

ShadowCube V8.0

인증보고서

인증번호 : KECS-CISS-1415-2026

2026년 7월



IT보안인증사무국

1. 제품 개요

ShadowCube V8.0(이하 'TOE')은 문서 암호화 제품으로 조직에서 관리되는 중요 문서를 보호하기 위한 목적으로 사용된다.

TOE가 제공하는 주요 보안기능은 보호대상 문서의 암호·복호화 및 암호키 관리, TOE에서 사용하는 핵심보안 매개변수에 대한 암호·복호화 및 암호키 관리이며 이때 적용되는 암호 기능은 검증필 암호모듈(MagicCrypto V2.3.0)의 검증대상 알고리즘이 사용된다.

TOE 및 TOE 구성요소는 다음과 같다.

구성	세부항목	배포형태
TOE	ShadowCube V8.0	-
TOE 구성요소	ShadowCube Server 8.0.0.4517 (server_8.0.0.4517.exe)	실행파일 (CD 1부)
	ShadowCube Client 8.0.0.4517 (scsetup_8.0.0.4517.exe)	
설명서	관리자 운영설명서: ShadowCube V8.0 관리자 운영설명서 V1.2.pdf	전자파일 (CD 1부)
	사용자 설명서: ShadowCube V8.0 사용자 설명서 V1.2.pdf	
	준비절차서: ShadowCube V8.0 준비절차서 V1.3.pdf	

검증필 암호모듈은 TOE의 각 구성요소에 탑재되어 있으며 식별정보는 다음과 같다.

구분	내용
암호모듈명	MagicCrypto V2.3.0
검증번호	CM-263-2030.1
개발사	(주)드림시큐리티
검증일	2025년 01월 24일
효력만료일	2030년 01월 24일

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

구분			최소 요구사항	비고
Server	H/W	CPU	Intel i7 Quad Core 2.0 GHz 이상	-
		HDD	TOE 설치에 필요한 공간 600 MB 이상	-
		RAM	8 GB 이상	-
		NIC	100/1000 Mbps 이상	-
	S/W	OS	Microsoft Windows Server 2022 Standard (64bit)	Server의 지원 운영체제
		3rd Party S/W	IIS (Internet Information Services) 10.0 Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 Microsoft .NET Framework 4.8 Chrome 149.0 PostgreSQL 18.4	Server 구동에 필요한 제 3자 제공 소프트웨어
Client	H/W	CPU	Intel i3 Dual Core 1.0 GHz 이상	-
		HDD	TOE 설치에 필요한 공간 180 MB 이상	-
		RAM	4 GB 이상	-
		NIC	100/1000 Mbps 1 Port 이상	-
	S/W	OS	Microsoft Windows 11 Pro (64bit)	Client의 지원 운영체제
		3rd Party S/W	Microsoft Visual C++ v14 Redistributable (x86) - 14.50.35719 Microsoft Visual C++ v14 Redistributable (x64) - 14.50.35719 MS Office 2024 한컴 오피스 2024 Adobe Acrobat Reader DC Autodesk AutoCAD 2026	Client 구동에 필요한 제 3자 제공 소프트웨어

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

구분	내용
Chrome 149.0	보안관리 기능을 위한 WEB GUI 제공

문서 암호화가 지원되는 문서 처리 프로그램 별 문서 유형은 다음과 같다.

응용 프로그램	응용 프로그램 버전	문서 유형(확장자)
메모장 (Notepad)	ShadowCube Client 운영환경인 Windows 11 Pro x64에서 기본 제공하는 버전	txt
그림판 (Mspaint)		bmp, gif, jpg, png, tif
워드패드 (Wordpad)		rtf
MS Office Word	2024	doc, docx
MS Office Excel	2024	xls,xlsx
MS Office Powerpoint	2024	ppt, pptx
Hancom Office 한글	2024	hwp, hwpk
Hancom Office 한셀	2024	nxl, cell
Hancom Office 한쇼	2024	show
Acrobat Reader DC	DC	pdf
Autodesk AutoCAD	2026	dwg, dxf

TOE에 포함되는 3rd party 소프트웨어는 다음과 같다.

3 rd party 소프트웨어	설명
OpenSSL 3.5.4	TOE에 포함된 3rd-party 모듈로 관리자와 ShadowCube Server 간의 웹 관리 접속 통신 시 사용
MagicCrypto V2.3.0	TOE에 포함된 3rd-party 모듈로 보호대상 문서의 암호·복호화 및 암호키 관리, 핵심보안매개변수에 대한 암호·복호화 및 암호키 관리를 위해 사용되는 검증필 암호모듈

2. 주요 기능

TOE가 제공하는 주요 보안기능은 다음과 같다.

■ 보안감사

TOE는 모든 보안기능 수행내역에 대한 감사 데이터를 생성한 후, 잠재적 보안위반 사건 발생 시 인가된 관리자에게 메일을 발송하여 경고하고 감사 기록한다.

TOE는 TOE 구성요소 별 감사 데이터를 다음과 같이 생성한다.

ShadowCube Server

- 감사기능의 시작/종료
- 관리자에 대한 식별 및 인증 성공/실패
- 제품 설정 변경 내역
- 보안기능 수행 내역

ShadowCube Client

- 감사기능의 시작/종료
- 객체에 대한 오퍼레이션 수행
- 문서사용자에 대한 식별 및 인증 성공/실패
- TSF 자체 시험의 결과와 무결성 검증 결과

감사 데이터는 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패)를 상세히 포함한다.

인가된 관리자는 GUI 인터페이스를 통해 TOE로부터 생성된 모든 감사 데이터를 검토할 수 있다. 감사 레코드는 인가된 관리자가 정보를 해석하기 적합하도록 생성되며 AND, OR 등 논리적 관계 기준에 따른 선택적인 검토가 가능하다.

TOE는 감사 데이터 손실 예측 시 감사 데이터를 생성하고 인가된 관리자에게 E-mail 전송을 취하며, 감사 데이터 손실을 대비하기 위해 감사 증적 저장소 포화 시 가장 오래된 레코드를 덮어쓰기하고 인가된 관리자에게 E-mail 전송하는 기능을 제공한다.

■ 암호지원

TOE는 보안 정책에 따라 TSF 데이터에 대한 암호·복호화 알고리즘을 적용하기 위하여 검증된 암호모듈인 드림시큐리티의 MagicCrypto V2.3.0을 사용하며, 이를 통해 비밀성, 무결성 및 인증을 보증한다.

암호키 생성 및 암호키 분배 시 사용되는 암호·복호화 알고리즘과 암호키 길이는

다음과 같으며, 메모리에 로드된 암호키 및 핵심매개변수가 더 이상 사용되지 않는 경우, 제로화 처리하여 파기한다.

ShadowCube Client: 문서 암호화

- ARIA_CTR 128 bits

ShadowCube Client: 문서파일의 작성자 및 ShadowCube Client 로그 생성자의 서명 검증

- RSA-PSS

ShadowCube Server, ShadowCube Client: TSF 데이터 및 통신 데이터 암호화

- ARIA_CBC 256 bits
- RSAES 2048 bits

ShadowCube Server, ShadowCube Client: HASH 생성

- SHA-256

ShadowCube Server, ShadowCube Client: 암호키 분배

- ARIA_CBC 256 bits

ShadowCube Server, ShadowCube Client: TOE 구성요소 간 상호인증 키 합의

- ECDH

ShadowCube Server, ShadowCube Client: KEK 생성

- PBKDF2

ShadowCube Server, ShadowCube Client: 난수 생성

- HASH_DRBG

■ 문서 암호화

TOE 구성요소인 ShadowCube Server는 문서 사용자가 보호대상 문서의 암호화를 수행하기 위해 필요한 문서그룹 기반 접근통제 정책을 인가된 관리자가 정의할 수 있다. TOE 구성요소인 ShadowCube Client는 인가된 관리자가 설정한 문서그룹 기반 접근통제 정책에 기반하여 보호대상 문서에 대한 읽기, 암호화(쓰기), 복호화 기능을 제공한다.

■ 식별 및 인증

TOE는 GUI 인터페이스를 통해 관리자나 문서사용자의 신원을 식별 및 인증하고, 인증 실패 시 접근을 제한한다. 식별 및 인증 실패 시 실패 이유에 대한 피드백(ID 오류, 패스워드 오류 등)을 제공하지 않는다. 관리자나 문서 사용자의 인증정보는

재사용할 수 없도록 처리한다. 관리자가 구성한 인증 실패 횟수에 도달하면, 관리자의 경우 5분 동안 인증을 비활성화하고, 문서 사용자의 인증을 시스템 재부팅 시까지 비활성화한다.

TOE는 ShadowCube Server와 ShadowCube Client 간 통신 시 검증필 암호모듈에서 제공하는 ECDH 알고리즘을 통해 상호 인증을 수행한다.

관리자나 문서 사용자의 패스워드는 9자리 이상, 16자리 이하의 길이로 구성되어야 하며 영문 대/소문자, 숫자, 특수문자의 4가지 조합으로 구성할 것을 요구한다.

TOE는 관리자 ID 및 E-mail 인증코드를 통하여 관리자를 식별 및 인증을 하고, 문서 사용자 인증서를 통하여 문서 사용자를 식별 및 인증을 한다. 또한, 인증이 진행되는 동안 관리자 및 사용자에게 패스워드를 보이지 않도록 한다.

■ 보안관리

TOE는 인가된 관리자가 GUI 인터페이스를 통해 보안 기능, 보안 정책, 보안 역할 등을 설정 및 관리할 수 있는 기능을 제공한다.

■ TSF 보호

TOE는 TOE의 분리된 부분 간에 TSF 데이터가 전송될 때 해당 TSF 데이터를 검증필 암호모듈로 암호화하여 노출, 변경으로부터 TSF 데이터를 보호한다. 또한, TOE에 의해 통제되는 저장소에 저장되는 TSF 데이터를 검증필 암호모듈로 암호화하여 비인가된 노출, 변경으로부터 보호한다.

TOE 구성요소인 ShadowCube Server는 시동 시, 정규 운영 중 주기적으로 인가된 관리자 요구 시 자체시험 및 무결성 검사를 진행한다. TOE 구성요소인 ShadowCube Client는 시동시, 정규 운영 중 주기적으로 TOE 주요 프로세스에 대한 자체 시험, TSF 데이터와 TSF에 대한 무결성 검증 기능을 수행한다.

TOE 구성요소인 ShadowCube Client의 환경설정 파일 및 실행 파일에 대한 비인가된 삭제 및 접근통제 정책을 하고, 실행 파일의 비인가된 종료를 방지한다.

TOE 구성요소인 ShadowCube Server와 ShadowCube Client는 버전정보를 조회할 수 있는 기능을 제공한다.

■ TOE 접근

TOE는 GUI 인터페이스를 통해 로그인된 인가된 관리자의 세션 만료 시간이 초과한 경우 세션 종료 기능을 수행한다. 또한 인가된 관리자가 스스로 세션을 종료할 수 있는 기능을 제공한다.

TOE는 관리자 세션을 1개로 제한하며, 관리자의 관리 접속 후 다른 단말에서 로

그인 수행되는 경우 신규 접속 세션은 허용하고 이전 접속 세션은 차단한다.

사전에 등록된 IP 주소에서만 ShadowCube Server에 접속할 수 있도록 제한한다. IP 주소는 인가된 관리자가 설정한 접속 가능 IP 개수만큼 등록할 수 있다.

※ 상기 제품은 인증서에 명시된 국가용 보안요구사항 제품 유형으로 인증되었으며, 국가용 보안요구사항을 준수하여 구현된 보안기능에 대한 세부 설명, 제품의 운영 환경 및 국가용 보안요구사항에 포함되지 않은 부가기능은 설명서를 참조한다. 관련 부가기능은 설명서에 기반하여 기능시험 되었으며, 제품 취약성 분석 시 포함되었다. 다만, 부가기능은 인증된 제품 유형과 무관하다.

3. 평가결과 요약

TOE에 대한 평가는 (재)한국화학융합시험연구원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부를 만족하고, 국가용 보호프로파일을 준수하여 공통평가기준 1부 13.7.3에 따라 “통과” 한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가·인증 등에 관한 고시(2022. 10. 31.) 정보보호제품 평가·인증 수행규정(2026. 4. 7.)
평가제품	ShadowCube V8.0
보호프로파일	국가용 문서암호화 보호프로파일 V3.1 (2025. 6. 27.)
보안요구사항	없음
보안목표명세서	ShadowCube V8.0 보안목표명세서 V1.5 (2026. 7. 28.)
평가보고서	ShadowCube V8.0 평가결과보고서 V1.02 (2026. 7. 28.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 CC:2022 R1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025
평가방법론	정보보호시스템 공통평가방법론 CEM:2022 R1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, CCMB-2025-001, October 2025
검증필 암호모듈 (탑재 필수)	MagicCrypto V2.3.0
평가신청인	(주)두루안
개발업체	(주)두루안
평가기관	(재)한국화학융합시험연구원

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