보안 정책서 V1.5

ePower Crypto V2.0

한전KDN|주|

목 차

1. 암호모듈 개요

ePower Crypto V2.0은 블록암호, 메시지 인증코드, 해시함수, 난수 발생기, 전자서명, 키 설정 방식을 구현한 암호모듈로 Windows 계열, Linux 계열의 운영체제와 Embedded Linux 계열의 운영체제상에서 외부 응용 프로그램과 연동하여 운영된다. ePower Crypto는 암호모듈 시험기준(KS X ISO/IEC 24759:2015)의 영역별 보안 요구사항에 대하여 물리적 보안, 비침투 보안을 제외하고 모두 보안수준 1을 만족한다.

[표 1] 암호모듈 보안수준

No.	시험영역	보안수준
1	암호모듈 명세	1
2	암호모듈 인터페이스	1
3	역할, 서비스 및 인증	1
4	소프트웨어/펌웨어 보안	1
5	운영환경	1
6	물리적 보안	N/A
7	비침투 보안	N/A
8	중요보안 매개변수 관리	1
9	자가시험	1
10	생명주기 보증	1
11	기타 공격에 대한 대응	1

2. 암호모듈 명세

ePower Crypto V2.0은 라이브러리 형태의 소프트웨어 암호모듈로 C언어로 작성되었으며 사용자가 응용 프로그램에서 호출한 라이브러리의 함수 코드가 실행 파일 안으로 복사되어 사용되는 정적 링크 라이브러리가 아닌, 실행 파일을 만들 때 라이브러리에서 사용한 함수에 대한 정보만을 복사하고 함수가 실제 실행되는 시점에 라이브러리가 메모리에 저장되어 사용되는 동적 객체(Windows용 : .dll (Dynamic Link Library), Linux, Embedded Linux용 : .so (Shared Object) 형태로 구성되어 있다. ePower Crypto는 검증대상 보호함수만을 포함하며 비검증대상 알고리즘을 포함하지 않는다. ePower Crypto가 제공하는 알고리즘 종류는 다음과 같다.

[표 2] 암호 알고리즘 종류

구 분	보호함수	비 고	참조 표준문서
블록암호	ARIA	운영모드: ECB/CBC/CTR/CCM/GCM key 길이: 128/192/256bit block 길이: 128/192/256bit	KS X 1213-1
	LEA	운영모드: ECB/CBC/CTR/CCM/GCM key 길이: 128/192/256bit block 길이: 128/192/256bit	TTAK.KO-12.0223
메시지 인증	HMAC	SHA-256/384/512 기반	ISO/IEC 9797-2
해시	SHA- 256/384/512	-	ISO/IEC 10118-3 ISO/IEC 10118-3 Amd 1
난수 발생기	CTR_DRBG	블록암호: ARIA-128	ISO/IEC 18031 NIST SP 800-90
전자서명	ECDSA	Curve : FIPS P-256 해시 : SHA-256	ISO/IEC 14888-2
	EC-KCDSA	Curve : FIPS P-256 해시 : SHA-256	ISO/IEC 14888-3 TTAS.KO-12.0015
키 설정	ECDH	Curve : FIPS P-256	ISO/IEC 11770-3

ePower Crypto V2.0은 검증대상 보호함수만 제공하기 때문에 검증대상 동작모드만을 제공한다. ePower Crypto를 적재하여 초기화를 수행하면 검증대상 동작모드로 진입하며, 비검증대상 보호함수를 제공하지 않기 때문에 별도 동작모드 전환은 사용하지 않는다.

3. 암호모듈 인터페이스

ePower Crypto V2.0의 모든 정보 흐름은 논리적 인터페이스를 통해 수행되며 ePower Crypto에 대한 직접적인 물리적 접근지점을 제공하지 않는다. ePower Crypto는 각 논리적 인터페이스를 통해서만 데이터 입출력, 제어 입력, 상태를 출력한다. ePower Crypto에서 사용자에게 제공하는 모든 API는 암호모듈 상태 변수 확인 후 해당 작업을 수행한다.

[표 3] 암호모듈 인터페이스

분류	논리적 인터페이스	물리적 포트
데이터 입력 인터페이스	- 암호모듈은 외부로부터 입력되는 제어 정보를 제외한 모든 데이터를 데이터 입력 인터페이스를 통해 입력받는다. - 입력 데이터 : 평문 및 암호문 데이터, 암호키 및 핵심보안 매개변수, 인증 데이터 및 다른 모듈로부터의 상태정보 등 - ePower Crypto는 API의 함수 인자를 통하여 데이터의 입력을 수행한다.	키보드, 마우스 포트
데이터 출력 인터페이스	- 암호모듈이 외부로 출력하는 상태정보를 제외한 모든 데이터는 데이터 출력 인터페이스를 통해 출력된다. - 출력 데이터 : 평문 및 암호문 데이터, 암호키 및 핵심보안 매개변수, 인증 데이터 및 그 밖의 암호모듈을 위한 제어 정보 등 - ePower Crypto는 API의 함수 인자를 통하여 데이터의 출력을 수행한다.	모니터 포트
제어 입력 인터페이스	- 암호모듈이 외부로부터 입력되는 제어 정보는 제어 입력 인터페이스를 통해 입력받는다. - 제어 정보 : 암호모듈의 동작을 제어하기 위해 사용되는 모든 입력 명령, 신호 및 제어 데이터 등 - ePower Crypto의 제어 입력은 암호모듈의 수행을 위한 응용 프로그램의 API 호출만으로 이루어진다.	키보드, 마우스 포트
상태 출력 인터페이스	- 암호모듈이 외부로 출력하는 상태정보는 상태 출력 인터페이스를 통해 출력된다. - 상태정보는 표시하기 위해서 사용되는 모든 출력 신호, 표시기 및 상태 데이터 등 - ePower Crypto는 API 함수의 리턴 값으로 출력되며 각 리턴 값을 통해 함수의 수행 성공, 실패 여부와 실패한 경우에는 원인이 제공된다.	모니터 포트

4. 역할, 서비스 및 인증

ePower Crypto V2.0이 지원하는 운영자에게 인가된 역할은 사용자 역할과 암호 관리자 역할 두 가지이다. 이들 역할은 수행 가능한 서비스에 따라서 논리적으로 분류되며 각 역할에 대한 설명은 다음과 같다.

[표 4] 암호모듈의 역할

역할	세부 내용
사용자 역할	암호기능과 검증대상 보호함수를 포함한 일반 보안 서비스의 수행
암호 관리자 역할	사용자 역할 뿐 아니라 암호 초기화나 관리 기능도 수행 - 암호모듈의 초기화 - 암호모듈의 상태확인, 자가시험, 상태관리

ePower Crypto는 이 두 가지 역할 외에 별도의 역할을 지원하지 않기 때문에 모듈이 제공하는 서비스를 수행할 때, 반드시 사용자 역할과 암호 관리자 역할 중 하나의 역할로 수행되어야 한다. 해당 역할은 주체가 선택한 서비스의 종류에 의하여 결정된다. 즉, “KDN_Terminate” 와 같은 암호 관리자에게만 인가된 서비스를 사용하는 경우 해당 역할은 암호 관리자가 된다. 또한, “KDN_BC_Encrypt” 와 같은 일반 사용자에게 인가된 서비스를 수행할 때는 해당 역할이 암호 관리자 또는 사용자 중 하나가 된다.

[표 5] 함수의 논리적 역할 구분

함수	역할	세부 내용
KDN_Start	관리자	라이브러리를 실행한다.
KDN_Terminate	관리자	라이브러리의 종료를 실행한다.
KDN_CurrState	관리자	라이브러리의 현재 상태를 확인한다.
KDN_SelfTest	관리자	라이브러리의 자가시험을 수행한다.
KDN_GetInfo	사용자	라이브러리의 명칭, 버전 등의 정보를 출력한다.
KDN_GetErrorMsg	사용자	입력된 에러코드에 해당하는 에러 메시지를 출력한다.

함수	역할	세부 내용
KDN_Keygen	사용자	암호키를 생성한다.
KDN_BC_Encrypt	사용자	블록암호 암호화를 수행한다.
KDN_BC_Decrypt	사용자	블록암호 복호화를 수행한다.
KDN_Key_Encrypt	사용자	중요정보 암호화를 수행한다.
KDN_Key_Decrypt	사용자	중요정보 복호화를 수행한다.
KDN_Digest	사용자	메시지 압축을 수행한다.
KDN_Gen_MAC	사용자	MAC값 생성을 수행한다.
KDN_Verify_MAC	사용자	MAC값 검증을 수행한다.
KDN_Keygen_ECDSA	사용자	ECDSA 키 쌍을 생성한다.
KDN_Sign_ECDSA	사용자	ECDSA 전자서명을 수행한다.
KDN_Verify_ECDSA	사용자	ECDSA 전자서명 검증을 수행한다.
KDN_Keygen_ECKCDSA	사용자	ECKCDSA 키 쌍을 생성한다.
KDN_Sign_ECKCDSA	사용자	ECDSA 전자서명을 수행한다.
KDN_Verify_ECKCDSA	사용자	ECDSA 전자서명 검증을 수행한다.
KDN_KT_ECDH	사용자	ECDH 키 교환을 위한 키 토큰을 생성한다.
KDN_SK_ECDH	사용자	ECDH 키 교환을 위한 세션키를 생성한다.
KDN_Gen_RandNumber	사용자	난수 데이터를 생성한다.
KDN_Reseed_Entropy	사용자	엔트로피를 갱신한다.

※ KDN_Key_Encrypt와 KDN_Key_Decrypt API는 특수한 목적으로 설계 및 구현된 것이므로, 통신 데이터 기밀성 제공과 같은 **일반적인 데이터 암호화 등의 목적으로 사용할 수 없음**

5. 소프트웨어 보안

ePower Crypto V2.0은 단일 사용자 모드에서 사용할 수 있다. 모듈의 사용 권한을 보증하기 위해 운영체제의 로그인을 수행하여야 한다. 또한 운영체제는 여러 명의 사용자가 동시에 로그인 상태를 유지하는 것을 방지하므로 여러 명의 사용자가 동시에 본 모듈에 접속하는 것은 불가능하다.

ePower Crypto는 다른 프로세스의 접근과 비 암호 프로세스의 간섭을 막기 위해 모듈이 사용하는 메모리에 대한 다른 프로세스의 접근을 막는다. ePower Crypto의 메모리 사용은 자신을 호출하는 프로그램이 할당한 영역 내의 주소로 국한되며 ePower Crypto를 호출하는 응용 프로그램과 연관되어 수행되며 다른 모듈과는 전혀 연관되지 않는다. 이는 운영체제가 제공하는 Access Violation 기능을 사용하여 다른 프로세스의 접근을 방지하기 위함이다. ePower Crypto에 할당된 주소로 다른 응용프로그램이 침범하는 경우 Access Violation 오류를 발생시키며 접근을 제한한다. 이로써 실행이나 운영 중 다른 프로세스는 평문으로 된 개인키, 대칭키, 핵심보안 매개변수 및 키 생성을 위한 중간값 등에 접근할 수 없다. 따라서 운영체제의 도움을 받아 응용 프로그램 단위에서 다른 프로세서의 본 모듈에 대한 침입을 방지할 수 있다.

ePower Crypto의 원시코드와 실행 코드는 노출 및 변경으로부터 보호된다. ePower Crypto는 컴파일된 .dll 또는 .so 파일의 형태로 제공되므로 정확한 소스코드를 얻기 힘들다. 이미 컴파일된 파일로부터 컴파일 전의 본래 소스코드를 추출해 내는 역 컴파일러를 사용하여 기계어와 어셈블러로의 번역은 가능하지만 이를 이용하여 고급언어인 ePower Crypto의 소스코드로의 완벽한 변환은 불가능하다. 또한, ePower Crypto의 초기화 과정에서 무결성 검사를 수행한다. 제공된 파일의 위변조 시 초기화 과정의 무결성 검사를 통과할 수 없기 때문에 모듈의 위변조를 방지할 수 있다.

6. 운영환경

ePower Crypto V2.0은 소프트웨어 라이브러리 암호모듈로 Windows 및 Linux, Embedded Linux 환경에서 사용할 수 있다. ePower Crypto는 다음 표에 나타난 운영환경을 만족하는 환경에서 동작하며 운영환경을 만족하지 못할 시 정상 운영을 보장할 수 없다.

[표 6] 암호모듈 형상과 운영환경 정보

No	운영체제	버 전	비트	아키텍처	식별자	라이브러리 파일명
1	Windows	8.1	32bit	x86	-	epowercrypto.dll
2			64bit	x64	-	
3		10	32bit	x86	-	
4			64bit	x64	-	
5		11	64bit	x64	-	
6		Server 2012 R2	64bit	x64	-	
7		Server 2016	64bit	x64	-	
8		Server 2019	64bit	x64	-	
9	Linux	Redhat Enterprise Linux 7.4	64bit	x64	-	libepowercrypto.so
10		Redhat Enterprise Linux 8.2	64bit	x64	-	
11		CentOS Stream 8	64bit	x64	-	
12		Ubuntu 16.04	32bit	x86	-	
13			64bit	x64	-	
14		Ubuntu 20.04	64bit	x64	-	
15		Ubuntu 21.10	64bit	x64	-	
16	Embedded Linux (ARM9)	Kernel 2.6	32bit	Armv5l	-	
17	Embedded Linux (Cortex A5)	Kernel 3.10	32bit	Armv7l		
18		Kernel 4.19	32bit	Armv7l		
19	Embedded Linux (Cortex A7)	Kernel 3.18	32bit	Armv7l	-	
20		Kernel 4.19	32bit	Armv7l	-	
21		Kernel 5.4	32bit	Armv7l	-	
22	Embedded Linux (Cortex A8)	Kernel 3.2	32bit	Armv7l	-	
23		Kernel 4.9	32bit	Armv7l	-	

No	운영체제	버 전	비트	아키텍처	식별자	라이브러리 파일명
24		Kernel 4.14	32bit	Armv7l	-	
25		Kernel 4.19	32bit	Armv7l	-	
26	Embedded Linux (Cortex A9)	Kernel 4.1	32bit	Armv7l	-	
27		Kernel 4.9	32bit	Armv7l	-	
28		Kernel 4.14	32bit	Armv7l	-	
29		Kernel 4.19	32bit	Armv7l	Type1	
30		Kernel 4.19	32bit	Armv7l	Type2	
31		Kernel 5.4	32bit	Armv7l	-	
32	Embedded Linux (Cortex A53)	Kernel 4.19	32bit	Armv8l	-	
33		Kernel 5.4	32bit	Armv8l	-	
34		Kernel 5.4	64bit	Armv8l	-	
35		Kernel 5.10	32bit	Armv8l	-	
36		Kernel 5.10	64bit	Armv8l	-	
37	Embedded Linux (Cortex A72)	Kernel 4.19	32bit	Armv8l	-	
38		Kernel 5.4	32bit	Armv8l	-	
39		Kernel 5.4	64bit	Armv8l	-	
40	Embedded Linux (PowerPC P1020)	Kernel 3.0	32bit	PPC	-	

※ 단, Ubuntu 16.04의 경우 ESM(Extended Security Maintenance)을 통해 보안 유지 관리 시 사용할 수 있음

7. 물리적 보안

해당사항 없음

8. 비침투 보안

해당사항 없음

9. 중요보안 매개변수 관리

ePower Crypto V2.0의 중요보안 매개변수는 운영환경에 의해 인가되지 않은 수정, 노출, 변경으로부터 보호하기 위하여 중요보안 매개변수의 입력 및 사용 이후 제로화까지의 모든 과정을 관리한다. 중요보안 매개변수는 핵심보안 매개변수와 공개보안 매개변수로 구분되며 핵심보안 매개변수는 비밀키, 난수발생기 초기값, 난수발생기 상태값, 개인키, 키 생성 중간값, 엔트로피 입력으로 생성된 데이터이며 공개보안 매개변수로는 공개키가 있다. 제로화를 포함한 중요보안 매개변수는 다음 표와 같이 관리한다.

[표 7] 중요보안 매개변수 관리표

구분		생성	설정	주입	출력	저장	제로화
핵심보안 매개변수 (CSP)	ARIA 비밀키	○	×	×	×	×	○
	ARIA 라운드키	○	×	×	×	×	○
	LEA 비밀키	○	×	×	×	×	○
	LEA 라운드키	○	×	×	×	×	○
	HMAC 비밀키	○	×	×	×	×	○
	난수발생기 엔트로피 입력	×	×	×	×	×	○
	난수발생기 논스	×	×	×	×	×	○
	난수발생기 내부상태 V, Key	○	×	×	×	×	○
	ECDSA 개인키	○	×	×	×	×	○
	ECDSA 난수 K	○	×	×	×	×	○

구분		생성	설정	주입	출력	저장	제로화
	EC-KCDSA 개인키	○	×	×	×	×	○
	EC-KCDSA 난수 K	○	×	×	×	×	○
	ECDH 개인키	○	×	×	×	×	○
	암호처리에 사용된 변수 중 민감한 정보	○	×	×	×	×	○
	ECDH로 합의된 공유키	×	○	×	×	×	○
공개보안 매개변수 (PSP)	ECDSA 공개키	○	×	×	×	×	○
	EC-KCDSA 공개키	○	×	×	×	×	○
	ECDH 공개키	○	×	×	×	×	○

10. 자가시험

ePower Crypto V2.0은 암호모듈이 올바르게 기능하는지 확인하기 위해 동작 전 자가시험과 조건부 자가시험, 주기적 자가시험을 수행한다. 동작 전 자가시험은 암호모듈이 시작되기 전에 수행되고, 조건부 자가시험은 자가시험이 적용되는 암호동작 상태나 연산이 동작될 때 수행되며 주기적 자가시험은 동작 전 자가시험과 동일하며, API를 제공하여 사용자가 주기적 자가시험을 수행할 수 있다. 자가시험 목록은 아래 표와 같다.

[표 8] 자가시험 목록

구분	시험 항목		내용
동작 전 자가시험	암호알고리즘 시험		암호모듈에 탑재된 모든 암호알고리즘에 대한 기지답안검사(KAT) 수행
	잡음원 건전성 시험	반복 횟수 테스트	암호모듈이 사용하는 잡음원의 고장 여부 확인
		적용성 비율 테스트	암호모듈이 사용하는 잡음원의 엔트로피량 이상 감지
	소프트웨어 무결성 시험		ECDSA(P-256)을 사용하여 암호모듈 바이너리 파일에 대한 무결성 검증 수행
조건부 자가시험	암호 키 쌍 일치 시험		암호모듈이 생성한 공개키와 개인키가 정상인지 확인

구분	시험 항목		내용
			(조건 : 키 쌍 생성 함수 호출 시) - ECDSA 키 생성 함수 내부 - EC-KCDSA 키 생성 함수 내부 - ECDH 키 토큰 생성 함수 내부
	잡음원 건전성 시험	반복 횟수 테스트	암호모듈이 사용하는 잡음원의 고장 여부 확인 (조건 : 엔트로피 소스 함수 호출 시) (방법 : 같은 값이 연속 출력되는 횟수 확인)
		적응성 비율 테스트	암호모듈이 사용하는 잡음원의 엔트로피량 이상 감지 (조건 : 엔트로피 소스 함수 호출 시) (방법 : 특정 범위 내에 같은 값이 출력된 빈도수 확인)
주기적 자가시험	동작 전 자가시험과 동일		

오류 상태는 암호모듈이 정상적으로 실행되지 않는 상태를 말한다. 암호모듈 내에서 해당 오류가 수정되더라도 정상적인 실행과는 다른 과정을 거쳐야 하므로 오류 상태로 분류한다. 오류 상태는 심각한 오류 상태와 단순한 오류 상태로 나뉜다.

단순한 오류 상태는 암호모듈 내에서 자체적으로 수정 및 회복이 가능한 오류 상태를 말하고 심각한 오류 상태는 암호모듈 내에서 자체적으로 수정 및 회복이 불가능한 오류 상태를 말한다. 단순한 오류 상태일 때는 암호모듈 내에서 수정 및 회복이 가능하므로 다른 상태로 천이되지 않는다. 다만 오류 수정 및 회복을 위한 과정을 거치게 된다. 하지만 심각한 오류 상태일 때는 자체적인 수정 및 회복이 불가능하므로 암호모듈 종료 상태로 천이되고 오류 표시를 출력한다. 이 경우 암호모듈 실행 과정에서 사용된 모든 데이터의 출력은 차단된다. 따라서 심각한 오류 상태일 경우는 암호모듈 개발자에게 문의하여 오류를 수정하거나 재설치를 해야 한다.

11. 생명주기 보증

ePower Crypto V2.0은 인가된 운영자에게 배포되며 개발 문서에 명시된 방법으로 설치, 초기화 및 시동을 시행한다. 배포 및 운영 방안은 다음과 같다.

[표 9] 배포 및 운영 방안

구분	세부 설명
배포	암호모듈 요청 시 유·무선 혹은 대면으로 암호모듈 운영자를 확인한 후 CD 또는 USB 등 안전한 전달방법으로 배포하며 인가된 운영자만 암호모듈에 접근하도록 한다.
암호모듈 무결성 검증	암호모듈은 자가시험의 암호모듈 무결성 검증을 통하여 인증된 모듈의 확인과 모듈의 변경을 확인한다.
배포처 및 담당 암호모듈 운영자 이력관리	배포된 암호모듈의 배포처와 담당자에 대한 이력 관리를 하여 무분별한 요청과 암호모듈의 정보유출에 대비한다.
장애대응	최초 장애 접수 후 빠른 시간 내 처리 및 응대한다. 장애 발생 시 방문 또는 유선 연락을 통하여 문제를 해결하도록 지원한다.
기술지원	사용자 요청 시 방문 또는 유선으로 기술 지원을 한다. 또한 암호모듈의 보안 취약점 개선 및 보완 시 재검증 진행 후 배포하도록 한다.
교육지원	사용자 안내서를 지원하며 암호모듈 운영자의 요청으로 인한 교육은 계약에 따라 지원한다.

12. 기타 공격에 대한 대응

ePower Crypto V2.0은 보안등급 1의 동적 객체 형태의 제품으로 블록암호 및 공개키 암호에 대한 부채널 공격 대응기법이 적용되었다.

블록암호에 대한 부채널 공격 대응기법인 마스킹 기법은 암호모듈이 동작하는 도중 예상되는 중간값을 랜덤하게 하여 공격자에 유출된 부채널 정보에서 의미있는 정보를 추출하지 못하도록 하는 대응기법이다. 공개키 암호에 대한 부채널 대응기법으로 단순 전력 분석 및 타이밍 공격에 대한 대응기법 및 차분 전력 분석에 대한 대응기법이 각각 적용되었다.

13. 보안정책 및 사용지침

가. 보안정책

ePower Crypto V2.0은 암호모듈 시험기준(KS X ISO/IEC 24759:2015)의 보안수준 1을 만족하는 암호모듈로 다음의 보안 규칙을 따른다.

1) 암호모듈 운영자는 관리자와 사용자로 구분된다.
2) 별도의 인증 메커니즘을 제공하지 않는다.
3) 관리자는 암호모듈 운영 중에 주기적 자가시험을 시행할 수 있다.
4) 동작 전 자가시험은 암호모듈 초기화 시 운영자의 개입 없이 수행되며 성공 시 암호 서비스를 이용할 수 있고 실패 시 오류 코드를 반환한다.
5) 암호모듈이 오류 상태나 자가시험 중에는 모든 데이터에 대한 출력은 중지된다.
6) 암호모듈은 핵심보안 매개변수 또는 암호모듈의 보안에 문제 될 수 있는 정보는 출력하지 않는다.
7) 암호기능이 종료되는 시점이거나 암호모듈에 심각한 오류가 발생하면 핵심보안 매개변수 및 사용된 데이터는 무조건 제로화가 시행된다.
8) 암호모듈의 데이터 입출력은 암호모듈에서 정의된 데이터 입출력 인터페이스만을 통해서 수행된다.
9) 블록암호의 비밀키 및 초기화 벡터, 메시지 인증코드의 인증키와 전자서명, 키 설정 시 사용되는 난수는 검증필 암호모듈에 탑재된 난수발생기를 사용한다.
10) 암호모듈은 유지보수 인터페이스나 관련된 역할을 제공하지 않는다.

나. 사용지침

암호모듈 운영자는 본 문서(보안 정책서)에 명시된 내용과 사용자 안내서에 따라 암호모듈을 사용해야 한다.

(58322) 전라남도 나주시 빛가람로 661
기술문의 : 061-931-5955 / 5956 FAX : 061-931-7954