KECS-CR-26-13

# Rathon-SSO v4.0
# 인증보고서

인증번호 : KECS-CISS-1395-2026

2026년 4월

IT보안인증사무국

# 1. 제품 개요

Rathon-SSO v4.0(이하 TOE)은 일반 사용자에게 한번의 로그인(Single Sign-On)으로 다양한 업무시스템에 추가적인 로그인 행위 없이 서비스를 제공하는 통합인증(SSO) 제품으로 소프트웨어 형태로 제공된다.

TOE 및 TOE 구성요소에 대한 식별정보 및 배포형태는 [표 1]과 같다.

| 구분 | 식별정보 | | 유형 | 배포 |
|---|---|---|---|---|
| TOE | Rathon-SSO v4.0 | | - | - |
| TOE 세부버전 | v4.0.1 | | - | - |
| TOE 구성요소 | SSO 서버 | Rathon-SSO Server v4.0.1 (Rathon-SSO_Server-v4.0.1.war) | S/W | CD |
| | SSO 에이전트 | Rathon-SSO Agent v4.0.1 (Rathon-SSO_Agent-v4.0.1.war) | | |
| 설명서 | 준비절차서 | Rathon-SSO v4.0 준비절차서 v1.1 (Rathon-SSO v4.0 준비절차서_v1.1.pdf) | 전자문서 (PDF) | CD |
| | 운영설명서 | Rathon-SSO v4.0 운영설명서 v1.1 (Rathon-SSO v4.0 운영설명서_v1.1.pdf) | | |

[표 1] TOE 구성요소 및 식별 정보

TOE가 설치 및 운영되는 하드웨어 및 소프트웨어 최소 요구사항은 아래의 표와 같다.

| 구분 | | 최소 요구사항 |
|---|---|---|
| SSO 서버 | CPU | AMD Ryzen 5 5600G with Radeon Graphics 4.464 GHz 이상 |
| | Memory | 16 GB 이상 |
| | HDD | TOE 설치를 위한 필요한 공간: 500 GB 이상 |
| | NIC | Ethernet 100/1000 Mbps * 1 Port 이상 |
| | OS | Ubuntu 24.04.3 (kernel 6.8.0, 64 bit) |
| | S/W | PostgreSQL 17.7<br>Apache Tomcat 11.0.18 |
| SSO 에이전트 | CPU | AMD Ryzen 5 5600G with Radeon Graphics 4.464 GHz 이상 |
| | Memory | 16 GB 이상 |

| | | |
|---|---|---|
| | HDD | TOE 설치를 위한 필요한 공간: 500 GB 이상 |
| | NIC | Ethernet 100/1000 Mbps * 1 Port 이상 |
| | OS | Ubuntu 24.04.3 (kernel 6.8.0, 64 bit) |
| | S/W | Apache Tomcat 11.0.18 |

[표 2] TOE 설치 요구사항

또한, TOE의 운영을 위해 연동되는 외부 IT 실체는 다음과 같다.

| 외부 IT 실체 | 내 용 |
|---|---|
| 메일 서버 | 인가된 관리자가 설정한 이메일로 경보 메일을 발송하기 위함 |

[표 3] 외부 IT 실체

인가된 관리자가 보안관리를 수행하기 위해 요구되는 시스템의 최소 요구사항은 다음과 같다.

| 구분 | 사양 |
|---|---|
| 소프트웨어 | Chrome 145.0(64bit) |

[표 4] 관리자 PC 요구사항

TOE에 포함되는 3rd party S/W는 다음과 같다.

| 구성요소 | 항목 | 용도 |
|---|---|---|
| SSO서버 | JRE 21.0.10+7 | 구성요소 간 TLS v1.3 암호통신 시 사용 |
| SSO 에이전트 | | |

[표 5] TOE 포함 3rd party S/W

TOE에서 사용하는 검증필 암호모듈은 아래와 같다.

| 구분 | 내 용 |
|---|---|
| 암호모듈 명칭 | RTJCrypto V1.0 |
| 개발업체 | ㈜라톤테크 |
| 검증번호 | CM-281-2030.10 |
| 검증일 | 2025년 10월 24일 |
| 효력만료일 | 2030년 10월 24일 |

[표 6] TOE에서 사용하는 검증필 암호모듈

**인증 효력에 관한 고지**: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

# 2. 주요 기능

TOE가 제공하는 주요 보안기능은 다음과 같다.

● 보안감사

SSO 서버는 보안과 관련된 이벤트에 대한 책임 추적을 위해 감사 데이터를 생성한다. SSO 서버에서 생성된 감사 데이터에는 이벤트의 날짜 및 시간, 이벤트 유형, 주체의 신원, 이벤트 결과(성공 또는 실패)가 기록된다. 모든 감사 데이터는 DBMS에 저장한다. 인가된 관리자는 관리자 화면을 통해 감사 데이터를 조회할 수 있으며, 이벤트의 날짜 AND 이벤트 유형을 기초하여 감사 데이터에 대한 이벤트의 시간 및 날짜 기준으로 내림차순 정렬을 적용하여 감사 데이터를 검색한다.

● 암호지원

TOE는 한국 암호모듈 검증 제도(KCMVP)를 통해 보안성과 구현 적합성이 확인된 검증된 암호모듈(RTJCrypto V1.0, CM-281-2030.10)을 사용하여 암호키를 관리하고 암호 연산을 수행한다. TOE는 표준에 부합하는 검증된 난수 생성 메커니즘인 'Hash_DRBG(SHA-384)'를 기반으로 암호키를 안전하게 생성한다. 생성되는 암호키에는 TOE 구성요소 무결성 검증을 위한 무결성 검증용 키(256bit), 데이터 암호화를 위한 데이터 암호화용 키(256bit), 인증토큰 보호를 위한 인증토큰 암호화용 키(128bit), SSO 서버와 SSO 에이전트 간 전송 정보 보호를 위한 세션키(128bit)가 포함된다. 또한 전송 정보 암호화를 위한 세션키 보호 및 전자서명을 위해 SSO 서버 및 SSO 에이전트의 공개/비공개 키 쌍(RSAES 및 RSA-PSS, 3072bit)을 각각 생성·사용하며, DEK 보호를 위한 KEK는 PBKDF2(SHA-256) 기반의 암호키 유도 함수를 통해 안전하게 생성한다.

● 식별 및 인증

SSO 서버는 관리자 인증 시 관리자 ID를 기반으로 식별 및 인증을 수행하며, 모든 작업에 앞서 관리자 인증을 필수로 요구한다. 또한 인증 정보 입력 과정에서 인증 피드백 보호 기능을 제공하고, 연속된 인증 실패가 5회 발생할 경우 5분간 인증을 차단한다. 관리자가 SSO 서버에 로그인할 때 인증 정보 재사용 시도를 방지하기 위해 CSRF 토큰을 사용한다.

SSO 에이전트는 일반 사용자의 최초 인증 및 인증 토큰 기반 인증을 통해 식별과 인증을 수행하며, 모든 작업 전에 인증을 필수로 요구한다. 또한 인증 정보 입

력 시 인증 피드백 보호 기능을 제공하고, 연속된 인증 실패가 5회 발생할 경우 5분간 접근을 차단하여 안전한 식별 및 인증을 보장한다. 일반 사용자가 SSO 에이전트에 로그인할 때 인증 정보 재사용 시도를 방지하기 위해 CSRF 토큰을 사용한다. SSO 에이전트와 SSO 서버 간에는 자체 프로토콜을 통해 상호 인증을 수행한다.

● 보안관리

SSO 서버는 일반 사용자 관리, 관리자 정보 관리, 감사 데이터 조회, 접근 제어 정책 관리, 업무시스템 환경 설정 등 보안 관리 기능을 인가된 관리자에게만 제공하도록 제한한다. 인가된 관리자는 보안 관리 인터페이스를 통해서만 해당 관리 기능을 수행할 수 있다. TSF 데이터 관리 기능은 인가된 관리자에게만 허용된다. TSF는 관리자 최초 접속 시 비밀번호 변경을 강제하며, 관리자 정보 수정 시 및 일반 사용자 비밀번호 생성 기능 또한 인가된 관리자에게만 제공한다.

● TSF 보호

SSO 서버는 TLS v1.3 암호화 통신 프로토콜을 적용하여 SSO 에이전트와의 통신 시 기밀성과 무결성을 보장한다. TSF 데이터 보호를 위해 일반 사용자 및 관리자의 인증 정보를 암호화하여 저장·관리하고, 무결성 검증 정보 또한 암호화하여 관리한다. 모든 중요 데이터는 파일 및 DBMS에 암호화된 형태로 저장 및 관리된다. 또한 TSF 자체 시험, TSF 무결성 시험 및 암호모듈 자가 시험을 초기 부팅 시와 정기적인 운영 중에 수행하며, 관리자의 수동 요청 시 TSF 무결성 시험을 수행함으로써 TSF 데이터 보호를 보장한다.

● TOE 접근

SSO 서버의 보안 관리 기능을 실행할 때, 동시 세션을 제한하고, 동일한 관리자에게 속한 관리 접근의 최대 동시 세션 수는 ‘1’로 제한한다. 인가된 관리자가 이미 로그인한 상태에서 동일한 관리자 계정이 로그인하려고 시도하면 새로운 접근을 차단한다. SSO 에이전트의 일반 사용자 접근 세션의 경우도 최대 동시 세션 수는 ‘1’로 제한한다. 또한, 관리자 세션 및 일반 사용자 세션이 지정된 비활성 시간 초과(고정값: 10분)을 넘길 경우, 해당 세션이 자동 종료된다.

● 안전한 경로/채널

TOE는 외부 IT 실체와의 안전한 통신을 보장하기 위해 표준화된 보안 통신 프로토콜인 TLS v1.3을 기반으로 한 보안 채널을 제공한다.

# 3. 평가결과 요약

TOE에 대한 평가는 한국시스템보증에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부를 만족하고, 국가용 보호프로파일을 준수하여 공통평가기준 1부 330항에 따라 “적합”한 것으로 평가하였다.

[ 인증제품 식별정보 ]

| | |
|---|---|
| **평가지침** | 정보보호시스템 평가·인증 등에 관한 고시 (2022. 10. 31.)<br>정보보호제품 평가인증 수행규정 (2021. 5. 17.) |
| **평가제품** | Rathon-SSO v4.0 |
| **보호프로파일** | 국가용 통합인증 보호프로파일 V3.1 (2025.06.27.) |
| **보안요구사항** | 없음 |
| **보안목표명세서** | Rathon-SSO v4.0 보안목표명세서 v1.1 (2026.02.13.) |
| **평가보고서** | Rathon-SSO v4.0 평가결과보고서 V2.00 (2026.03.24.) |
| **적합여부<br>평가결과** | 공통평가기준 2부 적합<br>공통평가기준 3부 적합 |
| **평가기준** | 정보보호시스템 공동평가기준 CC:2022 R1<br>Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025 |
| **평가방법론** | 정보보호시스템 공동평가기준 CC:2022 R1<br>Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025 |
| **검증필 암호모듈** | RTJCrypto V1.0 |
| **평가신청인** | ㈜라톤테크 |
| **개발업체** | ㈜라톤테크 |
| **평가기관** | 한국시스템보증 |