

KECS-CR-21-14

HEDES v1.0 인증보고서

인증번호 : KECS-CISS-1084-2021

2021년 3월



IT보안인증사무국

1. 제품 개요

HEDES v1.0(이하 TOE)는 관리하는 DB내의 사용자 데이터를 암호·복호화한다. 사용자 데이터는 암호화되어 DB에 저장 되기 전후의 데이터로, 일반적으로 조직에서 관리하는 개인 정보 및 민감한 정보와 같은 위협으로부터 보호해야하는 조직의 기밀 데이터를 포함한다. TOE 및 TOE 구성요소에 대한, 식별정보 및 배포형태는 [표 1]과 같다.

구분	종류		형태	배포
TOE 명	HEDES v1.0		-	
세부 버전	20210129-001		-	
TOE 구성 요소	정책관리 서버	HEDES 정책관리 서버 v1.0-20210129-001 (hedes_policy_server_1.0_002.tar)	S/W	CD
	에이전트 서버	HEDES 에이전트 서버 v1.0-20210129-001 (hedes_agent_server_1.0_002.tar)		
매뉴얼	준비절차서	HEDES v1.0 준비절차서 v1.3 (hds_pre_004.pdf)	전자 문서 (PDF)	
	사용자운용 설명서	HEDES v1.0 사용자운용설명서 v1.3 (hds_ope_004.pdf)		

[표 1] TOE 및 TOE 구성요소 식별정보

TOE에서 사용하는 검증필 암호모듈은 아래와 같다.

구분	내용
암호모듈명	MagicCrypto V2.2.0
검증번호	CM-162-2025.3
개발사	S/W
검증일	2020년 3월 3일
효력만료일	2025년 3월 3일

[표 2] TOE에서 사용하는 검증필 암호모듈

TOE가 설치 및 운영되는 하드웨어 및 소프트웨어 최소 요구사항은 아래의 [표 3]과 같다.

구분		최소 요구사항	
HEDES 정책관리 서버 / HEDES 에이전트 서버	H W	CPU	Intel Xeon CPU E3-1220 @ 3.10 Ghz (4 Core) 이상
		Memory	16 GB 이상
		HDD	TOE 설치에 필요한 공간 300 GB 이상
		NIC	10/100/1000 Mbps 1개 이상
	SW	OS	CentOS 7.9 (kernel v3.10, 64 bit)
		DBMS	MySQL 5.7
		etc	Java(JRE) 1.8.0_281 Jetty 9.4.36

[표 3] TOE 설치 요구사항

인가된 관리자가 보안 관리 기능을 수행하기 위한 시스템의 최소 요구사항은 아래의 [표 4]와 같다.

구분		최소요구사항
SW	Web Browser	Google Chrome 88

[표 4] 관리자 PC 요구사항

또한, TOE의 운영을 위해 연동되는 외부 IT 실체는 [표 5]과 같다.

구분	내용
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

TOE는 감사정보를 인가된 관리자에게만 검색 및 조회 기능을 제공하고 날짜, 시간, IP, 사건 유형, 사건 주체 및 사건 내역 등의 감사정보를 제공한다. 감사 대상 사건 발생 시 감사 데이터를 생성하고 잠재적인 위반 사항을 탐지하여, 인가된 관리자에게 경고 메일을 발송한다.

● 암호지원

TOE는 암호모듈 검증제도를 통해 안전성 및 구현적합성이 확인된 검증필 암호모듈을 통해 제품 운영에 사용되는 모든 암호키를 안전하게 생성, 폐기하고 암호 알고리즘을 정의한 암호정책에 따라 암호 연산을 수행한다.

● 사용자 데이터 보호

보호대상 DBMS내에 저장되는 사용자 데이터를 보호하기 위해 검증필 암호모듈을 사용하여 암호화하여 저장한다. 인가된 관리자가 설정한 보안정책에 따라 블록암호화 알고리즘 통해 압복호화를 수행한다. 추가적으로, 해시알고리즘을 통해 단방향 암호화를 지원한다.

● 식별 및 인증

TOE는 보안 관리 기능을 수행하는 관리자에 대해 식별 및 인증 기능을 제공하며 인증 데이터 입력 시 인증 피드백을 보호하는 기능을 제공한다. 추가로 비밀번호 조합규칙을 통해 허용기준을 검증한다.

● 보안관리

TOE는 인가된 관리자에게 정책 관리, 관리자 관리, 환경 설정 등의 보안 관리 기능을 제공하며, 인가된 관리자는 보안관리 인터페이스를 통해 보안 관리를 수행한다.

● TSF 보호

TOE는 TSF에 의해 통제되는 저장소에 저장되는 TSF 데이터 및 TOE 구성요소간 전송되는 TSF 데이터를 보호하고, TSF 자체시험을 통하여 주요 보안기능 프로세스 등에 대한 점검을 수행한다.

● TOE 접근

TOE의 보안 관리 기능 수행을 위해 접근 가능한 관리자의 관리접속 세션의 경우 동시 세션의 최대 수를 제한하며, 동일한 계정으로 새로운 접속이 수행되는 경우 기존 세션을 종료하고 감사데이터를 생성한다.

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	HEDES v1.0
보호프로파일	국가용 데이터베이스 암호화 보호프로파일 V1.1 (2019.12.11.)
보안요구사항	없음
보안목표명세서	HEDES v1.0 보안목표명세서 V1.4 (2021.01.29.)
평가보고서	HEDES v1.0 평가결과보고서 V1.00 (2021.02.22.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈	MagicCrypto V2.2.0
평가신청인	(주)휴메인시스템
개발업체	(주)휴메인시스템
평가기관	한국시스템보증