ABC V1.0

시험결과보고서

V3.00

2025 년 6 월 20 일

민간시험기관명

[문서 정보]

문서관리고유번호	민간시험기관명 -KCMVP-2025-001		
문서 제목	ABC V1.0 시험결과보고서 V3.00		
암호모듈 식별	ABC V1.0		
신청구분	신규검증		
신청기관	개발업체명		
시험기관	민간시험기관명		
시험원	시험자 _1	서명	(서명)
	시험자 _2	서명	(서명)
기술책임자	기술책임자 _1	서명	(서명)
승인자	기술책임자 _1	서명	(서명)

[문서 이력관리]

문서버전	개정 내용	날짜
V0.90	암호모듈에 대한 시험결과 최초작성	2024.09.25.
V1.00	기술책임자 검토 완료	2024.09.25.
V1.90	검증기관 검토의견 반영	2024.12.18.
V2.00	기술책임자 검토 완료	2025.02.24.

제 1 장 시험결과 요약

1. 개요

모듈명	모듈형태	전체 보안수준	개발사
ABC V1.0	S/W(라이브러리)	보안수준 1	개발업체 (주)

2. 적용 기준

표준 문서명	KS X ISO /IEC 19790:2015 KS X ISO/IEC 24759:2015

3. 검증대상 암호알고리즘

구분		세부 내용
블록암호	ARIA	키 길이 = 128 비트 운영모드 = ECB/CBC/CTR/GCM
해시함수	SHA-2	SHA2-256/384
메시지 인증	HMAC	해시함수 = SHA2-256/384
난수발생기	CTR_DRBG	블록암호 = ARIA 키 길이 = 128 비트
전자서명	ECDSA	타원곡선 좌표계 = P-256 해시함수 = SHA2-256
키 설정	ECDH	타원곡선 좌표계 = P-256
키 유도	PBKDF2	PRF = HMAC-SHA2-256

4. 시험결과

□ ABC V1.0 은 보안수준 1 을 만족하도록 설계된 소프트웨어 라이브러리 형태 암호모듈로 <KS X ISO/IEC 24759:2015> 의 적용 가능한 시험항목에 대한 요구사항을 만족한 다 .

암호모듈 명	ABC V1.0	모듈 형태	S/W(라이브러리)
개발사 명	개발업체 (주)	적용 기준	KS X ISO/IEC 19790:2015 KS X ISO/IEC 24759:2015

보안수준

☒ 전체 수준 : 보안수준 1

☒ 시험영역별 보안수준

시험영역	보안수준
암호모듈 명세	1
암호모듈 인터페이스	1
역할 , 서비스 및 인증	1
소프트웨어 / 펌웨어 보안	1
운영환경	1
물리적 보안	해당사항 없음
비침투 보안	해당사항 없음
중요 보안매개변수 관리	1
자가시험	1
생명주기 보증	1
기타 공격에 대한 대응	1

비고	SSO(Single Sign On) 정보보호제품에 탑재되는 암호모듈 라이브러리

목 차

제 2 장 개요

1. 시험모듈 개요

구분	내용
암호모듈	ABC V1.0
개발사	개발업체명
형태	S/W(라이브러리)
전체 보안수준	보안수준 1
운영환경	변경 가능한 운영환경 (00 종의 운영체제)

2. 적용기준

※ KS X ISO/IEC 19790:2015, KS X ISO/IEC 24759:2015

시험항목	보안수준	시험항목	보안수준
암호모듈 명세	1	암호모듈 인터페이스	1
역할 , 서비스 및 인증	1	소프트웨어 / 펌웨어 보안	1
운영환경	1	물리적 보안	해당없음
비침투 보안	해당없음	중요보안매개변수 관리	1
자가시험	1	생명주기 보증	1
기타 공격에 대한 대응	1	전체	**1**

3. 시험 담당자

직급	성명	비고
주임연구원	시험자 _1	주 시험자
주임연구원	시험자 _2	보조 시험자

4. 시험 일정

4.1 시험 일수

구분	일수
총 일수	00 일

4.2 시험 단계별 일정

단계	기간	참여기관		수행업무
시험 신청	0000.00.00	민간시험기관명 신청업체	-	신청업체에서 시험신청서 제출
사전검토 회의	0000.00.00	민간시험기관명 신청업체 검증기관	-	사전검토회의
시험 접수	0000.00.00	민간시험기관명 신청업체	-	시험 접수증 발급
시험계약	0000.00.00	민간시험기관명 신청업체	-	시험 계약 체결
시험착수	0000.00.00	민간시험기관명 신청업체	-	시험 착수
시험종료	0000.00.00	민간시험기관명 신청업체	-	시험종료
검토완료	0000.00.00	민간시험기관명 검증기관	-	검증기관 검토 의견 반영 완료

5. 시험 환경

	시험도구 및 환경	적용 방법	시험항목
시험 환경 **(OS)**	Ubuntu 22.04 (Kernel 5.15) (x86_64) Ubuntu 24.04 (Kernel 6.8) (x86_64)	기능 확인	AS02. 암호모듈 명세 AS04. 역할 , 서비스 및 인증

	Embedded Linux (Kernel 4.19) (aarch64 64bit)		AS06. 운영환경 AS11. 생명주기 보증
시험 도구	- Visual Studio Code 1.94.2 - GDB 15.2 - 암호모듈 사전검증 서비스 - Code-RAY XG V6.0	소스코드 & 인터페이스 분석 중요보안매개변수 분석 엔트로피 분석 소스코드 취약점 분석	AS03. 암호모듈 인터페이스 AS05. 소프트웨어 / 펌웨어 보안 AS09. 중요 보안매개변수 관리 AS10. 자가시험 AS12. 기타 공격에 대한 대응
CAVP	- 암호모듈 사전검증 서비스	암호알고리즘 구현 적합성 검증	암호알고리즘 검증기준

제 3 장 시험 내용

1. 암호모듈 명세 (AS02)

□ 암호모듈은 암호알고리즘과 키 생성을 포함하는 보호함수와 프로세스를 구현한 하드웨어 , 소프트웨어 , 펌웨어 및 이들 조합의 집합 형태이다 .

□ 암호모듈 명세에서는 암호경계 , 구성요소 , 동작모드 , 지원 암호알고리즘 , 중요보안매개변수 등을 파악함으로써 암호모듈의 전체적인 구조를 확인하고자 한다 .

1.1 AS02 시험항목

AS	TE	확인사항
AS02.03	1, 2	암호모듈의 유형
AS02.07	1, 2	암호경계 내의 구성요소
AS02.09	1	암호경계 내의 알고리즘 , 프로세스 등 보안 관련 요소
AS02.10	1, 2	검증대상 서비스 (또는 동작) 에 영향을 주는 경계 내의 비보안 요소
AS02.11	1, 2	암호모듈의 명칭
AS02.12	1	구성요소별 버전 부여 및 관리 방법
AS02.13	1	검증대상 서비스 (또는 동작) 에 영향을 주는 경계 외의 요소
AS02.14	1, 2, 3	보안요구사항을 적용 받지 않는 암호모듈의 구성요소
AS02.16	1,2,3,4,5	정의된 암호경계의 적절성 (소프트웨어 암호모듈의 암호경계)
AS02.19	1, 2	검증대상 동작모드의 동작 절차
AS02.20	1, 2	검증대상 및 비검증대상 암호알고리즘 목록
AS02.21	1, 2	검증대상 동작모드에서 사용되는 비검증대상 요소
AS02.22	1, 2	검증대상 및 비검증대상 동작모드간 핵심보안매개변수 분리 여부
AS02.24	1, 2	검증대상 서비스 (또는 동작) 에 대한 표시

1.2 TE02.03.01

1.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.03.01	암호모듈의 유형 식별	개발문서 검토

1.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

■ OpenSSL Security Policy Version 3.1.2

나) 개발문서 검토내용

☒ OpenSSL 암호모듈의 유형이 소프트웨어 모듈로 명시되어 있으며 , 실행 환경 및 구현 방식이 명확하게 기술됨 .

다) 증빙자료

☒ 개발 문서 5 페이지의 암호모듈 유형 설명을 인용하여 제시함 .

Table 3-1 표 제목

No	대분류	중분류	내용
1	문서명	버전	OpenSSL Security Policy Version 3.1.2
2	문서구성	암호모듈 유형	소프트웨어
3	문서구성	구현 프로그래밍 언어	C 언어
4	실행환경	운영체제	Linux Kernel 5.10
5	파일	파일명	libcrypto.so, libsslso
6	문서관리	개정이력	개정일자 : 2024.05.10

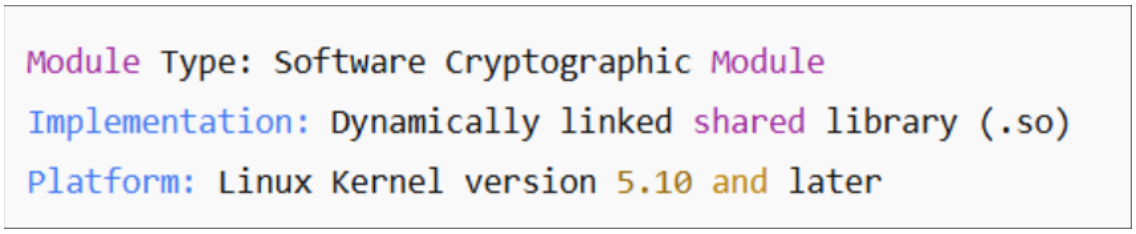

Figure 3-1 암호모듈 유형 (개발문서)

2) 소스코드 검토

라) 소스코드명

■ crypto.h, opensslv.h

마) 소스코드 검토내용

☒ 암호모듈명이 기본 헤더파일 소스코드에 명시적으로 선언되어 있음

바) 증빙자료

☒ crypto.h 파일과 opensslv.h 파일에서 암호모듈명 식별자 및 버전 (OpenSSL 3.1.2) 이 명확하게 명시됨

Table 3-2 표 제목

No	대분류	중분류	내용
1	소스코드	파일명	crypto.h, opensslv.h
2	코드 구성	모듈 식별정보	OEPNSSL_VERSION_TEXT 선언
3	코드 검토	명시적 식별자	FIPS_mode() API 존재
4	파일	라이브러리	libcrypto.so, libssl.so
5	코드 형식	구현 언어	C 언어
6	코드 관리	버전 관리 시스템	Git 5.0

```
/* crypto.h */
#define OPENSSL_VERSION_TEXT "OpenSSL 3.1.2 10 May 2024 (FIPS validated)"

/* openssl.h */
#define OPENSSL_VERSION_NUMBER 0x3010200fL
```

Figure 3-2 암호모듈 식별 정보 (소스코드)

3) 암호모듈 시험

사) 암호모듈 시험명

■ OpenSSL Module Type Identification Test

아) 암호모듈 시험내용

☒ 모듈이 정상적으로 로드되었을 때 , 모듈의 유형과 버전이 정확히 식별되는지 확인하는 시험을 수행함 .

자) 증빙자료

☒ "openssl version -a" 명령어 실행으로 모듈의 유형과 버전 및 FIPS 인증 여부 확인 .

Table 3-3 표 제목

No	대분류	중분류	내용
1	시험 환경	운영체제	Ubuntu Linux 22.04
2	시험 절차	명령어	opessl version -a
3	시험 결과	출력 내용	OpenSSL 3.1.2
4	시험 결과	모듈 유형	Software Module

```
OpenSSL 3.1.2 10 May 2024 (FIPS validated)
built on: Mon May 13 10:45:32 2024 UTC
platform: linux-x86_64
options:  bn(64,64) rc4(16x,int) des(int) aes(partial)
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib/engines-3"
MODULEDIR: "/usr/local/ssl/lib/ossl-modules"
```

Figure 3-3 암호모듈명 출력 시험결과

1.2.3 판정근거

Table 3-4 TE02.03.01 시험결과 판정 근거

No	판정 항목	판정 근거 설명	근거 자료
1	개발문서 일치성	개발문서에 명시된 소프트웨어 모듈과 실제 검증된 모듈 유형이 일치함	Table 3-1
2	소스코드 일치성	소스코드에 명시된 버전과 식별 정보가 개발문서와 일치함	Table 3-2
3	암호모듈 시험 결과	명령어 출력과 개발문서 , 소스코드 식별 정보가 모두 일치함	Table 3-3
4	전체 시험 일관성	개발문서 , 소스코드 , 모듈 시험결과가 상호 일치함	Figure 3-1, Figure 3-2, Figure 3-3

1.2.4 판정결과

차) 판정 : 통과

1.3 TE02.03.02

1.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.03.02	구성요소들을 통한 암호모듈의 유형 확인	개발문서 검토

1.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-5 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

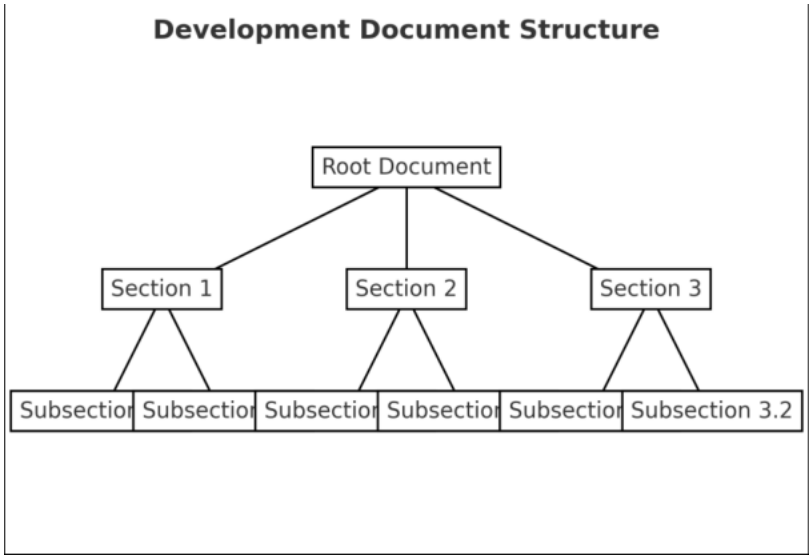

Figure 3-4 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-6 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

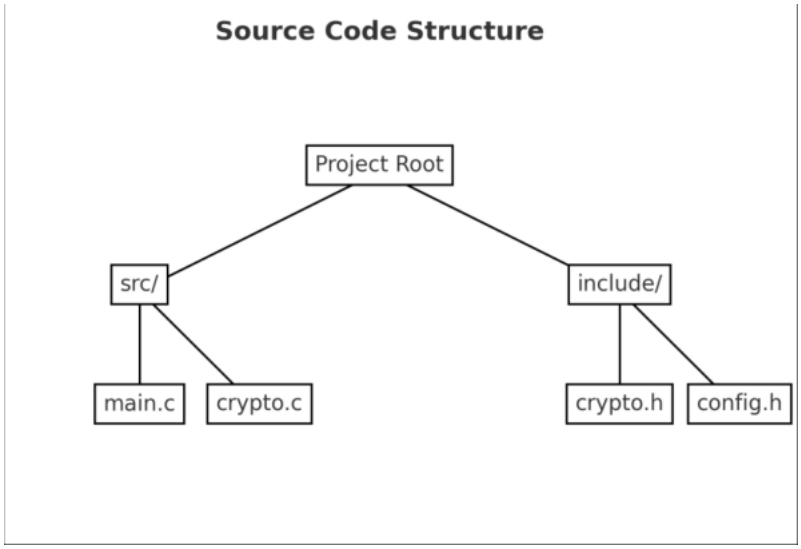

Figure 3-5 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-7 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

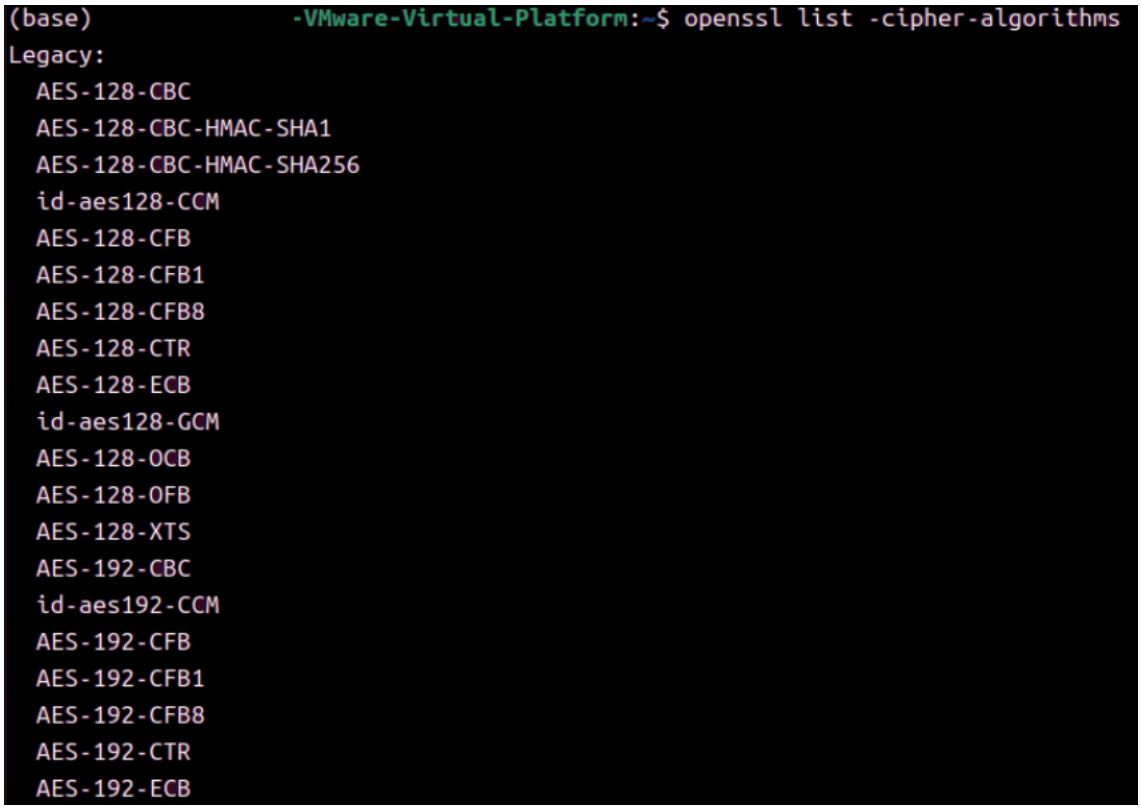

Figure 3-6 그림 제목

1.3.3 판정근거

Table 3-8 TE02.03.02 시험결과 판정근거

No	판정 항목	판정 근거 설명	근거 자료
1			
2			
3			
4			

1.3.4 판정결과

차) 판정 : <“ 통과 ” 또는 “ 실패 ”>

제 4 장 암호알고리즘 시험결과

1. 시험방법

시험대상 암호알고리즘			시험항목
블록암호	ARIA	|K| = 128 Mode = ECB/CBC/CTR	KAT/MCT/MMT
	ARIA	|K| = 128 Mode = GCM	AE/AD
해시함수	SHA-2	Hash = SHA-256/384	SMT/LMT/MCT
메시지 인증코드	HMAC	Hash = SHA-256/384	KAT
난수발생기	CTR_DRBG	ARIA, |K| = 128, 유도함수 미지원 예측내성 미지원	KAT
전자서명	ECDSA	P-256, Hash = SHA-256	KPG, SGT, PKV
키 설정	ECDH	P-256	PKV, KPG, KKAKAT
키 유도	PBKDF2	HMAC-SHA2-256	KAT

2. 시험결과

시험대상 암호알고리즘		시험 항목	결과
블록암호	ARIA	KAT/MCT/MMT	만족
인증암호화	GCM	AE/AD	만족
해시함수	SHA-2	SMT/LMT/MCT	만족
메시지 인증	HMAC	KAT	만족
난수발생기	CTR_DRBG	KAT	만족
전자서명	ECDSA	KPG/SGT/SVT/PKV	만족
키 설정	ECDH	KPG/PKV/KAKAT	만족
키 유도	PBKDF2	KAT	만족

※ 참조 : 자세한 시험결과는 '\[첨부 4] VS 시험결과 \ABC V1.0 CAVP 시험결과 .pdf'

제 5 장 결론

1. 시험결과

□ 이 암호모듈은 보안수준 1 을 만족하도록 신청된 소프트웨어 암호모듈로 「 KS X ISO/IEC 19790:2015, 24759:2015 를 적용한 결과 , 적용 가능한 보안영역에 대한 요구사항을 만족한다 .

시험항목	보안수준	시험항목	보안수준
- 암호모듈 명세	1	- 암호모듈 인터페이스	1
- 역할 , 서비스 및 인증	1	- 소프트웨어 / 펌웨어 보안	1
- 운영환경	1	- 물리적 보안	해당없음
- 비침투 보안	해당없음	- 중요보안매개변수 관리	1
- 자가시험	1	- 생명주기 보증	1
- 기타 공격에 대한 대응	1		

보안 요구사항		시험 항목	평결
암호모듈 명세	암호모듈 유형	AS02.03	만족
	암호경계	AS02.07	만족
		AS02.09	만족
		AS02.10	만족
		AS02.11	만족
		AS02.12	만족
		AS02.13	만족
		AS02.14	만족
		AS02.16	만족
		AS02.19	만족
	동작모드	AS02.20	만족
		AS02.21	만족
		AS02.22	만족
		AS02.24	만족
암호모듈 인터페이스	일반 요구사항	AS03.01	만족
	인터페이스 정의	AS03.04	만족
		AS03.05	만족
		AS03.06	만족
		AS03.07	만족
		AS03.08	만족
		AS03.09	만족
		AS03.10	만족
		AS03.11	만족
		AS03.15	만족
역할 , 서비스 및 인증	역할 , 서비스 및 인증 일반 요구사항	AS04.02	만족
	역할	AS04.05	만족

	서비스	AS04.06	만족
		AS04.11	만족
		AS04.13	만족
		AS04.14	만족
		AS04.15	만족
	운영자 인증	AS04.43	만족
		AS04.44	만족
		AS04.56	만족
소프트웨어 / 펌웨어 보안	-	AS05.02	만족
		AS05.04	만족
		AS05.05	만족
		AS05.06	만족
		AS05.09	만족
운영환경	운영환경 일반 요구사항	AS06.02	만족
		AS06.03	만족
	변경 가능한 운영환경의 요구사항	AS06.05	만족
		AS06.06	만족
		AS06.07	만족
		AS06.08	만족
중요 보안매개변수 관리	중요 보안매개변수 관리 일반 요구사항	AS09.01	만족
		AS09.02	만족
		AS09.04	만족
		AS09.05	만족
	난수 발생기	AS09.06	만족
		AS09.07	만족
	중요보안매개변수 생성	AS09.08	만족

		AS09.09	만족
	중요 보안매개변수 설정	AS09.10	만족
	중요 보안매개변수의 주입 및 출력	AS09.19	만족
	중요 보안매개변수의 제로화	AS09.29	만족
		AS10.07	만족
		AS10.08	만족
	자가시험 일반 요구사항	AS10.09	만족
		AS10.10	만족
		AS10.11	만족
		AS10.15	만족
	동작 전 자가시험	AS10.17	만족
		AS10.20	만족
자가시험		AS10.24	만족
		AS10.25	만족
		AS10.27	만족
		AS10.28	만족
		AS10.29	만족
	조건부 자가시험	AS10.33	만족
		AS10.34	만족
		AS10.35	만족
		AS10.53	만족
	생명주기 보증 일반 요구사항	AS11.01	만족
생명주기 보증		AS11.03	만족
	형상 관리	AS11.04	만족

	유한상태모델	AS11.05	만족
		AS11.08	만족
		AS11.11	만족
	개발	AS11.13	만족
		AS11.15	만족
		AS11.16	만족
	벤더 시험	AS11.19	만족
		AS11.29	만족
		AS11.30	만족
	배포 및 운영	AS11.32	만족
	수명의 종료	AS11.36	만족
	안내서	AS11.38	만족
		AS11.39	만족
기타 공격에 대한 대응	-	AS12.02	만족

Table 5-1 암호모듈 시험결과 요약표

2. 종합의견

< 개발업체 (주)> 에서 신청한 <ABC V1.0> 은 검증기준 (KS X ISO/IEC 19790:2015, KS X ISO/IEC 24759:2015) 에 명시된 보안수준 1 을 만족한다 .

3. 암호모듈 구성요소 해시값

Table 5-2 암호모듈 구성요소 해시값

운영체제	제품명 및 버전	비트	아키텍처	모듈 명	해시 값 (SHA-512)
Ubuntu	22.04 LTS	64	x86_64	libsscrypto.so	0587E07F84031BB5EDDA117B8AB9F3879656930D792A5052B79C297BA9EE3E3C7349D30983A6FDE7C218E3D7E95837C3D50AA12BC53DCD171C46605E8BB3F724
Ubuntu	24.04 LTS	64	x86_64	libsscrypto.so	044C261582D5C783D92AD3FDF831DB8EE4048B5F216DF4D76BDC0800A72EA4B101A2443E582E852EA7F21365DDEC514694BAE0653F85DDF984CE2E3BD61F1EE3
Embedded Linux	Linux Kernel 4.19	64	aarch64	libsscrypto.so	E84BA109A99E3417DB4D136D7D270B503D537C1EB602B5F6B738385777C0F3137E82613CE516347AD4195496191168009EFCA54CAF56EAC5FF2E489FC808986F

부록

[별첨 1] 소스목록 및 소스 해시 값
[별첨 2] 보안정책서

[첨부 1] 소스코드
[첨부 2] 암호모듈
[첨부 3] 개발문서
[첨부 4] VS 시험결과
[첨부 5] 테스트프로그램