KECS-CR-21-10

ShadowCube V7.0
인증보고서

인증번호 : KECS-CISS-1080-2021

2021년 3월

IT보안인증사무국

1. 제품 개요

ShadowCube V7.0(이하 "TOE"라 함)은 조직에서 관리되는 중요 문서를 보호하기 위한 목적으로 사용된다. 중요 문서를 보호하기 위해 인가된 관리자가 설정한 문서그룹 정책에 따라 해당 그룹에 속한 문서를 암호화하여 해당 문서 그룹 사용자의 요청 시 문서를 복호화하는 소프트웨어 형태의 문서암호화 제품이다.
TOE는 정책센터, 클라이언트로 구성된다. 정책센터는 TOE의 암·복호화 정책 설정 등 인가된 관리자가 보안관리를 수행할 수 있는 기능을 제공하며, 클라이언트는 사용자 문서에 대한 암·복호화 기능을 수행하는 기능을 제공한다. TOE의 참조는 다음과 같이 식별된다.

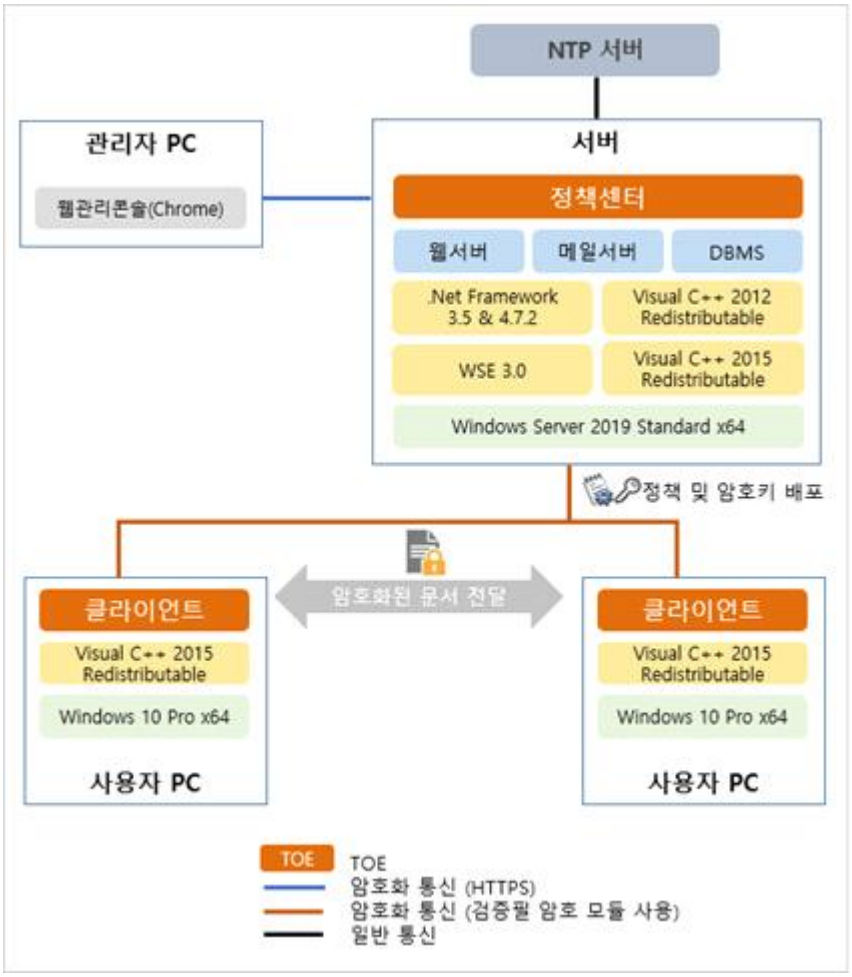
구분		식별자	배포형태
TOE명		ShadowCube V7.0	CD 1부
TOE 구성요소	정책센터	- 정책센터 7.0.7.1409 설치파일 : server_7.0.7.1409.exe	
	클라이언트	- 클라이언트 7.0.7.1409 설치파일 : scsetup_7.0.7.1409.exe	
매뉴얼	관리자 운영설명서	ShadowCube V7.0 관리자 운영 설명서 V1.4.pdf	
	사용자 설명서	ShadowCube V7.0 사용자 설명서 V1.4.pdf	
	준비 절차서	ShadowCube V7.0 준비 절차서 V1.5.pdf	

TOE에 포함되어 함께 배포 및 설치되어 운영되는 3rd Party 요소는 다음과 같다.
- 정책센터 설치파일(server_7.0.7.1409.exe)
  - 검증필 암호모듈 : MagicCrypto V2.2.0
  - 암호 지원 라이브러리 : OpenSSL 1.1.1i
- 클라이언트 설치파일(scsetup_7.0.7.1409.exe)
  - 검증필 암호모듈 : MagicCrypto V2.2.0

TOE에서 사용하는 검증필 암호모듈의 정보는 다음과 같다.

구분	세부구분	내용
검증필 암호모듈	암호모듈명	MagicCrypto V2.2.0
	검증번호	CM-162-2025.3
	개발사	㈜드림시큐리티
	검증일	2020. 3. 3.

TOE 운영환경은 다음과 같다.



TOE는 사용자 단말 암호화 방식을 통해 보안기능을 수행하며 정책센터와 클라이언트로 구성된다. 검증필 암호모듈(MagicCrypto V2.2.0)을 탑재하여 암호 통신을 한다. 정책센터는 문서그룹 정책 및 암호키를 관리하며, 관리자는 관리자 PC의 웹 브라우저(Chrome)를 통해 설정한 문서그룹 정책 및 암호키를 클라이언트에게 전송한다. 클라이언트는 정책센터로부터 전달받은 문서그룹 정책 및 권한을 통해 보호대상 문서를 검증필 암호모듈을 사용하여 암·복호화를 수행할 수 있으며, 암·복호화된 문서는 사용자 단말에 파일 형태로 저장된다.

TOE 운영 시 TOE 이외에 요구되는 하드웨어, 소프트웨어는 다음과 같다.

구분	최소 요구사항	
정책센터	CPU	Intel i7 Quad Core 2.0GHz 이상
	Memory	8GB 이상
	HDD	TOE 설치에 필요한 공간 600MB 이상
	NIC	100/1000 Mbps X 1Port 이상
	OS	Microsoft Windows Server 2019 Standard (64bit)
	DBMS	PostgreSQL 12.5

구분	최소 요구사항	
	필수 S/W	IIS (Internet Information Services) 10.0
		SMTP Virtual Server 10.0
		Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030
		Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030
		Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215
		Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215
		Microsoft .NET Framework 3.5
		Microsoft .NET Framework 4.7.2
		WSE (Web Service Enhancements) 3.0
		Chrome 88.0
클라이언트	CPU	Intel i3 Dual Core 1.0GHz 이상
	Memory	4GB 이상
	HDD	TOE 설치에 필요한 공간 180MB 이상
	NIC	100/1000 Mbps X 1Port 이상
	OS	Microsoft Windows 10 Pro (64bit)
	필수 S/W	Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24215
		Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215
		MS Notepad, MS WordPad, MS Paint
		Microsoft Office 2007, 2010, 2013, 2016, 2019
		Hancom Office 2010, 2014(VP), NEO, 2018, 2020
		Acrobat Reader 11, DC
		Autodesk AutoCAD 2019, 2020, 2021
관리자 PC	웹브라우저	Chrome 88.0

TOE 운영을 위해 연동되는 외부 IT 실체는 다음과 같다.

구분	내용
NTP 서버	감사데이터 생성 시 신뢰할 수 있는 타임스탬프를 제공함으로써 시간동기화를 위해 사용됨

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

2. 주요기능

TOE가 제공하는 보안기능은 다음과 같다.

■ 사용자 데이터 보호

TOE는 인가된 관리자가 설정한 문서그룹 기반 및 보안속성 접근통제정책에 기반하여 보호대상 문서에 대한 읽기 및 저장, 암·복호화 기능을 제공한다.

응용 프로그램	응용 프로그램 버전	문서 유형(확장자)
MS Office Word	2007, 2010, 2013, 2016, 2019	doc, docx
MS Office Excel	2007, 2010, 2013, 2016, 2019	xls, xlsx
MS Office Powerpoint	2007, 2010, 2013, 2016, 2019	ppt, pptx
Hancom Office 한글	2010, 2014(VP), NEO, 2018, 2020	hwp, hwpx
Hancom Office 한셀	2010, 2014(VP), NEO, 2018, 2020	nxl, cell
Hancom Office 한쇼	2010, 2014(VP), NEO, 2018, 2020	show
Acrobat Reader DC	11, DC	pdf
Autodesk AutoCAD	2019, 2020, 2021	dwg, dxf
메모장 (Notepad)	클라이언트 운영환경인 Windows 10 Pro x64에서 기본 제공하는 버전	txt
그림판 (MS Paint)		bmp, gif, jpg, png, tif
워드패드 (Wordpad)		rtf

■ 식별 및 인증

TOE는 TOE 구성요소간 상호인증을 수행하고, 관리자 신원은 관리 ID/패스워드 및 E-mail 인증코드 기반 식별 및 인증 기능을 제공하며 클라이언트는 문서 사용자의 인증서 기반 식별 및 인증 기능을 제공한다. 패스워드 생성시, 영문자/특수문자/숫자를 조합해야 하며, 길이는 9 ~ 16 문자 이내로 설정할 수 있다. TOE는 인증 피드백 보호를 위해 패스워드를 화면에서 볼 수 없도록 마스킹 처리한다. 또한 식별 및 인증 실패 시, 실패 이유에 대한 피드백을 제공하지 않는다. 인증시도 3회(기본 값) 실패시, 5분간(고정 값) 잠금기능 및 사용자 PC 재부팅 완료시까지 잠금 기능을 제공한다.

■ 보안관리

TOE는 인가된 관리자가 보안정책 및 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공한다. 인가된 관리자는 웹 브라우저(Chrome)를 통해 보안관리 기능을 수행한다.

■ 보안감사

TOE는 정의된 감사대상 사건들에 대하여 감사 레코드를 생성하고 기록한다. 감사 레코드 생성 시 감사대상 사건 일시, 사건 유형, 신원, 사건 결과 등이 기록된다.

정책센터 및 클라이언트에서 생성된 감사 레코드는 정책센터가 설치된 서버의 DBMS에 저장된다. 또한, 인가된 관리자가 감사데이터를 조회할 수 있는 기능을 제공한다. TOE는 잠재적인 보안 위반을 탐지한 경우 인가된 관리자에게 E-mail을 통한 알람을 제공한다. 감사 증적이 감사 저장소 용량의 기본 값 60%를 초과할 경우 인가된 관리자에게 E-mail으로 통보하고, 감사 증적이 포화인 용량의 기본 값 70%인 경우 가장 오래된 감사데이터를 덮어쓰기 한다.

■ 암호지원

TOE는 구성요소 간 전송 데이터 보호, TSF 데이터 보호 및 문서 암·복호화를 위해 암호 키 생성, 분배, 파기 기능 및 암호연산 기능을 제공한다. TOE는 암호모듈검증제도(KCMVP)를 통해 안전성 및 구현적합성이 확인된 검증필 암호모듈(MagicCrypto V2.2.0)의 검증대상 암호 알고리즘을 사용하여 암호 키 생성, 분배 및 연산을 수행한다. 암호키가 더 이상 필요하지 않은 경우 암호키는 파기 되며, 문서 암호화에 사용된 암호키는 복호화 및 암호화된 문서가 삭제될 때 문서와 함께 파기 되고, 그 외의 용도로 생성된 암호키는 키 제로화(Zeroization)의 방법으로 0으로 덮어 씌워 암호키를 파기한다.

■ TOE 접근

TOE는 등록된 IP에서만 보안관리 인터페이스에 접속할 수 있도록 TOE 접근을 제어하며, 동시 접속 세션의 최대 수를 1로 제한한다. 동시접속 시도 시 이전에 접속한 관리자의 세션이 종료된다. TOE는 인가된 관리자가 로그인 이후 유휴시간(기본 값 10분) 간 활동이 없을 경우 세션을 종료한다.

■ TSF 데이터 보호

TOE는 구동 시/ 주기적으로 주요 프로세스에 대한 자체시험을 수행하고 구동 시/주기적으로/인가된 관리자 요청 시 TOE 실행 파일 등에 대한 무결성을 검증하여 검증에 실패 하는 경우 관리자에게 실시간으로 통보한다. TOE의 분리된 부분 간에 TSF 데이터가 전송될 때 노출, 변경으로부터 보호하기 위해 검증필 암호모듈을 사용하여 전송 TSF 데이터를 보호하고, TSF데이터 저장소에 저장되는 인가된 관리자 및 사용자의 패스워드, 암호키, 핵심보안매개변수, TOE 설정 값(보안정책, 환경설정 매개변수), 감사 데이터 등을 비인가된 노출, 변경으로부터 보호한다.

3. 평가결과 요약

TOE에 대한 평가는 한국정보통신기술협회에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부를 만족하고 국가용 보호프로파일을 준수하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가·인증지침 (2017. 8. 24.) 정보보호제품 평가인증 수행규정 (2017. 9. 12.)
평가제품	ShadowCube V7.0
보호프로파일	국가용 문서 암호화 보호프로파일 V1.1 (2019.12.11)
보안요구사항	없음
보안목표명세서	ShadowCube V7.0 보안목표명세서 V1.9 (2021.02.04.)
평가보고서	ShadowCube V7.0 평가결과보고서 V1.5 (2021.02.25.)
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	㈜두루안
개발업체	㈜두루안
평가기관	한국정보통신기술협회