MagicFCrypto

Version 1.0.0

보안 정책

1. 암호모듈 명세

MagicFCrypto 암호모듈은 API 함수를 이용하여 암/복호화, 해시, 전자서명 생성/검증, 메시지인증(MAC) 등의 암호서비스를 제공한다.
KS X ISO/IEC 19790/24759 의 요구사항인 보안수준 1 을 만족한다.

2. 알고리즘 및 동작모드

2.1. 검증대상 알고리즘

MagicFCrypto 암호모듈에서 제공되는 지원 암호 알고리즘은 다음과 같다. 펌웨어 일반 환경에서는 경량에 비해 키 설정, 전자서명, 난수 생성 알고리즘을 추가적으로 지원한다.

펌웨어 환경 (경량) 지원 알고리즘

구분	알고리즘	운영 모드	키길이	참조표준문서	비고
블록암호	ARIA	ECB, CBC, CTR, GCM	|K|=128,192,256	KS X 1213-1	
	LEA	ECB, CBC, CTR, GCM	|K|=128,192,256	TTAK.KO-12.0223	
해시	SHA256	-	-	ISO/IEC 10118-3	
메시지 인증	HMAC-SHA256		|K|≧256	ISO/IEC 9797-2	

펌웨어 환경 (일반) 지원 알고리즘

구분	알고리즘	운영 모드	키길이	참조표준문서	비고
블록암호	ARIA	ECB, CBC, CTR, GCM	|K|=128,192,256	KS X 1213-1	
	LEA	ECB, CBC, CTR, GCM	|K|=128,192,256	TTAK.KO-12.0223	
해시	SHA256	-	-	ISO/IEC 10118-3	
메시지 인증	HMAC-SHA256		|K|≧256	ISO/IEC 9797-2	
키 설정	ECDH	-	P-256	ISO/IEC 11770-3	

전자서명	ECDSA	-	P-256	ISO/IEC 14888-3	SHA256
난수발생기	SHA256 Hash_DRBG	-	-	ISO/IEC 18031	엔트로피 소스 외부 입력

2.2. 동작모드

MagicFCrypto 암호모듈은 검증대상 동작모드만을 지원하며 비검증대상 동작모드는 지원하지 않는다.

3. 운영환경

MagicFCrypto 암호모듈은 암호모듈 검증기준 보안수준 1 이 적용된 펌웨어 암호모듈이다.
MagicFCrypto 암호모듈의 운영환경인 대상 MCU 는 다음과 같다.

펌웨어 환경 (경량)

MCU	아키텍처
STM32F103VE	ARMv7-M Cortex-M3
STM32F103ZE	ARMv7-M Cortex-M3
STM32F103VG	ARMv7-M Cortex-M3
STM32L432KC	ARMv7-M Cortex-M4
STM32F091RC	ARMv6-M Cortex-M0
STM32L152RE	ARMv7-M Cortex-M3
STM32F401RE	ARMv7-M Cortex-M4
STM32F446RE	ARMv7-M Cortex-M4
STM32F746NG	ARMv7-M Cortex-M7

STM32L151CC	ARMv7-M Cortex-M4
MK22FN512VLL12	ARMv7-M Cortex-M4
MK22FN1M0VLL12	ARMv7-M Cortex-M4

펌웨어 환경 (일반)

MCU	아키텍처
STM32F103VE	ARMv7-M Cortex-M3
STM32F103ZE	ARMv7-M Cortex-M3
STM32F103VG	ARMv7-M Cortex-M3
STM32L432KC	ARMv7-M Cortex-M4
STM32F091RC	ARMv6-M Cortex-M0
STM32L152RE	ARMv7-M Cortex-M3
STM32F401RE	ARMv7-M Cortex-M4
STM32F446RE	ARMv7-M Cortex-M4
STM32F746NG	ARMv7-M Cortex-M7
STM32L151CC	ARMv7-M Cortex-M4
STM32L476VE	ARMv7-M Cortex-M4
STM32F723IE	ARMv7-M Cortex-M7
MK22FN512VLL12	ARMv7-M Cortex-M4
MK22FN1M0VLL12	ARMv7-M Cortex-M4
MAX32510	ARMv7-M Cortex-M3
MAX32558	ARMv7-M Cortex-M3

GDM7243i	ARMv7-R Cortex-R4
FIGHTER	ARMv7-M Cortex-M4

4. 보안수준

MagicFCrypto V1.0.0 은 암호모듈 검증기준/시험기준(KS X ISO/IEC 19790/24759)의 11 개 보안영역 중 본 암호모듈에 해당되는 10 개의 영역 모두 보안수준 1 을 만족한다.

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

5. 운영 시 고려사항

<보안수준 1>의 요구사항을 만족하는 MagicFCrypto V1.0.0 을 사용하는 펌웨어 개발자는 공격자로 인하여 암호모듈이 변조되는 것을 막기 위하여 디버깅 단자를 제거해야 하고, 메모리 보호 기능이나 시큐어 부트 기능 등을 사용하여 암호모듈이 설치된 메모리를 보호해야 한다.
암호모듈은 심각한 오류 상태, 오동작 또는 버전 변경 시 별도의 '유지보수 상태'를 제공하지 않으므로 해당 암호모듈을 폐기한다.
MagicFCrypto V1.0.0 는 내부적으로 난수 엔트로피를 생성하고 있지 않아 보안강도를 만족하는 엔트로피를 암호모듈 외부에서 입력해 주어야 한다.
MagicFCrypto V1.0.0 에서는 비밀키 및 키 쌍 생성하는 기능을 제공하지 않으므로 별도의 검증필 암호모듈을 사용하여 안전하게 생성된 키를 사용해야 한다.