MagicCrypto
Version 2.2.0

보안 정책

1. 암호모듈 명세

MagicCrypto 암호모듈은 단일파일 형태의 소프트웨어 암호모듈로 API 함수를 이용하여 암/복호화, 해쉬, 전자서명생성/검증, 메시지 인증(MAC), 키 생성, 키 설정, 키 유도 등의 암호 서비스를 제공한다.

2. 지원 알고리즘 및 동작모드

2.1. 검증대상 알고리즘

검증대상 알고리즘으로 아래와 같은 알고리즘을 지원한다.

구분	알고리즘	동작모드	파라메터	참조표준
블록암호	ARIA	ECB, CBC, CTR, CCM, GCM	|K|=128,192,256 Pad=PKCS5, SSL, ONE, X923	KS X 1213-1
	SEED	ECB, CBC, CTR, CCM, GCM	|K|=128 Pad=PKCS5, SSL, ONE, X923	TTAS.KO-12.0004/R1
	LEA	ECB, CBC, CTR, CCM, GCM	|K|=128,192,256 Pad=PKCS5, SSL, ONE, X923	TTAK.KO-12.0223
	HIGHT	ECB, CBC, CTR	|K|=128 Pad=PKCS5, SSL, ONE, X923	TTAK.KO-12.0040/R1
해시함수	SHA-224	-	-	ISO/IEC 10118-3
	SHA-256	-	-	ISO/IEC 10118-3
	SHA-384	-	-	ISO/IEC 10118-3
	SHA-512	-	-	ISO/IEC 10118-3
	LSH-224	-	-	TTAS.KO-12.0276
	LSH-256	-	-	TTAS.KO-12.0276
	LSH-384	-	-	TTAS.KO-12.0276
	LSH-512	-	-	TTAS.KO-12.0276

MAC	HMAC (SHA-256)	-	|K|≥256	ISO/IEC 9797-2
	HMAC (SHA-384)	-	|K|≥384	ISO/IEC 9797-2
	HMAC (SHA-512)	-	|K|≥512	ISO/IEC 9797-2
	GMAC (ARIA)	-	|K|=128,192,256	KS X 1213-1
	GMAC (LEA)	-	|K|=128,192,256	TTAK.KO-12.0223
	GMAC (SEED)	-	|K|=128	TTAS.KO-12.0004/R1
난수발생기	HASH_DRBG (SHA-256)	-	-	ISO/IEC 18031
공개키암호	RSAES (SHA-256)	-	|n|=2048,3072 e=65537	ISO/IEC 18033-2
전자서명	RSA-PSS (SHA-256)	-	|n|=2048,3072 e=65537	ISO/IEC 14888-2
	KCDSA (SHA-256)	-	|p|=2048 |q|=256	TTAS.KO-12.0001/R1
	ECDSA (SHA-256)	-	P-224, P-256 B-283, K-283	ISO/IEC 14888-3
키 설정	DH	-	|p|=2048 |q|=256	ISO/IEC 11770-3
	ECDH (SHA-256)	-	P-224, P-256	ISO/IEC 11770-3
키 유도	PBKDF2 (SHA-256)	-	-	TTAS.KO-12.0334
	HMAC_KDF (SHA-256)	Counter mode	-	TTAS.KO-12.0333

2.2. 비검증대상 알고리즘

비검증대상 알고리즘으로 아래와 같은 알고리즘을 지원한다.

구분	알고리즘	동작모드	파라메터	참조표준
블록암호	TripleDES	ECB, CBC	|K|=192	FIPS 46-3
	AES	ECB, CBC	|K|=128,192,256	FIPS 197
	RC2	ECB, CBC	|K|=40,128,192,256	RFC 2268
스트림암호	RC4	-	(가변)	RFC 6229

해시함수	MD5	-	-	RFC 1321
	SHA-1	-	-	FIPS 180-2
	HAS-160	-	-	TTAS.KO-12.0011/R2
MAC	HMAC (SHA-1)	-	-	FIPS 198
공개키암호	RSAES-PKCS-V1.5	-	|n|=1024,2048, 3072,4096 e=65537	PKCS #1 v1.5
	RSAES (SHA-1/384/512)	-	|n|=1024,2048 3072,4096 e=65537	PKCS #1 v2.1
	RSAES (SHA-256)	-	|n|=1024, 4096 e=65537	PKCS #1 v2.1
전자서명	RSA-PKCS-V1.5 (SHA-1/256/384/512)	-	|n|=1024,2048 3072,4096 e=65537	PKCS #1 v1.5
	RSA-PSS (SHA-1/384/512)	-	|n|=1024,2048, 3072,4096 e=65537	PKCS #1 v2.1
	RSA-PSS (SHA-256)	-	|n|=1024, 4096 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
	ECDSA (SHA-1)	-	B-163 #3, #5	ANSI X9.62
	ECDSA (SHA-256)	-	P-384, P-521	ISO/IEC 14888-3
	ECDSA (SHA-384/512)	-	P-256, P-384, B-283, P-521	ANSI X9.62
키설정	DH	-	|p|=1024 |q|=160	ANSI X9.42

2.3. 동작모드

MagicCrypto V2.2.0은 검증대상 동작모드와 비검증대상 동작모드 두 가지 형태의 동작모드를 제공한다. 검증대상 동작모드에서는 검증대상 알고리즘만을 수행할 수 있으며 비검증대상 동작모드에서는 비검증대상 알고리즘을 포함한 모든 암호알고리즘의 수행이 가능하다.

3. 운영환경

암호모듈 운영환경은 다음과 같다.

MagicCrypto V2.2.0은 Windows, SunOS, IBM AIX, HP-UX, Linux, Embeded Linux, QNX, MacOS 그리고 무선 단말 환경인 Android, iOS, Tizen 운영체제에서 동작한다.

운영체제	버전	비트	Arch	비고 (식별자)
windows	XP	32	x86	-
	Vista	32	x86	-
		64	x64	-
	7	32	x86	-
		64	x64	-
	8	32	x86	-
		64	x64	-
	8.1	32	x86	-
		64	x64	-
	10	32	x86	-
		64	x64	-
	2000	32	x86	-
	2008	32	x86	-
		64	x64	-
	2012	64	x64	-
	2016	64	x64	-
	2019	64	x64	-
SunOS	5.9	64	sparc	-
	5.10	64	sparc	-
	5.11	64	sparc	-
	5.10	32	x86	-
	5.11	64	x64	-
IBM AIX	5.3	64	ppc	-
	6.1	64	ppc	-
	7.1	64	ppc	-
	7.2	64	ppc	-

HP-UX	11.11	64	PA-RISK	64(Ae)
	11.23	64	PA-RISK	64(Ae)
	11.31	64	PA-RISK	64(Ae)
	11.23	64	ia64	64(Ae)
	11.31	64	ia64	64(Ae)
Linux	2.6	32	x86	-
	3.2	32	x86	-
	3.5	32	x86	-
	3.10	32	x86	-
	3.13	32	x86	-
	4.1	32	x86	-
	4.14	32	x86	-
	4.19	32	x86	-
	4.4	32	x86	-
	2.6	64	x64	-
	3.2	64	x64	-
	3.4	64	x64	-
	3.10	64	x64	-
	3.11	64	x64	-
	3.13	64	x64	-
	3.16	64	x64	-
	3.18	64	x64	-
	3.19	64	x64	-
	4.1	64	x64	-
	4.10	64	x64	-
	4.13	64	x64	-
	4.14	64	x64	-
	4.19	64	x64	-
	4.4	64	x64	-
	4.9	64	x64	-

Embedded Linux	2.6	32	armv5l	el01
	2.6	32	armv5l	el02
	2.6	32	armv5l	el03
	2.6	32	armv5l	el36
	2.6	32	armv5l	el05
	2.6	32	armv7l	el44
	2.6	32	mips	el18
	2.6	32	mipsel	el23
	2.6	32	mipsel	el24
	2.6	64	mips64	el28
	2.6	64	mips64	el29
	3.0	32	armv7l	el12
	3.2	32	armv7l	el09
	3.4	32	armv7l	el13
	3.4	32	mips	el26
	3.4	64	mips64	el35
	3.4	32	armv7l	el08
	3.8	32	armv7l	el06
	3.10	32	armv5l	el04
	3.10	32	armv6b	el17
	3.14	32	armv7l	el10
	3.10	32	mipsel	el27
	3.12	32	ppc	el34
	3.18	32	armv7l	el11
	3.18	32	armv7l	el14
	3.18	32	armv7l	el37
	3.18	32	mipsel	el25
	4.14	32	armv7l	el42
	4.14	32	mipsel	el40
	4.19	32	armv7l	el45
	4.19	32	mipsel	el46
	4.19	64	armv8l	el43
	4.4	32	armv7l	el41
	4.4	32	armv7l	el07
	4.4	64	armv8l	el38
	4.9	64	armv8l	el39
	4.14	32	armv7l	el15

QNX	7	64	armv8l	-
MacOS	10.11	64	x86_64	-
	10.13	64	x86_64	-
	10.14	64	x86_64	-
	10.15	64	x86_64	-
iOS	13	64	arm64	-
Android	4.0	32	armeabi-v7a	-
	4.1	32	armeabi-v7a	-
	4.2	32	armeabi-v7a	-
	4.4	32	armeabi-v7a	-
	6.0	32	armeabi-v7a	-
		64	arm64-v8a	-
	7.0	32	armeabi-v7a	-
		64	arm64-v8a	-
	8.0	32	armeabi-v7a	-
		64	arm64-v8a	-
	9.0	32	armeabi-v7a	-
		64	arm64-v8a	-
	10.0	32	armeabi-v7a	-
		64	arm64-v8a	-
Tizen	4.0	32	armv8l	-

4. 보안수준

MagicCrypto V2.2.0은 시험기준(KS X ISO/IEC 24759)의 11개 보안영역 중 본 암호모듈에 해당되는 9개의 영역 모두 보안수준 1을 만족한다.

시험영역	보안수준	시험영역	보안수준
암호모듈명세	1	암호모듈 인터페이스	1
역할, 서비스 및 인증	1	소프트웨어/펌웨어 보안	1
운영환경	1	물리적 보안	N/A
비침투 보안	N/A	중요보안매개변수	1
자가시험	1	생명주기 보증	1
기타 공격에 대한 대응	1		