zeroization.

Furthermore, the TSF performs deterministic random bit generation using the Hash_DRBG (SHA-384) algorithm in accordance with KS X ISO/IEC 18031 and TTAK.KO-12.0331.

When the reseed count limit (1000 times) is reached, the DRBG is reseeded using a software-based entropy source (new SecureRandom().nextBytes()) in accordance with TTAK.KO-12.0235/R2 to update the internal state.
The TSF securely seeds the DRBG using a single internal entropy source with at least 2^{112} bits of entropy to provide random bits required for performing security functions such as cryptographic key generation.

▣ Identification and authentication

The SSO server performs identification and authentication based on the administrator ID during administrator authentication and requires administrator authentication prior to all

operations. Additionally, it provides authentication feedback protection during authentication information input and blocks access for 5 minutes when five consecutive authentication failures occur. Furthermore, the SSO server uses a CSRF token to prevent authentication information reuse attempts when administrators log in.

The SSO agent performs identification and authentication through initial authentication and authentication token-based authentication for general users and requires authentication prior to all operations. Additionally, it provides authentication feedback protection during authentication information input and blocks access for 5 minutes when five consecutive authentication failures occur. Furthermore, the SSO agent uses a CSRF token to prevent authentication information reuse attempts when general users log in.

The SSO agent and the SSO server perform mutual authentication through a proprietary protocol.

When issuing an authentication token, the SSO server generates the authentication token using a validated cryptographic module, and authentication token verification is also performed through the same validated cryptographic module.

The SSO server verifies secure password composition rules for administrators and general users based on the defined criteria and securely hashes verified passwords using a SHA-256-based algorithm with a 16-byte salt and 1000 iterations before storage.

When generating an authentication token for general users during the single sign-on process, the authentication token is generated using a validated cryptographic module based on authentication token generation information. Additionally, upon authentication token destruction, the data is overwritten with ‘0’ three times for secure destruction.

The TSF displays the password entered by administrators and general users as “▪” instead of the actual characters during the authentication process.

The TSF successfully identifies each user before performing any actions on behalf of that user.

▣ Security Management

The SSO server restricts security management functions such as general user management, administrator information management, audit data inquiry, access control policy management, and business system configuration settings so that they are

provided only to authorized administrators. Authorized administrators can perform such management functions only through the security management interface.

TSF data management functions are permitted only to authorized administrators. The TSF enforces password change upon the administrator's initial access and provides administrator information modification and general user password generation functions only to authorized administrators.

The TSF classifies roles into authorized administrators as the super administrator role and general users as the user role. The super administrator has all privileges (Read/Write), and the general user can perform only the function of changing their own password.

Authorized administrators consist solely of super administrators, and the super administrator performs all security management functions of the TOE through the security management interface.

When an authorized administrator accesses the security management interface for the first time, password change is mandatorily required.

▣ Protection of the TSF

The SSO server applies the TLS v1.3 encrypted communication protocol based on JRE to ensure confidentiality and integrity when communicating with the SSO agent.For TSF data protection, authentication information of general users and administrators is encrypted for storage and management, and integrity verification information is also encrypted and managed. All critical data is stored and managed in encrypted form in files and the DBMS.

In addition, TSF self-tests, TSF integrity tests, and cryptographic module self-tests are performed during initial boot and periodic operation, and TSF integrity tests are performed upon the administrator's manual request to ensure TSF data protection.

The SSO agent applies the TLS v1.3 encrypted communication protocol based on JRE to ensure confidentiality and integrity when communicating with the SSO server.

For TSF data protection, authentication information of general users is encrypted for storage and management, and integrity verification information is encrypted and managed. All critical data is stored and managed in encrypted form in files.

The TSF is protect important information stored in repositories controlled by the TSF, such as passwords, cryptographic keys, account information, authentication keys, and TOE configuration values, from unauthorized disclosure.

If entropy source errors such as noise source health test failure occur, the SSO server and SSO agent transition to a fatal error state, and in such cases, the validated cryptographic module and TOE operation are blocked. Thereafter, authorized administrators maintain a secure state by reinstalling the system and restarting the WAS server in accordance with the manual recovery procedures specified in the preparation procedures document.

▣ TOE access

When executing security management functions of the SSO server, concurrent sessions are restricted, and the maximum number of concurrent management access sessions belonging to the same administrator is limited to ‘1’. If an authorized administrator is already logged in and the same administrator account attempts to log in, the new access is blocked.

For general user access sessions of the SSO agent, the maximum number of concurrent sessions is also limited to ‘1’.

In addition, if an administrator session or general user session exceeds the designated inactivity timeout (fixed value: 10 minutes), the session is automatically terminated.

Authorized administrators are restricted according to allowed IP access rules (maximum of 2 IP addresses), and the results of session restrictions are generated as audit data in the security management interface.

▣ Trusted Path/Channels

The TOE provides a secure channel based on TLS v1.3, a standardized secure communication protocol, to ensure secure communication between external IT entities such as TSF.

6. Documentation

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

Identification	Date
Rathon-SSO Preparation Procedure v1.1 : Rathon-SSO_Preparation_Procedure_v1.1.pdf	Feburary 13, 2026
Rathon-SSO Operating Manual v1.1 : Rathon-SSO_Operating_Manual_v1.1.pdf	Feburary 13, 2026

[Table 10] 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: Rathon-SSO v4.0(v4.0.1)

- Rathon-SSO Server v4.0.1
- Rathon-SSO Agent v4.0.1

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 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+).

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 defined 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, it covers security procedures for all operating modes and facilitates the prevention and detection of unsafe TOE conditions. 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 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.

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
		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 11] 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 checks 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**

Rathon-SSO v4.0 Security Target v1.1[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, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November, 2022

[2] Common Methodology for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-006, November, 2022

[3] Korean National Protection Profile for Single Sign On V3.1

[4] Rathon-SSO v4.0 Security Target v1.1, February 13, 2026

[5] Rathon-SSO v4.0 Independent Testing Report(ATE_IND.1) V1.00, March 13, 2026

[6] Rathon-SSO v4.0 Penetration Testing Report (AVA_VAN.1) V2.00, March 13, 2026

[7] Rarthon-SSO v4.0 Evaluation Technical Report V2.00, March 24, 2026