KECS-CR-23-38

TouchEn Wiseaccess v1.4
인증보고서

인증번호 : KECS-CISS-1244-2023

2023년 6월

IT보안인증사무국

1. 제품 개요

TouchEn Wiseaccess v1.4(이하 TOE)는 일반 사용자에게 한 번의 로그인(Single Sign-On)으로 다양한 업무시스템에 추가적인 로그인 행위 없이 서비스를 제공하는 통합인증 제품으로 소프트웨어 형태로 제공된다.

TOE 및 TOE 구성요소는 다음과 같이 식별된다.

구분		식별정보	형태	배포 방법
TOE		TouchEn Wiseaccess v1.4	-	-
TOE 세부버전		v1.4.4.3		
TOE 구성요소	SSO Server	TouchEn Wiseaccess v1.4 Server v1.4.4.3 (wiseaccess_server_v1.4.4.3_linux.tar.gz)	소프트웨어	CD
	SSO Agent	TouchEn Wiseaccess v1.4 Agent v1.4.4.3 (wiseaccess_agent_v1.4.4.3_linux.tar.gz)		
매뉴얼	관리자 매뉴얼	TouchEn Wiseaccess v1.4 관리자 매뉴얼 v1.4.3 (TouchEn Wiseaccess v1.4 관리자 매뉴얼 v1.4.3.pdf)	PDF	
	API 매뉴얼	TouchEn Wiseaccess v1.4 API 매뉴얼 v1.4.2 (TouchEn Wiseaccess v1.4 API 매뉴얼 v1.4.2.pdf)		
	설치 지침서	TouchEn Wiseaccess v1.4 설치지침서 v1.4.3 (TouchEn Wiseaccess v1.4 설치지침서 v1.4.3.pdf)		

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

구 분			최소 요구사항
SSO Server	하드웨어	CPU	Intel(R) Xeon(R) 2.8 GHz 이상
		RAM	8 GB 이상
		HDD	TOE 설치에 필요한 공간 1 GB 이상
		NIC	100/1000 Ethernet Port 1개 이상
	소프트웨어	운영체제	Oracle Linux 8.7 (64 비트, Kernel 5.15.0)
		DBMS	MySQL 8.0.33
		Java	OpenJDK 1.8.0_372 (64 비트)
		WAS	Apache Tomcat 8.5.88
SSO Agent	하드웨어	CPU	Intel(R) Xeon(R) 2.8 GHz 이상
		RAM	8 GB 이상
		HDD	TOE 설치에 필요한 공간 1 GB 이상
		NIC	100/1000 Ethernet Port 1개 이상

	소프트웨어	운영체제	Oracle Linux 8.7 (64 비트, Kernel 5.15.0)
		Java	OpenJDK 1.8.0_372 (64 비트)
		WAS	Apache Tomcat 8.5.88

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

구 분		최소요구사항
S/W	Browser	Chrome 112.0

TOE에서 사용되는 검증필 암호모듈 상세 정보는 다음과 같다.

구분	세부구분	내용
검증필 암호모듈	암호모듈명	Key# Crypto V1.5
	검증번호	CM-220-2027.11
	개발사	㈜라온시큐어
	검증일	2022년 11월 2일
	효력만료일	2027년 11월 2일

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.

■ 보안 감사

<SSO Server>

SSO Server는 브라우저를 통해 제공되는 TSF 데이터 관리 및 보안관리에 대한 감사데이터를 생성한다. 관리 및 보안설정, TSF 데이터의 정보변경과 식별 및 인증, 무결성 검사, 감사기능의 시작/종료, 보안 위반에 대한 감사데이터가 생성된다.

SSO Server는 보안위반에 따른 대응 행동 및 SSO Server와 SSO Agent 간의 상호인증, 그에 생성되는 암호키 관리, 무결성 검사, 감사기능의 시작/종료에 대한 감사데이터를 생성한다. 생성된 감사데이터는 로그생성시간, 주체의 신원, 사건결과(성공 또는 실패), 사건유형에 대한 항목 및 추가적으로 생성되는 감사데이터를 포함한다.

감사데이터는 DBMS에 저장되어, SSO Server를 통해 인가된 관리자에게 적합한 형식으로 정보를 제공하고 비 인가된 사용자로부터의 데이터를 삭제되지 않도록 보호한다.

최고관리자만 감사데이터 조회가 가능하다.

SSO Server는 관리자가 설정한 알림 주기에 따라 감사데이터 저장소를 주기적으로 검사하여, 경고 알림 임계치를 초과하는 경우 관리자에게 경고 메일을 발송하고 과거 기록 삭제 임계치를 초과하는 경우 DBMS의 과거 기록을 삭제한다.

또한 보안위반(검증필 암호모듈 'Key# Crypto V1.5' 자가시험 실패, 감사저장소 용량 초과, SSO Server, SSO Agent 자가검증 및 무결성 검사 실패, 감사 저장 실패 시, 관리자/일반 사용자 실패 허용 횟수 초과)에 대한 대응 행동(관리자에게 이메일 발송)을 수행한다.

<SSO Agent>

SSO Agent에서는 SSO Agent와 SSO Server와의 상호인증, 암호키를 이용한 인증토큰 생성, 연산, 파기, 암호키 관리, 무결성 검사, 감사기능의 시작/종료에 대한 감사데이터가 생성된다. 생성된 감사데이터는 로그생성시간, 주체의 신원, 사건결과(성공 또는 실패), 사건유형에 대한 항목 및 추가적으로 생성되는 감사데이터를 포함한다.

■ 암호지원

<SSO Server>

SSO Server는 상호인증을 위해 난수발생기를 통해 난수를 생성하고, 상호인증 시 전자서명 알고리즘을 이용하여 서명 검증을 수행한다. 상호인증이 완료되면, 공개키 알고리즘을 이용하여 SSO Agent로 암호키를 분배한다. 이때, 사용되는 알고리즘은 검증필 암호모듈인 Key# Crypto V1.5을 이용한다. 생성된 암호키는

저장되지 않고 파기한다.

<SSO Agent>

SSO Agent는 SSO Server와 상호인증을 위해 난수발생기를 통해 난수를 생성하고, 상호인증 시 전자서명 알고리즘을 이용하여 서명 검증을 수행한다. 상호인증 이후 대칭키 알고리즘과 MAC 알고리즘을 이용하여 인증토큰을 생성, 관리하며, 암호 알고리즘은 검증필 암호모듈인 Key# Crypto V1.5을 이용한다. 생성된 암호키는 저장되지 않고 파기한다.

■ 식별 및 인증

<SSO Server>

식별 및 인증 시도 시에는 아이디로 관리자를 식별하고, 모든 행동 이전에 관리자 인증을 수행한다. 인증을 위한 비밀번호는 'o'로 표시하고 인증 실패 원인 정보만을 제공하므로 비밀번호의 노출을 방지한다.

관리자에 대한 인증정보 재사용 시도를 차단하는 기능을 제공한다.

관리자의 비밀번호는 비밀번호 규칙에 따라 비밀번호를 생성해야 하며, 식별 및 인증 성공 시 관리자는 보안관리 권한을 유지한다.

SSO Server를 통해 인증 시도 시 관리자가 설정한 인증시도실패 횟수를 초과할 경우 관리자가 설정한 계정잠금 시간 동안 계정을 잠근다.

SSO Server와 SSO Agent 구성요소간 안전한 통신을 위해 자체 구현된 프로토콜을 통한 상호인증을 수행한다.

<SSO Agent>

최초 일반 사용자 식별 및 인증 시도 시에는 아이디로 일반 사용자를 식별하고, 모든 행동 이전에 일반 사용자 인증을 수행한다. 인증을 위한 비밀번호는 'o'로 표시하고 인증 실패 메시지만을 제공하므로 비밀번호의 노출을 방지한다.

최초 일반 사용자 식별 및 인증이 완료되면 인증토큰 구현방식에 따라 인증토큰을 생성하며, 이후 인증토큰을 통한 식별 및 인증을 수행한다. 인증토큰은 Onetime Token을 사용하여 재사용을 방지한다. 생성된 인증토큰은 저장되지 않고 파기한다.

일반 사용자 인증 시도 시 인증실패 허용횟수를 초과할 경우 관리자가 설정한 잠금 지속시간 동안 일반 사용자의 계정을 잠근다.

■ 보안 관리

<SSO Server>

인가된 관리자는 SSO Server를 통해 보안관리를 수행한다. 조직/서비스 등을 통해 보안정책을 설정할 수 있으며, 인가된 관리자는 보안관리 인터페이스에 최초 접속 시 패스워드를 강제 변경해야 한다.

인가된 관리자 권한에는 모든 보안관리 기능의 정책 설정 및 수행이 가능한 최고 관리자 하나만 존재한다.

■ TSF 보호

<SSO Server>

SSO Server는 TSF에 의해 통제되는 저장소에 저장되는 TSF 데이터 및 TOE 구성요소간 전송되는 TSF 데이터를 보호하고, TSF 자체시험을 통하여 주요 보안 기능 프로세스 등에 대한 점검을 수행한다. 또한, 주요 프로세스에 대해 시동 시, 운영 중 주기적으로 자체시험을 수행하며, TOE 설정파일 및 주요 프로세스에 대한 무결성 검사를 시동 시, 운영 중 주기적으로 수행한 후 무결성이 손상된 경우 관리자에게 경보메일을 발송한다. 또한 TSF 데이터 보호를 위해 일반 사용자 및 관리자 인증정보 등을 DBMS에 안전하게 저장하여 관리한다.

<SSO Agent>

SSO Agent는 TSF에 의해 통제되는 저장소에 저장되는 TSF 데이터 및 TOE 구성요소간 전송되는 TSF 데이터를 보호하고, TSF 자체시험을 통하여 주요 보안 기능 프로세스 등에 대한 점검을 수행한다. 또한, 주요 프로세스에 대해 시동 시, 운영 중 주기적으로 자체시험을 수행하며, TOE 설정파일 및 주요 프로세스에 대한 무결성 검사를 시동 시, 운영 중 주기적으로 수행한 후 무결성이 손상된 경우 관리자에게 경보메일을 발송한다.

인증토큰은 일반 사용자의 브라우저를 통해 PC 메모리에 임시로 적재하고 사용 후 즉시 파기한다.

■ TOE 접근

<SSO Server>

SSO Server를 비활동 기간 동안 사용하지 않을 경우 자동으로 세션을 종료하는 기능을 수행하며, 재사용을 위해서는 재인증이 필요하다.

또한, 보안관리를 위한 관리자 세션의 경우 세션 연결의 최대 수를 1개로 제한하여 중복 로그인을 방지한다. 인가된 관리자 로그인 후 다른 관리자 PC에서 동일 계정으로 로그인 시도 시 기존 접속을 종료하는 기능을 제공한다.

관리자 허용 IP 주소는 2개까지 설정이 가능하며, 허용된 IP 이외에서 접근할 경우 오류 문구를 출력한다.

<SSO Agent>

일반 사용자 식별 및 인증 이후 인증토큰의 유휴시간을 초과할 경우 세션 종료를 수행하고, 이후 재인증을 통해서 식별 및 인증을 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·인증 등에 관한 고시 (2022. 10. 31.) 정보보호제품 평가·인증 수행규정 (2021. 5. 17.)
평가제품	TouchEn Wiseaccess v1.4
보호프로파일	국가용 통합인증 보호프로파일 V1.1 (2019. 12. 11.)
보안요구사항	없음
보안목표명세서	TouchEn Wiseaccess v1.4 보안목표명세서 v1.4.4 (2023. 5. 31.)
평가보고서	TouchEn Wiseaccess v1.4 평가결과보고서 V2.00 (2023. 5. 31.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈 (탑재 필수)	Key# Crypto V1.5
평가신청인	라온시큐어㈜
개발업체	라온시큐어㈜
평가기관	한국시스템보증