KECS-CR-23-31

OTACToken V1.0
인증보고서

인증번호 : KECS-CISS-1237-2023

2023년 5월

IT보안인증사무국

1. 제품 개요

OTACToken V1.0(이하 'TOE')는 1회성 무작위 고유식별 인증코드를 이용한 인증 기능을 제공하는 제품이다. TOE는 다양한 업무서비스에 사용자가 모바일 디바이스를 통해 업무시스템에 접근할 수 있도록 해주는 간편인증 솔루션으로, 소프트웨어 형태로 제공된다. TOE 및 TOE 구성요소에 대한, 식별정보 및 배포 형태는 [표 1]과 같다.

구분		종류	형태	배포
구성 요소	OTACToken Server	OTACToken Server V1.0.02 : OTACToken Server V1.0.02.tar	S/W	CD
	OTACToken App(Android)	OTACToken App(Android) V1.0.02 : OTACToken App(Android) V1.0.02.apk		
	OTACToken App(iOS)	OTACToken App(iOS) V1.0.02 : OTACToken App(iOS) V1.0.02.ipa		
설명서		OTACToken V1.0 관리자 매뉴얼 V1.4 : OTACToken V1.0 관리자 매뉴얼 V1.4.pdf OTACToken V1.0 사용자 매뉴얼 V1.4 : OTACToken V1.0 사용자 매뉴얼 V1.4.pdf OTACToken V1.0 설치지침서 V1.4 : OTACToken V1.0 설치지침서 V1.4.pdf	전자 문서 (PDF)	

[표 1] TOE 및 TOE 구성요소 식별정보

OTACToken Server가 설치 및 운영되는 하드웨어 및 소프트웨어 최소 요구사항은 아래 [표 2]과 같다.

구분		최소 요구사항
HW	CPU	Intel(R) Core(TM) i5-6400 CPU @ 2.70 GHz 4 core 이상
	Memory	8 GB 이상
	HDD	TOE 설치에 필요한 공간 150 MB 이상
	NIC	10/100/1000 Mbps * 1 EA 이상
SW	OS	Ubuntu 18.04 (64 bit) (kernel 5.4.0-139)

	DBMS	MariaDB 10.11.2
	WAS	Apache Tomcat 9.0.73
	JRE	jre 1.8.0_362

[표 2] OTACToken Server 설치 최소 요구사항

OTACToken APP(Android)가 설치되어 운영되는 시스템 요구사항은 아래 [표 3]과 같다.

제품명	모델명	OS	
		버전	커널 버전
SAMSUNG Galaxy S22	SM-S901N	13	5.10.81

[표 3] OTACToken APP(Android) 설치 시스템 요구사항

OTACToken APP(iOS)가 설치되어 운영되는 시스템 요구사항은 아래 [표 4]와 같다.

제품명	모델명	OS	
		버전	커널 버전
iPhone 13	A2633	15.4.1	-

[표 4] OTACToken APP(iOS) 설치 시스템 요구사항

보안관리를 수행하기 위해 요구되는 관리자 PC의 시스템 요구사항은 아래 [표 5]와 같다.

구분		요구사항
S/W	웹브라우저	Google Chrome 108.0

[표 5] 관리자 PC의 S/W 요구사항

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

OTACToken Server는 웹 브라우저를 통해 제공되는 TSF데이터 관리 및 보안관리에 대한 감사데이터를 생성한다. 보안관리 및 보안설정, TSF 데이터의 정보변경과 식별 및 인증, 무결성 검사, 감사기능의 시작/종료, 보안 위반에 대한 감사데이터가 생성된다. 생성된 감사데이터는 생성시간, 주체의 신원, 사건결과, 사건유형에 대한 항목 및 추가적으로 생성되는 감사데이터를 포함한다. 감사데이터는 DBMS에 저장되어 있으며, 웹 브라우저를 통해 인가된 관리자에게 적합한 형식으로 정보를 제공한다.

○ 암호지원

OTACToken Server는 난수생성기를 통해 대칭키를 생성하고, 생성된 대칭키를 이용하여 OTAC 정보값을 암호화한다. 암호화한 데이터를 업무시스템으로 전달한다.

- 난수생성기 : SP 800-90A HMAC DRBG
- 대칭키 알고리즘 : AES 128 Bit

OTACToken APP(Android)와 OTACToken APP(iOS)는 QRCODE로 제공되는 OTAC 정보값을 읽어들여 복호화한다. 새로운 대칭키를 생성하여 OTAC 정보값을 암호화하여 APP 저장공간에 저장한다.

- 공개키 알고리즘 : RSA 2048 Bit
- 대칭키 알고리즘 : AES 128 Bit

사용자의 인증을 위해 OTAC 코드 생성 요청 시 저장되어 있는 OTAC 정보값을 대칭키로 복호화여 OTAC 데이터를 제공한다.

○ 식별 및 인증

OTACToken Server는 식별 및 인증 시도 시에는 아이디로 관리자를 식별하고, 모든 행동 이전에 관리자 인증을 수행한다. 인증을 위한 비밀번호는 '•'로 표시하고 인증 실패 원인 정보만을 제공하므로 비밀번호의 노출을 방지한다. 관리자의 비밀번호는 비밀번호 규칙에 따라 비밀번호를 생성해야 하며, 식별 및 인증 성공 시 관리자는 보안관리 권한을 유지한다. 웹 브라우저를 통해 인증 시도 시 인증 시도실패 횟수를 초과할 경우 5분 동안 계정을 잠근다.

○ 보안관리

OTACToken Server는 서비스 별 보안정책을 설정하고, 관리자 및 등록된 사용자를 관리한다

○ TSF 보호

OTACToken Server와 웹 브라우저의 보안통신으로 TSF 데이터 전송 시 노출, 변경으로부터 보호하며, 저장소에 저장되는 정보 역시 비인가된 노출, 변경으로부터 보호하며, 시동 시, 이후 주기적으로 무결성 검사 및 자체시험을 수행한다.

○ TOE 접근

관리자는 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.

○ 안전한 경로

OTACToken Server는 원격 사용자가 안전한 경로를 통하여 통신 데이터를 변경, 노출로부터 보호하는 통신 경로를 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.) 정보보호제품 평가인증 수행규정 (2021. 05. 17.)
평가제품	OTACToken V1.0
보호프로파일	없음
보안요구사항	없음
보안목표명세서	OTACToken V1.0 보안목표명세서 V1.7 (2023.04.24.)
평가보고서	OTACToken V1.0 평가결과보고서 V2.00 (2023.04.25.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈 (탑재 필수)	없음
평가신청인	㈜센스톤
개발업체	㈜센스톤
평가기관	한국시스템보증