KECS-CR-19-70

Magic SSO V4.0
인증보고서

인증번호 : KECS-CISS-0977-2019

2019년 11월

IT보안인증사무국

1. 제품 개요

Magic SSO V4.0 (이하 'TOE')는 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		Magic SSO V4.0	-	
세부버전		v4.0.0.2	-	
TOE 구성요소	SSO 서버	Magic SSO V4.0 Server v4.0.0.2 (magicsso-server-4.0.0.2.tar)	S/W	CD
	SSO 에이전트	Magic SSO V4.0 Agent v4.0.0.2 (magicsso-agent-4.0.0.2.tar)	S/W	CD
매뉴얼	설치지침서	Magic SSO V4.0 설치지침서 v1.2 (Magic_SSO_V4.0-PRE-v1.2.pdf)	PDF (CD 배포)	CD
	운영설명서	Magic SSO V4.0 운영설명서 v1.2 (Magic_SSO_V4.0-OPE-v1.2.pdf)		

[표 1] TOE 및 TOE 구성요소 식별정보

TOE는 ID/PW 방식의 일반 사용자 로그인 기능을 제공하고, 일반 사용자 로그인 과정에서 인증토큰을 발급하며, 일반 사용자 로그인 후 다른 업무시스템으로 접속하는 경우 발급된 인증토큰을 검증한다.

TOE는 보안기능 및 관리기능 구동 시 주요 사건에 대해 감사 데이터를 기록하여 관리하는 보안감사 기능, TSF가 통제하는 저장소 내에 저장된 데이터 보호, TSF 자체 시험 등의 TSF 보호 기능을 제공한다. 또한, 인증 실패 처리, TOE 구성요소 간 상호인증 등의 식별 및 인증 기능, 인증토큰 발급을 위한 암호키 관리 및 암호 연산 기능 등의 암호 지원 기능, 보안 기능 관리 및 환경설정 등을 위한 보안관리 기능, 인가된 관리자의 접속 세션 관리를 위한 TOE 접근 기능을 제공한다. 추가적으로, 인증토큰의 경우 비밀성과 무결성을 제공하고 TOE 실행코드는 무결성을 제공한다.

일반 사용자 식별 및 인증 과정은 ID/PW를 통한 일반 사용자 식별 및 인증 단계와 사용자 인증 이후 SSO 서버로부터 발급된 인증 토큰을 이용하여 업무 시스템으로 접속하기 위한 인증 토큰 기반 인증 단계로 구분한다.

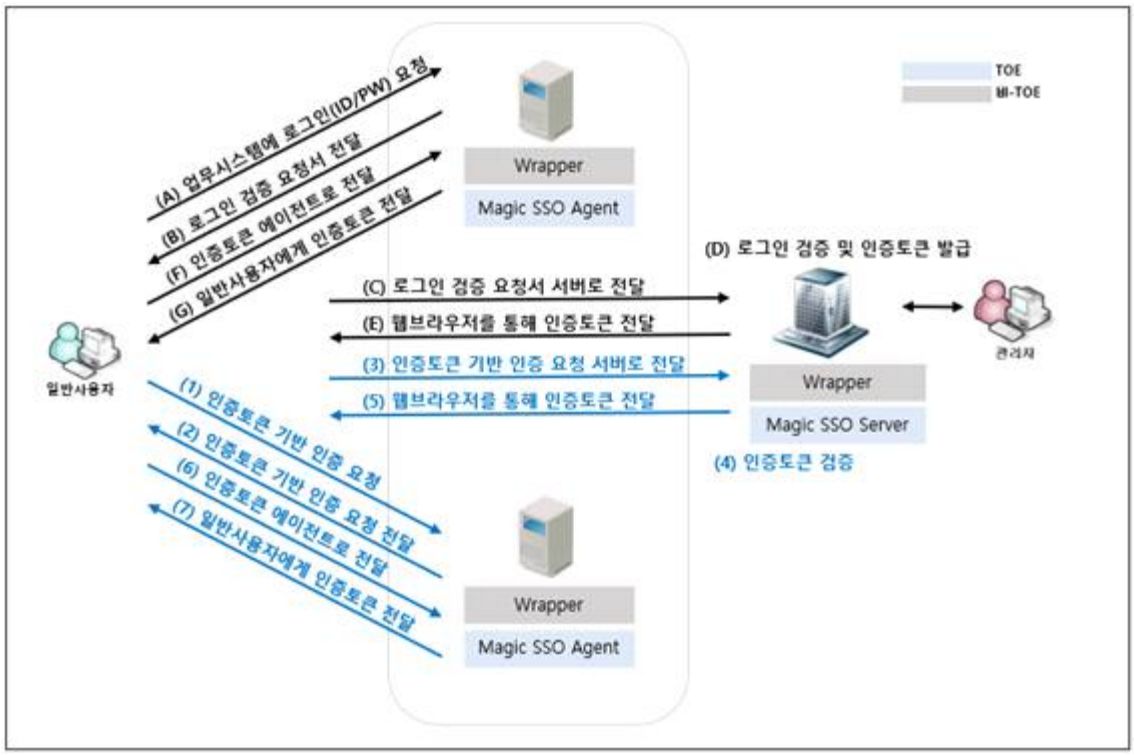
최초 인증 단계의 수행 절차는 다음과 같다.

일반 사용자가 업무시스템에 접근하여 ID/PW를 입력하면 SSO 에이전트는 SSO 서버에게 정당한 일반 사용자 여부를 확인하는 로그인 검증 요청을 보낸다. 로그인

검증 요청을 수신한 SSO 서버는 DBMS에 저장된 일반 사용자 정보를 사용하여 로그인 검증을 수행 후 로그인 검증 결과가 유효한 경우 인증토큰을 발급한다. 발급된 인증토큰은 SSO 에이전트로 전달된다. SSO 에이전트에서는 인증토큰을 검증하고 해당 인증토큰이 유효한 경우에만 일반 사용자에게 전달한다.

인증토큰 기반 인증단계는 최초 인증단계를 통해 인증토큰을 정상적으로 발급한 경우에만 수행된다.

일반 사용자가 업무시스템에 설치된 SSO 에이전트에 인증토큰기반 인증 요청을 수행하면 인증 요청을 수신한 SSO 에이전트는 SSO 서버에게 인증토큰 검증 요청을 보낸다. 인증토큰 검증 요청을 수신한 SSO 서버는 저장하고 있는 인증토큰 검증을 수행 후 검증 결과가 유효한 경우, 인증토큰을 SSO 에이전트로 전달한다. 해당 인증토큰을 수신한 SSO 에이전트는 인증토큰을 검증하고, 유효한 경우 일반 사용자에게 전달한다.



[그림 1] 사용자 식별 및 인증 절차

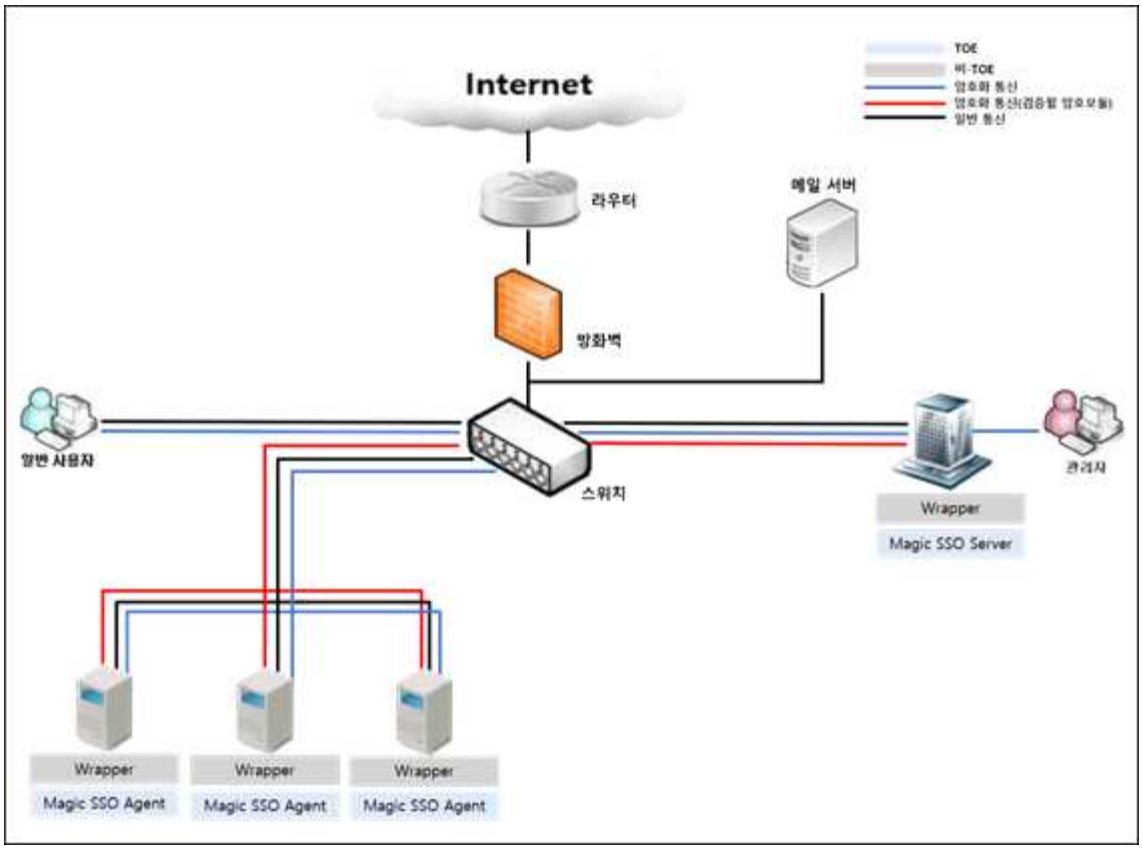
인증단계	동작절차
최초인증	(A) 업무시스템에 로그인(ID/PW) 요청→ (B) 로그인 검증 요청서 전달 → (C) 로그인 검증 요청서 서버로 전달 → (D) 로그인 검증 및 인증토큰 발급 → (E) 웹브라우저를 통해 인증토큰 전달 → (F) 인증토큰 에이전트로 전달 → (G) 일반사용자에게 인증토큰 전달
인증토큰 기반인증	(1) 인증토큰 기반 인증 요청→ (2) 인증토큰 기반 인증 요청 전달 → (3) 인증토큰 기반 인증 요청 서버로 전달 → (4) 인증토큰 검증 →

	(5) 웹브라우저를 통해 인증토큰 전달 → (6) 인증토큰 에이전트로 전달 → (7) 일반사용자에게 인증토큰 전달

[표 2] 인증단계별 동작 절차

- 인증토큰 발급주체 : SSO 서버
- 인증토큰 저장 위치 : 일반 사용자 PC 브라우저
- 인증토큰 검증 수행 주체 : SSO 서버, SSO 에이전트

TOE는 [그림 2]과 같은 운영환경에서 동작한다.



[그림 2] TOE 운영환경

TOE는 관리서버와 업무시스템에 설치되어 운영된다.

SSO 서버는 관리서버의 DBMS에 저장된 일반 사용자 정보를 사용하여 직접 일반 사용자 로그인 검증, 인증토큰 발급 및 관리, 정책 설정 등의 기능을 제공하고, 웹 어플리케이션 형태로 TOE 관리를 위한 보안관리 인터페이스 기능을 제공한다.

SSO 에이전트는 라이브러리 파일로 구성된 'API 형태' 로 SSO 서버에게 일반 사용자 로그인 검증 요청, 인증토큰 발급 및 검증 요청 등의 기능을 수행하며, 각 업무시스템에 설치되어 동작한다.

TOE 관리자가 브라우저 상에서 관리서버 웹 주소를 입력하여 TOE 보안관리 인터페이스에 접근할 때 브라우저는 HTTPS 보안 채널을 형성한다.

TOE를 운영하기 위해 필요한 외부 실체로는 감사데이터 손실 예측 시 인가된 관리자 알림을 위한 메일 서버가 있으며, TOE를 제외한 외부 실체인 메일서버는 TOE 운영환경에 해당한다.

TOE가 설치 및 운영되는 하드웨어 및 소프트웨어 최소 요구사항은 아래표와 같다.

구분			최소 요구사항
Magic SSO Server	HW	CPU	Intel Dual Core 2 GHz 이상
		Memory	8 GB 이상
		HDD	TOE 설치에 필요한 공간 100 GB 이상
		NIC	100/1000 Mbps 1개 이상
	SW	OS	CentOS 6.10 kernel 2.6.32 (64 bit)
		DBMS	Oracle 11g(11.2.0.1.0)
		Java	Java(JDK) 1.8.0_211
		WAS	Apache Tomcat 8.5.45
Magic SSO Agent	HW	CPU	Intel Dual Core 2 GHz 이상
		Memory	8 GB 이상
		HDD	TOE 설치에 필요한 공간 100 GB 이상
		NIC	100/1000 Mbps 1개 이상
	SW	OS	CentOS 6.10 kernel 2.6.32 (64 bit)
		Java	Java(JDK) 1.8.0_211
		WAS	Apache Tomcat 8.5.45

[표 3] TOE 설치 요구사항

인가된 관리자가 보안 관리 기능을 수행하기 위한 시스템의 최소 요구사항은 아래의 표와 같다.

구 분		최소요구사항
HW	CPU	Intel Dual Core 2 GHz 이상
	Memory	8 GB 이상
	Disk	50 GB 이상
	NIC	100/1000 Mbps 1개 이상
SW	OS	Windows 10 Pro (64 bit)
	Browser	Internet Explorer 11

[표 4] 관리자 PC 요구사항

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

구 분	내 용
메일 서버	관리자에게 경고 메일을 발송하기 위한 서버

[표 5] 외부 IT실체

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 행동에 대한 책임을 추적하기 위해 보안 관련 사건들에 대한 감사데이터를 생성한다. 모든 생성되는 감사데이터는 DBMS에 저장한다. 인가된 관리자는 관리자 화면을 통해서 감사데이터를 검토할 수 있으며, 감사 데이터를 검색할 수 있다.

○ TOE 접근

TOE는 관리자 접속 세션의 경우 동시 세션 수를 제한한다. 관리자/일반사용자 접속 세션은 비활동 기간 후에는 세션 종료된다. 관리자 관리접속은 관리자가 설정 가능한 접속 IP 이외의 접속은 거부된다.

○ 암호지원

TOE는 암호모듈 검증제도를 통해 안전성 및 구현적합성이 확인된 검증필 암호모듈인 MagicJCrypto V2.0.0.0을 통해 제품 운영에 사용되는 모든 암호키를 안전하게 생성, 폐기하고 암호 알고리즘을 정의한 암호정책에 따라 인증토큰 생성/검증 등에 대한 암호 연산을 수행한다. 또한 물리적으로 분리된 SSO 서버와 SSO 에이전트간 암호화 통신을 위해 검증필 암호모듈인 MagicJCrypto V2.0.0.0을 통해 암호키를 생성 및 교환한다.

○ 식별 및 인증

TOE는 보안 관리 기능을 이용하려는 관리자를 모든 행동 이전에 식별 및 인증을 수행하며 인증 데이터 입력 시 인증 피드백을 보호하는 기능을 제공한다. TOE는 일반 사용자가 통합인증 기능을 이용하기 위해 SSO 에이전트에 식별 및 인증을 수행한다.

○ 보안관리

SSO 서버는 보안관리 인터페이스를 통해 인가된 관리자에게 보안 역할, 정책, 일반 사용자 정보, 감사 정보 관리 기능을 제공한다. 인가된 관리자는 보안관리 인터페이스를 통해 관리자 또는 일반사용자의 패스워드를 변경할 수 있으며,

일반 사용자와 인가된 관리자의 패스워드 생성 및 변경 시 패스워드 정책에 따라 패스워드 값에 대한 유효성을 검증한다.

○ TSF 보호

TOE는 암호모듈을 통해 암호통신을 수행함으로써 TOE 구성요소간 통신에 대한 기밀성과 무결성을 보장한다. TOE는 안전한 상태를 유지하고 보안기능이 정상적으로 동작함을 보장하기 위해 시동 시 및 정규 운영 동안 주기적으로 프로세스의 상태를 확인하는 자체 시험을 수행하고 무결성 점검 대상인 TSF 데이터 및 TSF 실행 코드에 대한 무결성 검사를 수행한다.

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·인증지침 (2017. 08. 24.) 정보보호제품 평가인증 수행규정 (2017. 09. 12.)
평가제품	Magic SSO V4.0
보호프로파일	국가용 통합인증 보호프로파일 V1.0 (2017.08.18.)
보안요구사항	없음
보안목표명세서	Magic SSO V4.0 보안목표명세서 v1.4 (2019.10.30.)
평가보고서	Magic SSO V4.0 평가결과보고서 V2.00 (2019.11.12.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈	MagicJCrypto V2.0.0.0
평가신청인	㈜드림시큐리티
개발업체	㈜드림시큐리티
평가기관	한국시스템보증