# MagicJCrypto

## Version 2.0.0.0

## 보안 정책

# 1. 암호모듈 명세

MagicJCrypto 암호모듈은 Java 언어로 개발된 API 함수를 이용하여 암/복호화, 해쉬, 전자서명생성/검증, 메시지인증(MAC), 키 생성 등의 암호서비스를 제공한다.

# 2. 보호함수 및 동작모드

## 2.1. 검증대상 보호함수

지원하는 검증대상 알고리즘 목록은 다음과 같다

| 구분 | 보호함수 | 동작모드 | 키길이 | 참조표준문서 |
|---|---|---|---|---|
| 블록암호 | ARIA | ECB, CBC | \|K\|=128,192,256 | KS X 1213 |
| | SEED | ECB, CBC | \|K\|=128 | TTAS.KO-12.0004 |
| | LEA | ECB, CBC | \|K\|=128,192,256 | TTAK.KO-12.0223 |
| 해쉬함수 | SHA-224 | - | - | FIPS 180-2 |
| | SHA-256 | - | - | FIPS 180-2 |
| | SHA-384 | - | - | FIPS 180-2 |
| | SHA-512 | - | - | FIPS 180-2 |
| MAC | HMAC (SHA-256) | - | - | FIPS 198 |
| | HMAC (SHA-224) | - | - | FIPS 198 |
| | HMAC (SHA-384) | - | - | FIPS 198 |
| | HMAC (SHA-512) | - | - | FIPS 198 |
| 난수생성기 | HASH_DRBG (SHA-256) | - | - | ISO/IEC 18031 |
| 공개키암호 | RSAES (SHA-256) | - | \|n\|=2048 e=65537 | PKCS #1 v2.1 |
| 전자서명 | RSA-PSS (SHA-256) | - | \|n\|=2048 e=65537 | PKCS #1 v2.1 |
| | KCDSA (SHA-256) | - | \|p\|=2048 \|q\|=256 | TTAS.KO-12.0001/R1 |

## 2.2. 비검증 대상 보호함수

지원하는 비검증 대상 알고리즘 목록은 다음과 같다.

| 구분 | 보호함수 | 동작모드 | 키길이 | 참조표준문서 |
|---|---|---|---|---|
| 블록암호 | AES | ECB, CBC | 128,192,256 | FIPS 197 |
| 해쉬함수 | SHA-1 | - | - | FIPS 180-2 |
| | HAS-160 | - | - | TTAS.KO-12.0011/R2 |
| MAC | HMAC (SHA-1) | - | - | FIPS 198 |
| 난수생성기 | DSA_PRNG (SHA-1) | - | - | FIPS 186-2 |
| 공개키암호 | RSAES-PKCS-V1.5 | - | \|n\|=1024,2048 e=65537 | PKCS #1 v1.5 |
| | RSAES (SHA-1) | - | \|n\|=1024,2048 e=65537 | PKCS #1 v2.1 |
| 전자서명 | RSA-PKCS-V1.5 (SHA-1) | - | \|n\|=1024,2048 e=65537 | PKCS #1 v1.5 |
| | RSA-PKCS-V1.5 (SHA-256) | - | \|n\|=1024 e=65537 | PKCS #1 v1.5 |
| | RSA-PSS (SHA-1) | - | \|n\|=1024,2048 e=65537 | PKCS #1 v2.1 |
| | RSA-PSS (SHA-256) | - | \|n\|=1024 e=65537 | PKCS #1 v2.1 |
| | KCDSA (HAS-160/SHA-1) | - | \|p\|=1024,2048 \|q\|=160,256 | TTAS.KO-12.0001/R1 |
| | KCDSA (SHA-256) | - | \|p\|=1024 \|q\|=160 | TTAS.KO-12.0001/R1 |

## 2.3. 동작모드

MagicJCrypto 암호모듈은 검증대상 알고리즘으로 기본 동작 하며, 비검증 대상 알고리즘 사용 시 모드 변경하여 사용 가능하다.

# 3. 운영환경

MagicJCrypto 암호모듈은 자바 압축파일 (JAR)로 된 소프트웨어로 응용프로그램 실행 시 로드되어 동작하며, J2SE 4,5,6,7,8 의 SDK/JRE 가 설치된 컴퓨터 하드웨어 및 운영체제에서 MagicJCrypto 암호모듈을 설치하여 운영할 수 있다.
세부 운영체제 지원 항목은 다음과 같다.

| OS 및 bits / JRE 버전 | | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| SunOS 5.10 (x86) | 32 | O | O | - | - | - |
| HP 11.11 | 64 | O | O | - | - | - |
| HP 11.23 | 64 | O | O | - | - | - |
| IBMAIX 5.3 | 64 | - | O | O | - | - |
| Linux k-2.6 | 64 | - | - | - | - | O |
| Windows 7 | 64 | O | O | O | O | O |
| Windows 10 | 64 | - | - | - | O | O |
| Windows Server 2016 | 64 | - | - | - | O | O |
| Linux k-3.10 | 64 | - | - | - | O | O |

# 4. 보안등급

MagicJCrypto 는 시험기준(KS X ISO/IEC 24759)의 11 개 보안영역 중 본 암호모듈에 해당되는 9 개의 영역 모두 보안등급 1 을 만족한다.

| 시험영역 | 보안등급 | 시험영역 | 보안등급 |
|---|---|---|---|
| 암호모듈명세 | 1 | 암호모듈포트와 인터페이스 | 1 |
| 역할, 서비스 및 인증 | 1 | 소프트웨어/펌웨어 보안 | 1 |
| 운영환경 | 1 | 물리적 보안 | N/A |
| 비침투 보안 | N/A | 중요 보안 매개변수 관리 | 1 |
| 자가시험 | 1 | 생명주기 보증 | 1 |
| 기타 공격에 대한 대응 | 1 | | |