ABC V1.0

시험결과보고서

V2.00

2025 년 6 월 20 일

민간시험기관명

[문서 정보]

문서관리고유번호	민간시험기관명 -KCMVP-2025-001		
문서 제목	ABC V1.0 시험결과보고서 V2.00		
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	2025.01.25
V1.00	기술책임자 검토 완료	2025.01.30
V1.90	검증기관 검토의견 반영	2025..06.02
V2.00	기술책임자 검토 완료	2025.06.30

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

☒ 전체 수준 : 보안수준 1

☒ 시험영역별 보안수준

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 1 장 시험결과 요약 4
1. 개요 4
2. 적용 기준 4
3. 검증대상 암호알고리즘 4
4. 시험결과 5
제 2 장 개요 7
1. 시험모듈 개요 7
2. 적용기준 7
3. 시험 담당자 7
4. 시험 일정 8
5. 시험 환경 8
제 3 장 시험 내용 10
1. 암호모듈 명세 (AS02) 10
2. 암호모듈 인터페이스 (AS03) 123
3. 역할 , 서비스 및 인증 (AS04) 236
4. 소프트웨어 / 펌웨어 보안 (AS05) 293
5. 운영환경 (AS06) 318
6. 중요 보안매개변수 관리 (AS09) 363
7. 자가시험 (AS10) 446
8. 생명주기 보증 (AS11) 591
9. 기타 공격에 대한 대응 (AS12) 720
제 4 장 암호알고리즘 시험결과 729
1. 시험방법 729
2. 시험결과 730
제 5 장 결론 731
1. 시험결과 731
2. 종합의견 736
3. 암호모듈 구성요소 해시값 736
부록 737

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

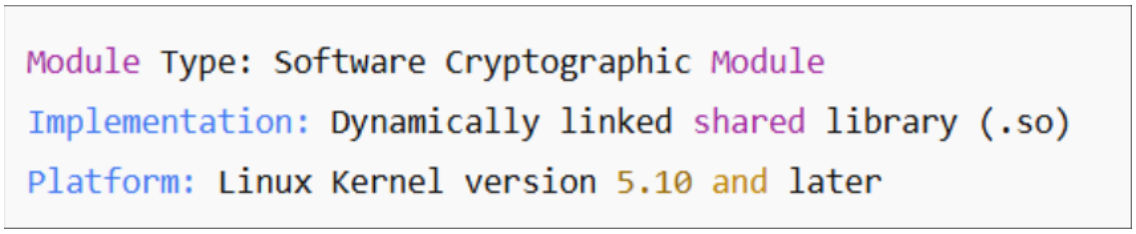


Figure 3-1 암호모듈 유형 (개발문서)

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			

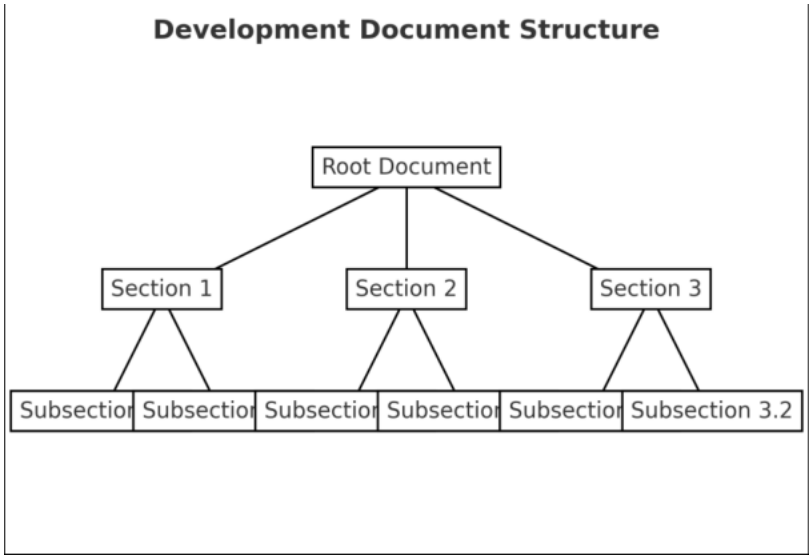


Figure 3-4 그림 제목

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			

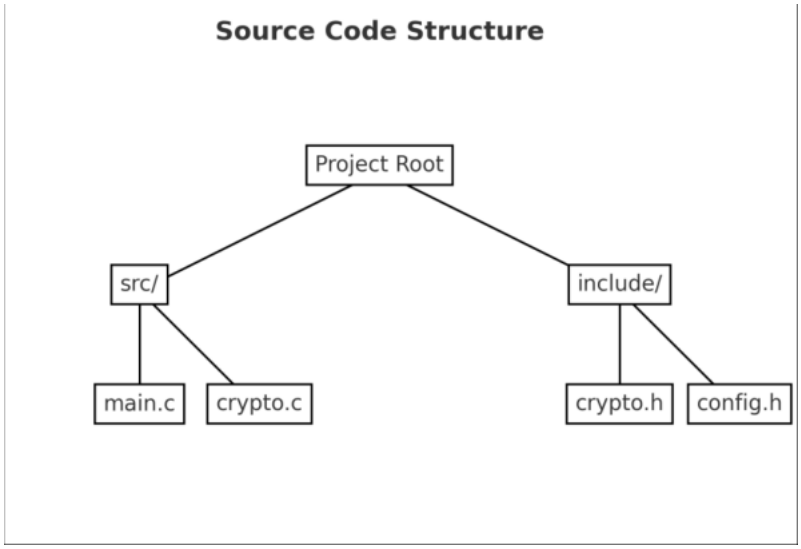


Figure 3-5 그림 제목

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			

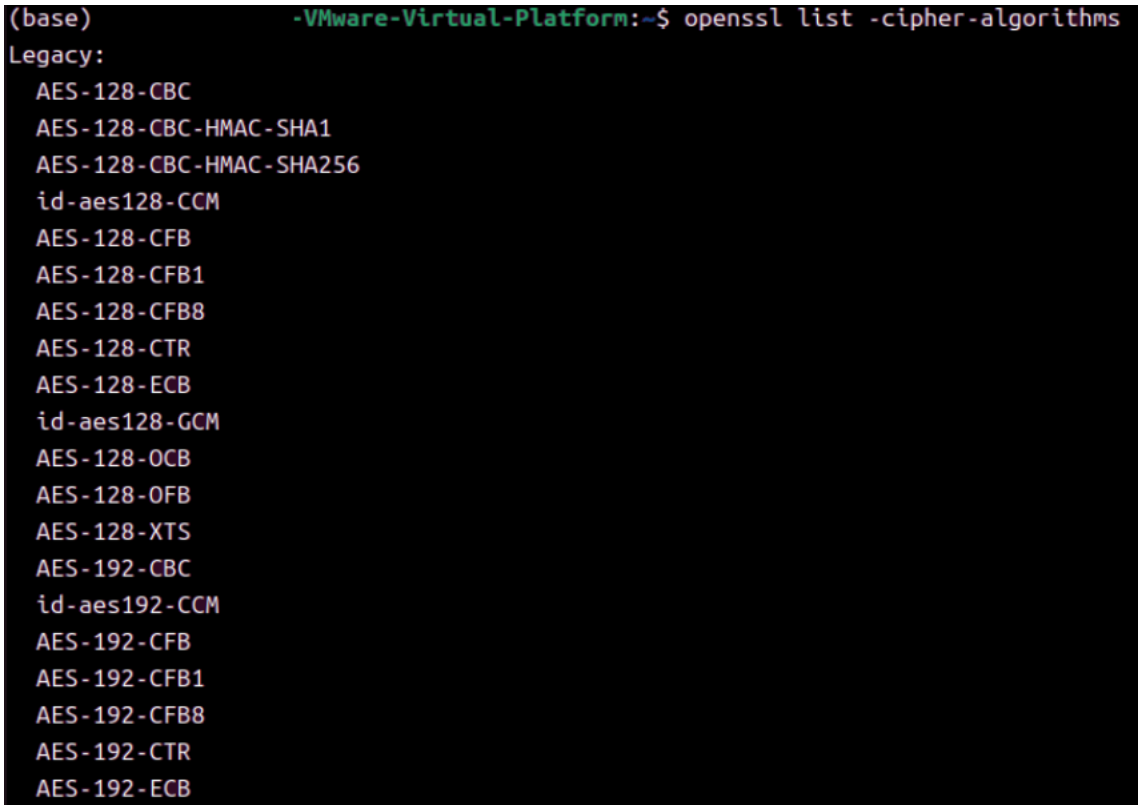


Figure 3-6 그림 제목

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 ”>

1.4 TE02.07.01

1.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.07.01	암호경계 내의 구성요소 확인	암호모듈 검사

1.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-9 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

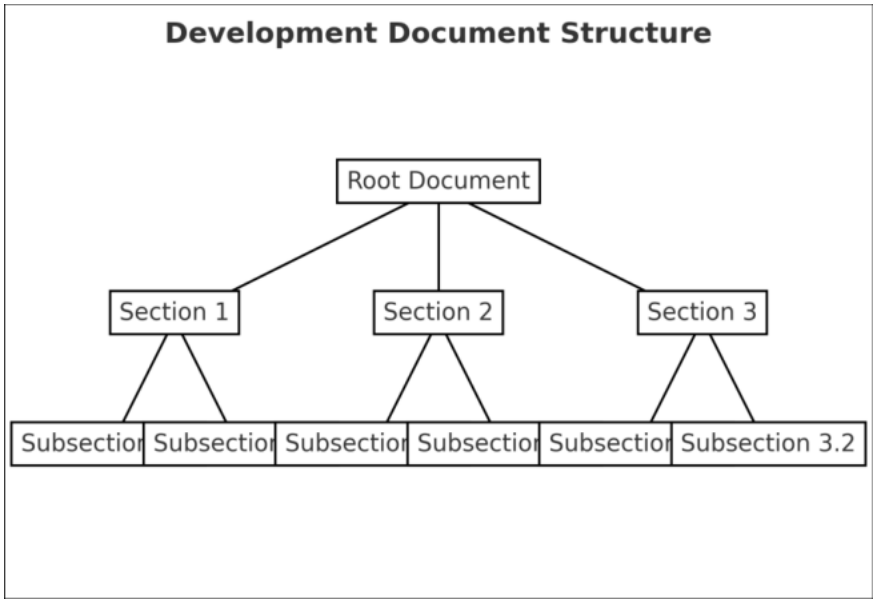


Figure 3-7 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-10 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

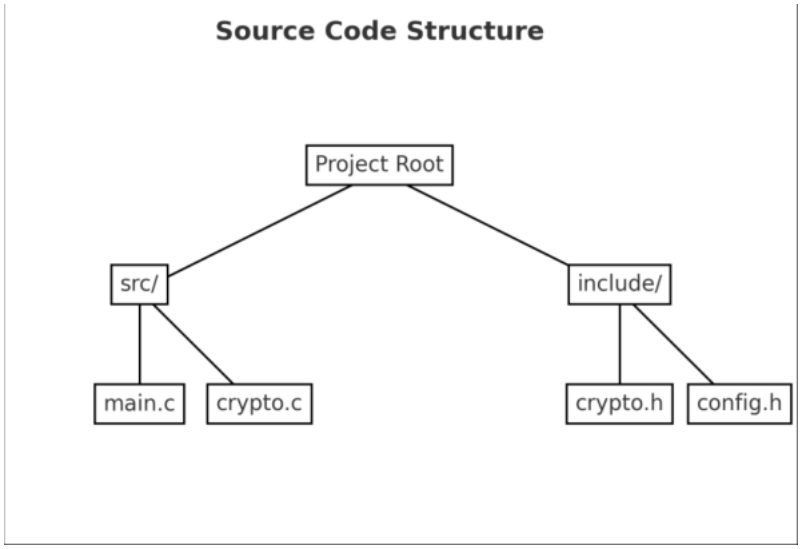


Figure 3-8 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-11 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

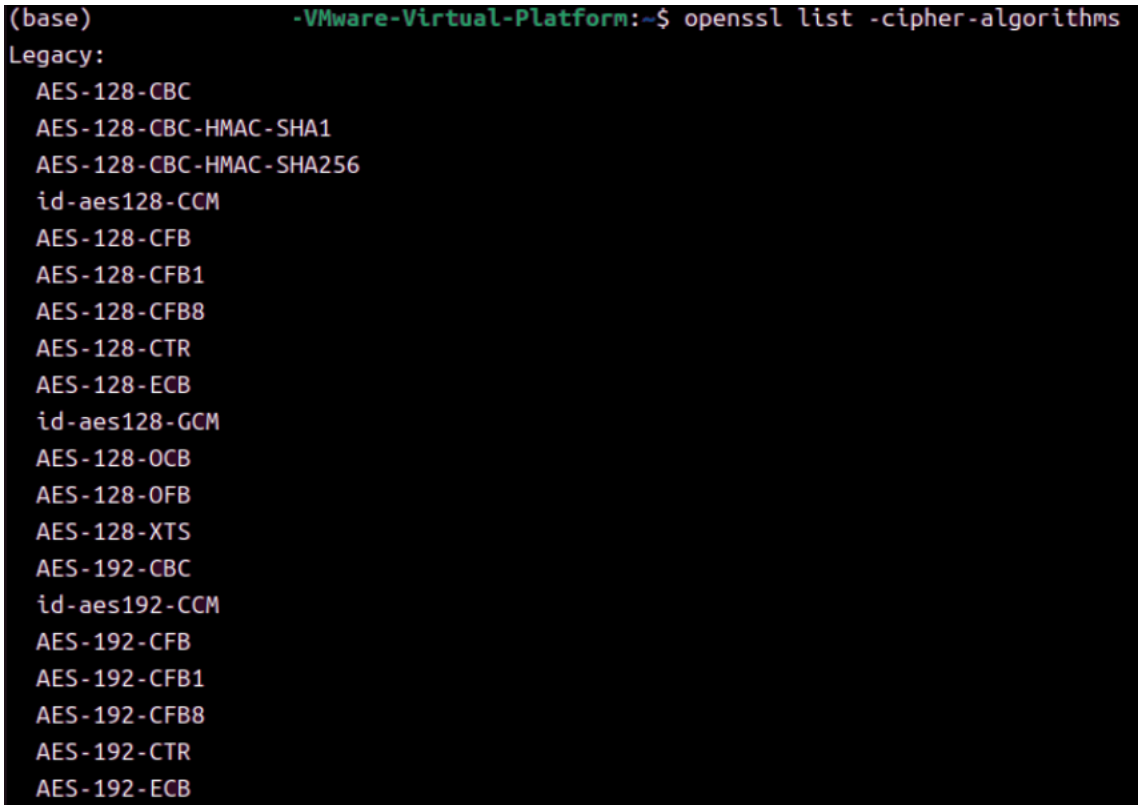


Figure 3-9 그림 제목

1.4.3 판정근거

Table 3-12 TE02.07.01 시험결과 판정근거

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

1.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.5 TE02.07.02

1.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.07.02	명세되지 않는 구성요소 존재 여부 확인	암호모듈 검사

1.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-13 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

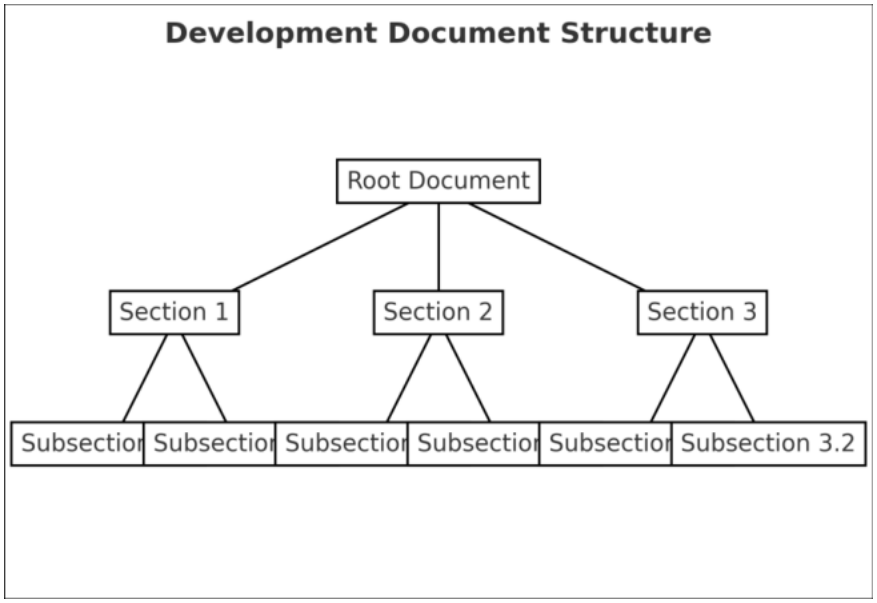


Figure 3-10 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-14 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

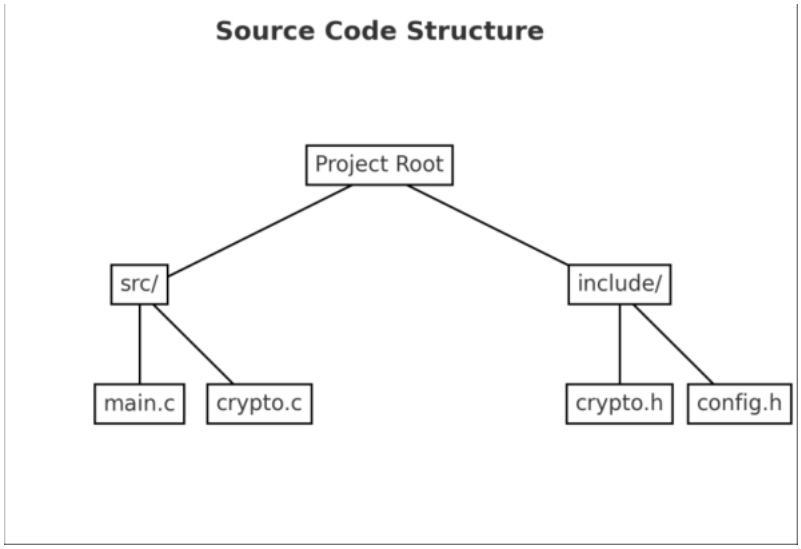


Figure 3-11 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-15 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

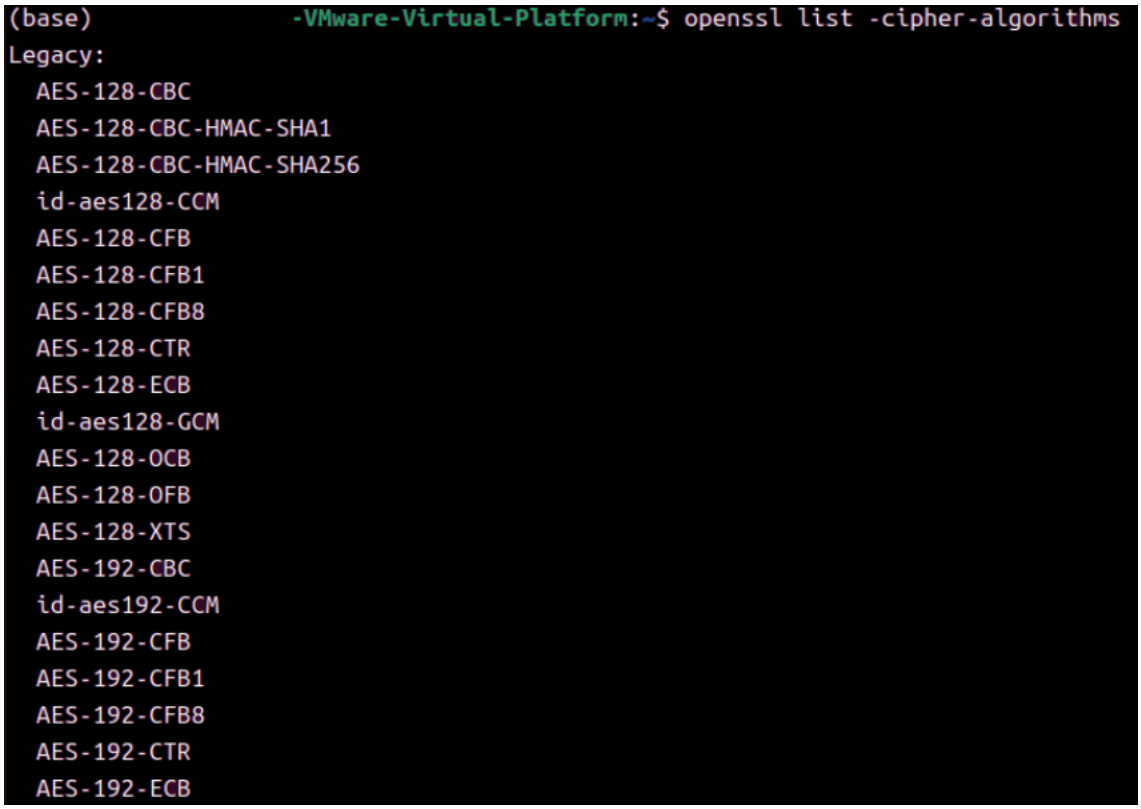


Figure 3-12 그림 제목

1.5.3 판정근거

Table 3-16 TE02.07.02 시험결과 판정근거

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

1.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.6 TE02.09.01

1.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.09.01	암호경계 내 보안 관련 요소 및 알고리즘 정보	개발문서 검토

1.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-17 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

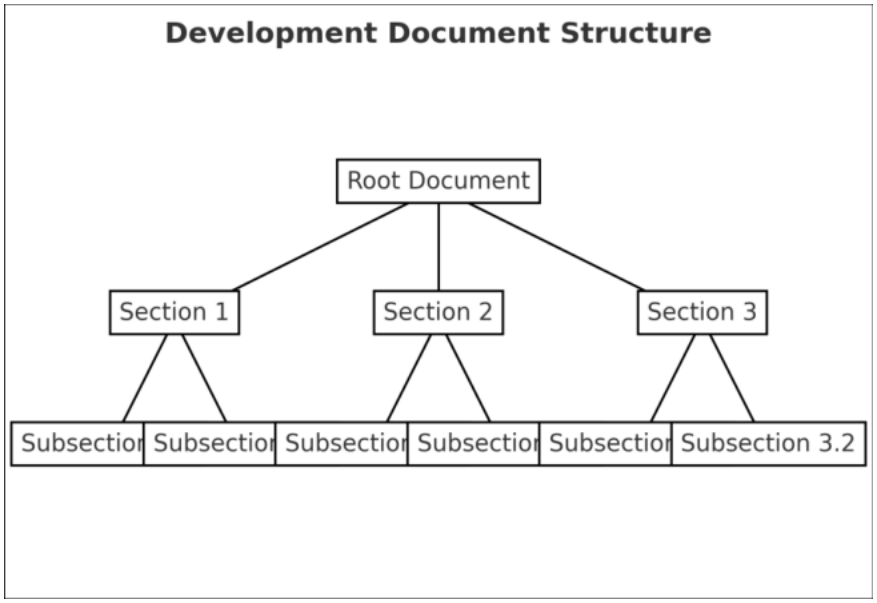


Figure 3-13 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-18 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

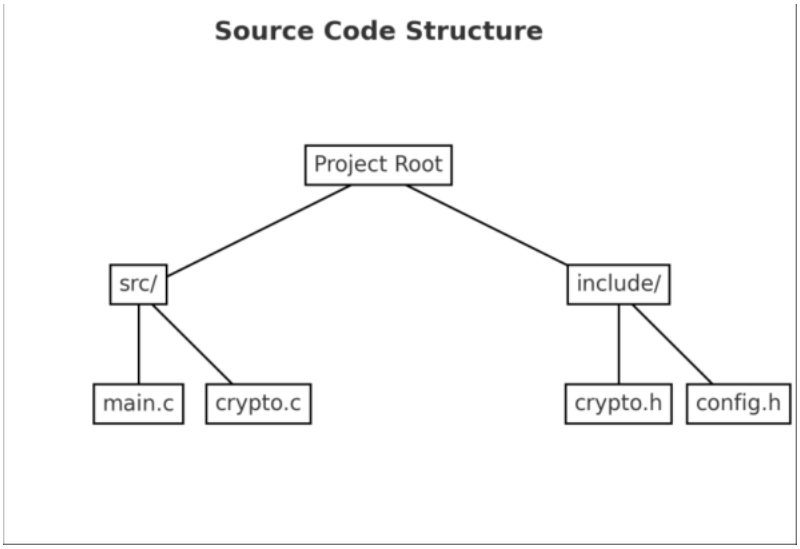


Figure 3-14 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-19 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

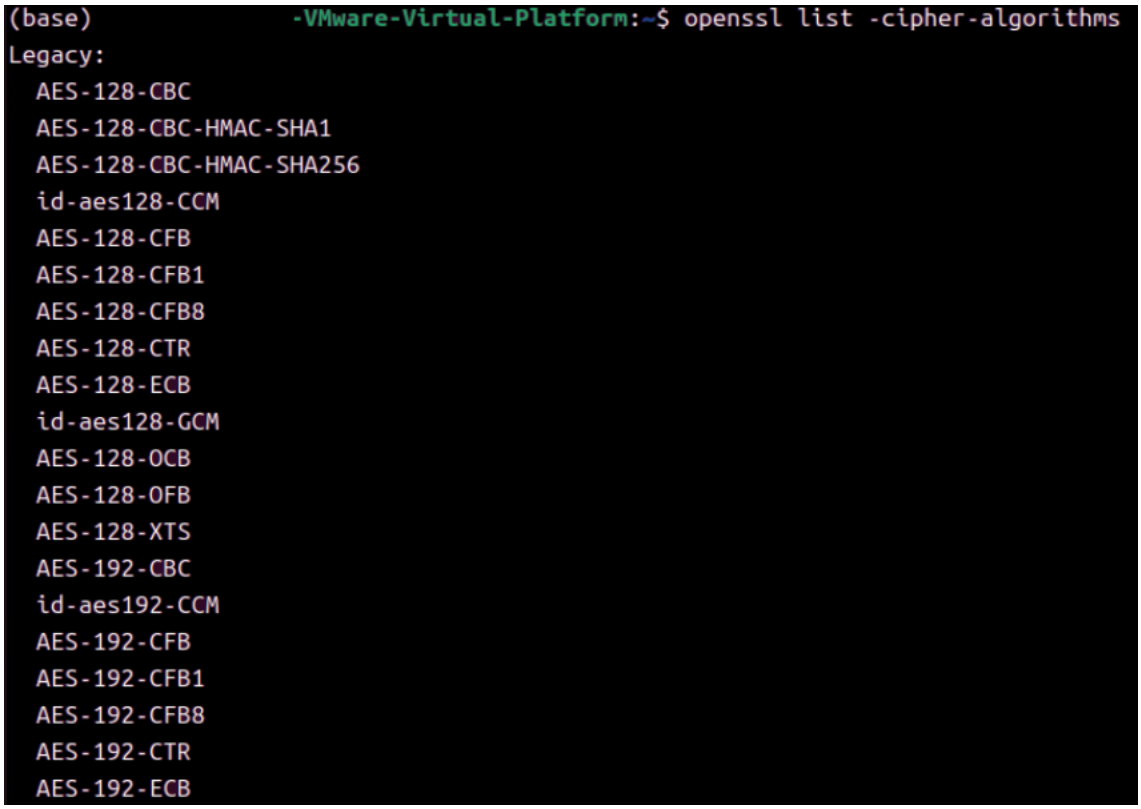


Figure 3-15 그림 제목

1.6.3 판정근거

Table 3-20 TE02.09.01 시험결과 판정근거

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

1.6.4 판정결과

차) 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.7 TE02.10.01

1.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.10.01	비보안함수의 검증대상 동작모드 방해·손상 여부	개발문서 검토

1.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-21 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

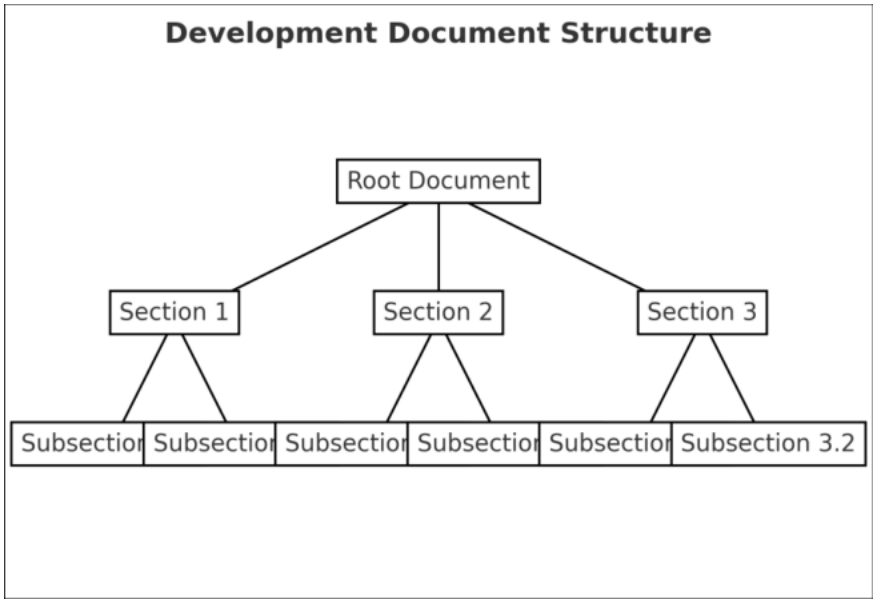


Figure 3-16 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-22 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

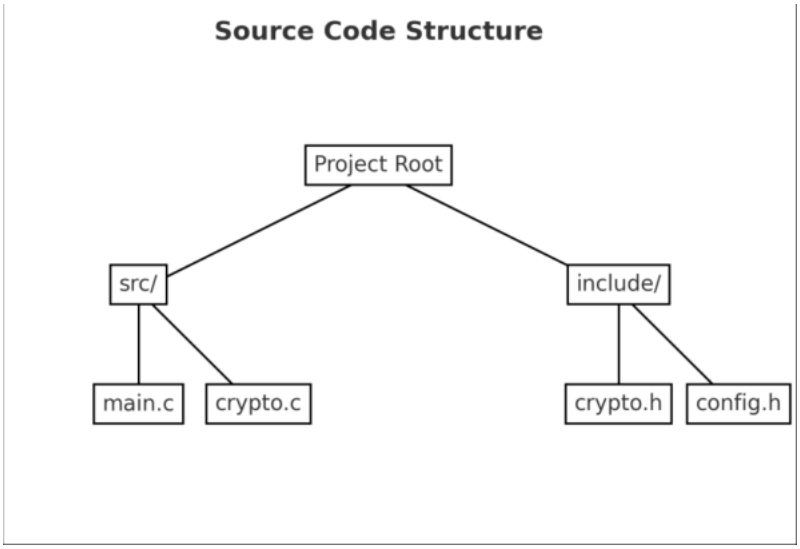


Figure 3-17 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-23 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

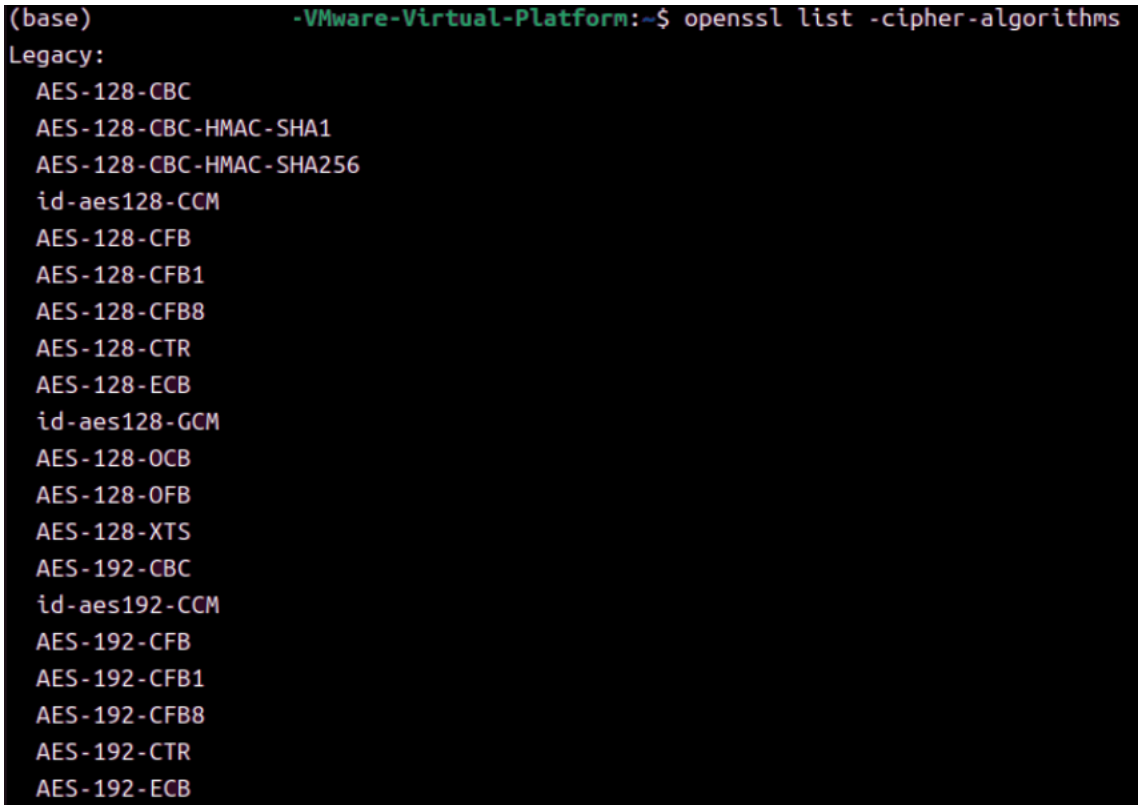


Figure 3-18 그림 제목

1.7.3 판정근거

Table 3-24 TE02.10.01 시험결과 판정근거

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

1.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.8 TE02.10.02

1.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.10.02	검증대상 동작모드를 방해·손상시키지 않는 근거	개발문서 검토

1.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-25 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

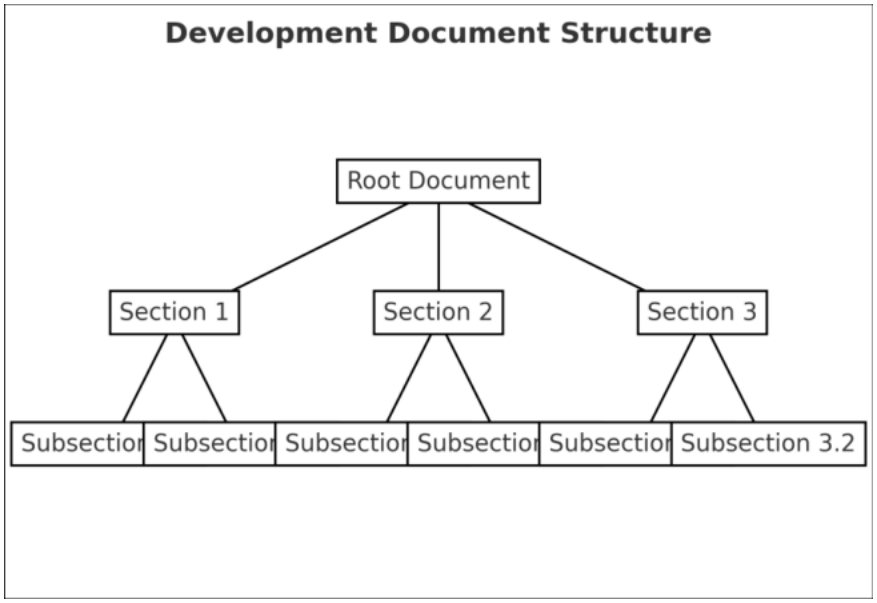


Figure 3-19 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-26 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

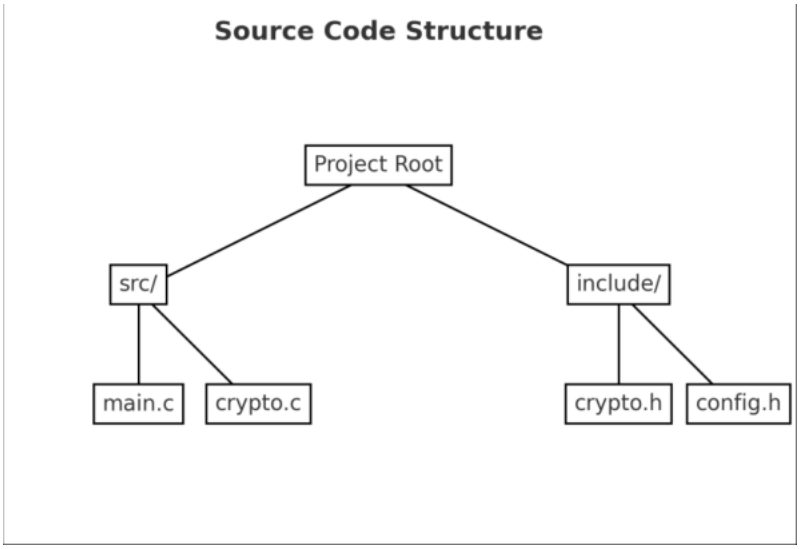


Figure 3-20 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-27 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

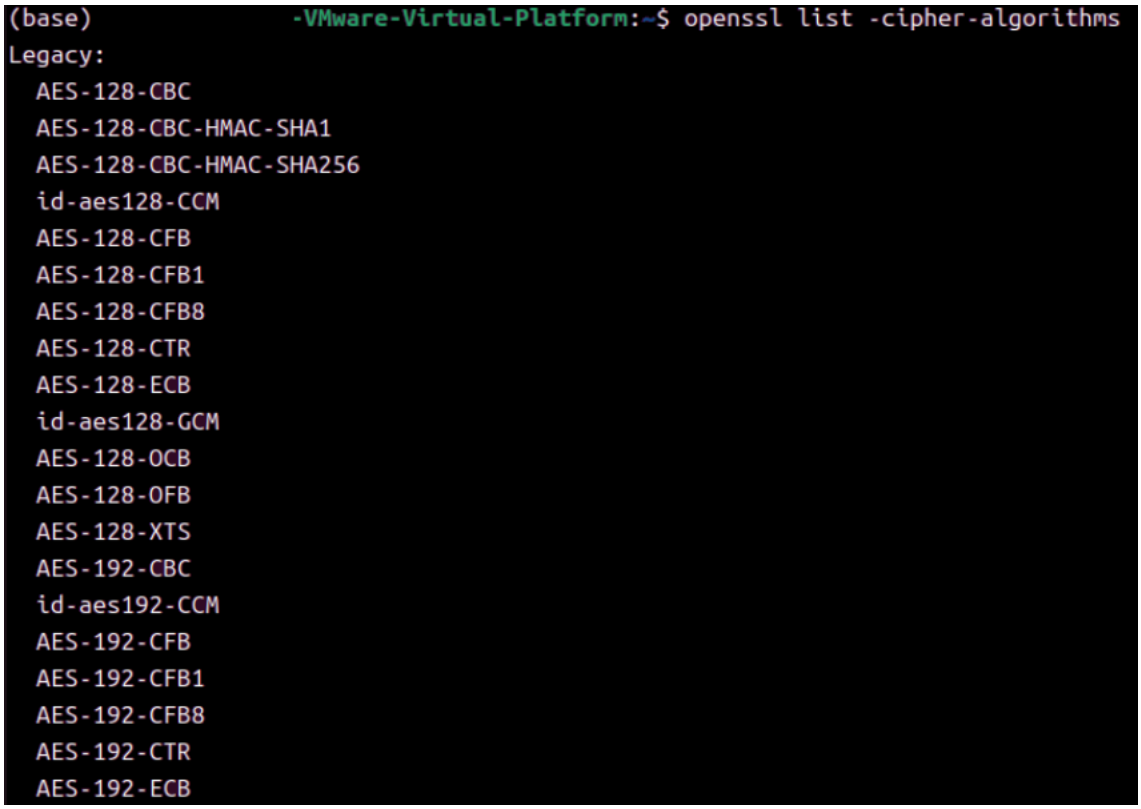


Figure 3-21 그림 제목

1.8.3 판정근거

Table 3-28 TE02.10.01 시험결과 판정근거

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

1.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.9 TE02.11.01

1.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.11.01	구성요소와 암호모듈 명칭의 적절성	개발문서 검토

1.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-29 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

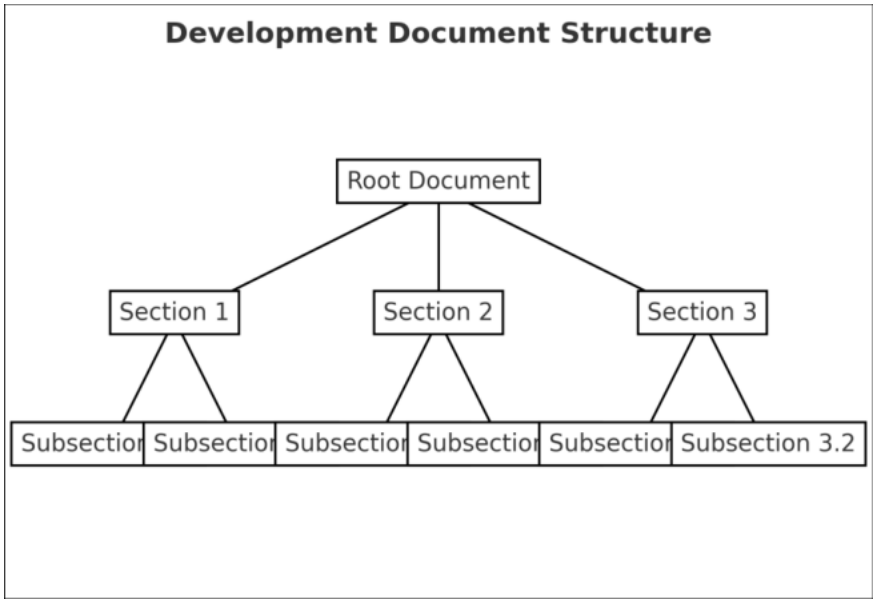


Figure 3-22 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-30 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

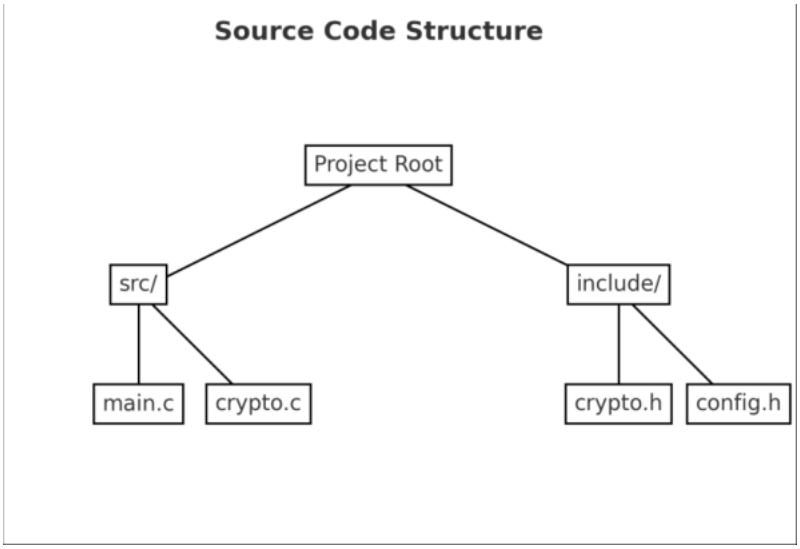


Figure 3-23 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-31 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

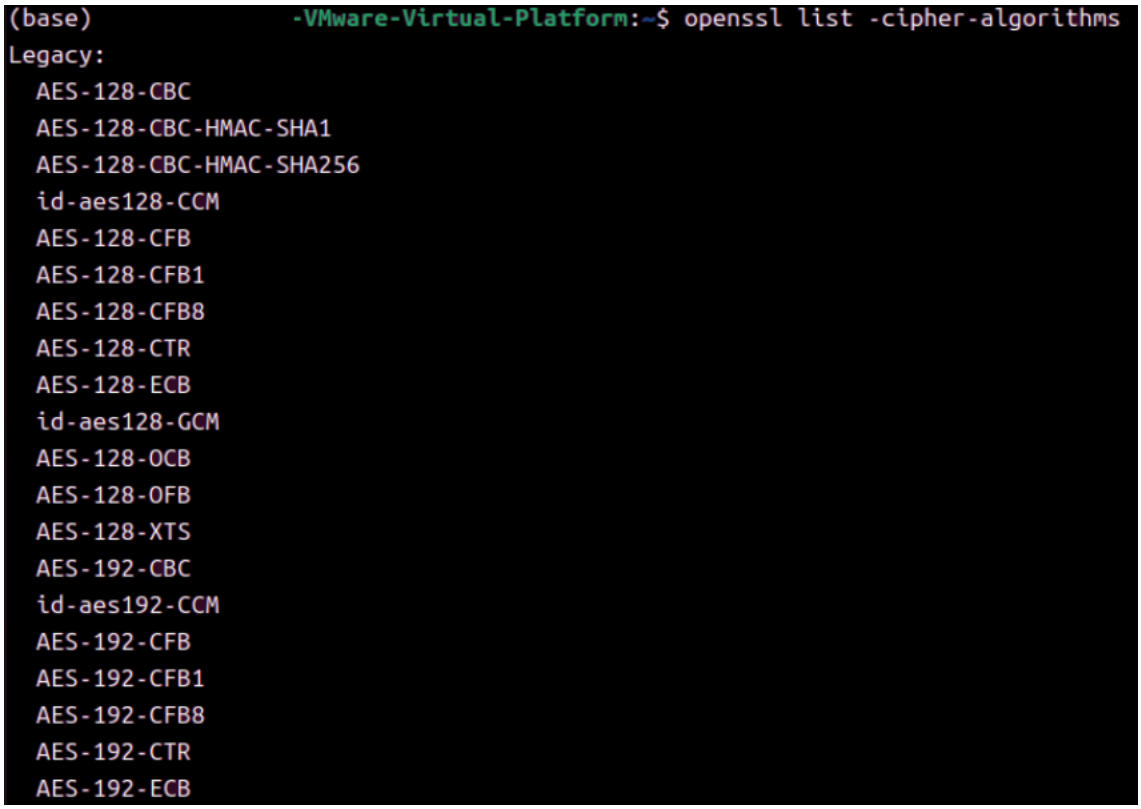


Figure 3-24 그림 제목

1.9.3 판정근거

Table 3-32 TE02.11.01 시험결과 판정근거

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

1.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.10 TE02.11.02

1.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.11.02	암호모듈 명칭과 일치하지 않는 구성요소 및 기능	개발문서 검토

1.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-33 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

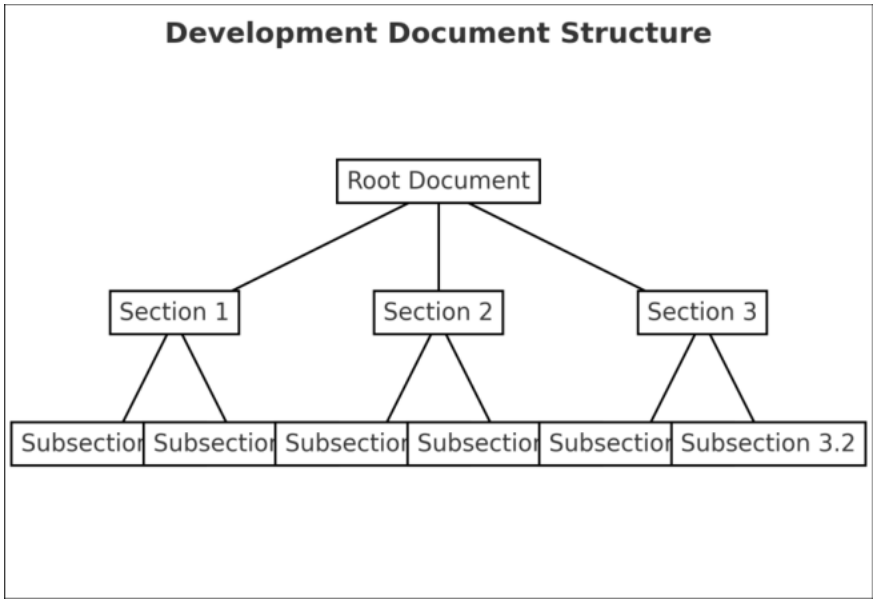


Figure 3-25 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-34 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

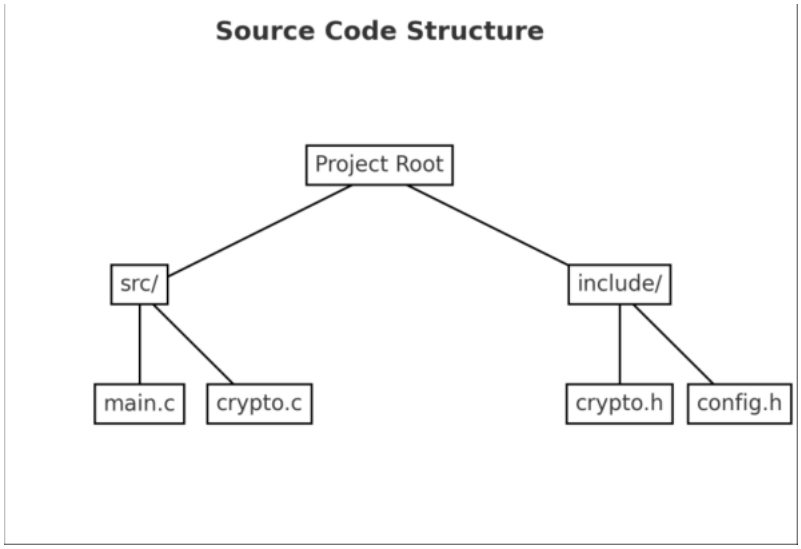


Figure 3-26 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-35 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

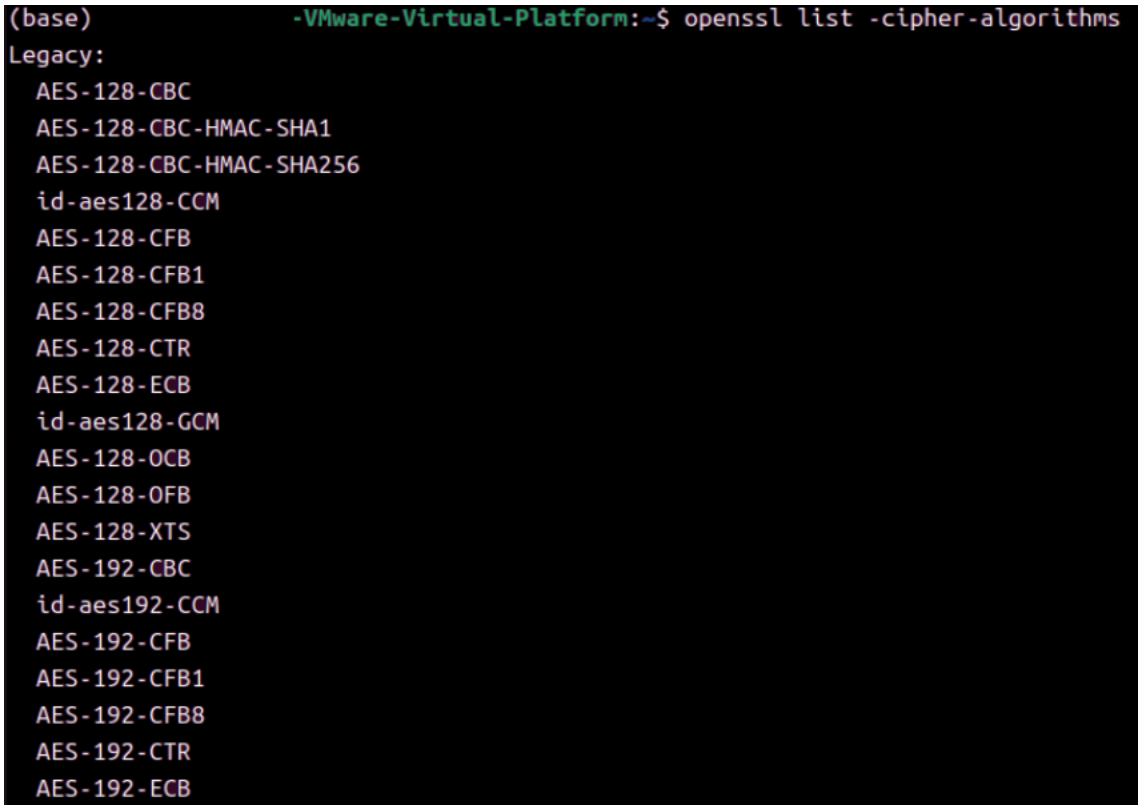


Figure 3-27 그림 제목

1.10.3 판정근거

Table 3-36 TE02.11.02 시험결과 판정근거

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

1.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.11 TE02.02.01

1.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.12.01	구성요소별 버전 관리	개발문서 검토

1.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-37 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

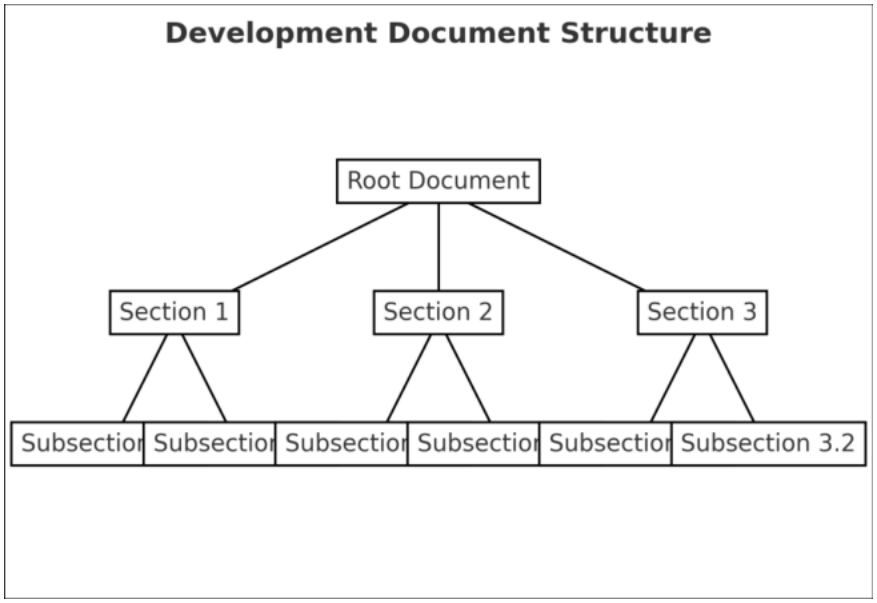


Figure 3-28 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-38 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

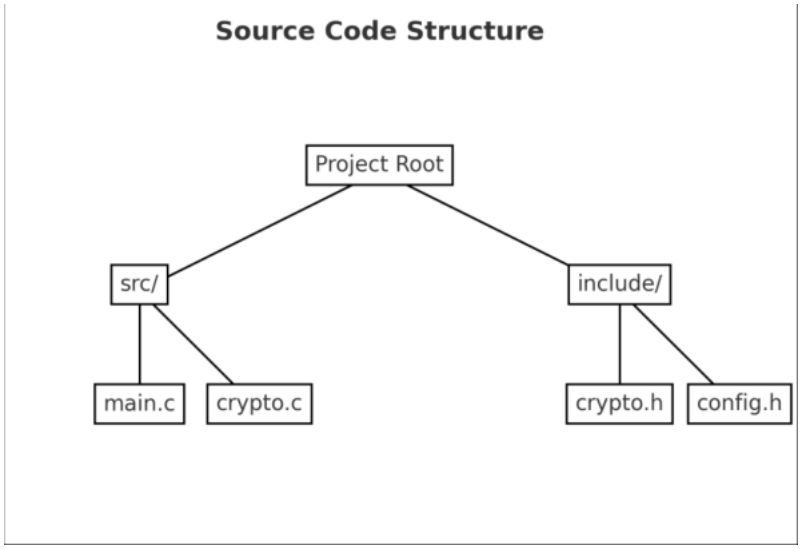


Figure 3-29 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-39 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

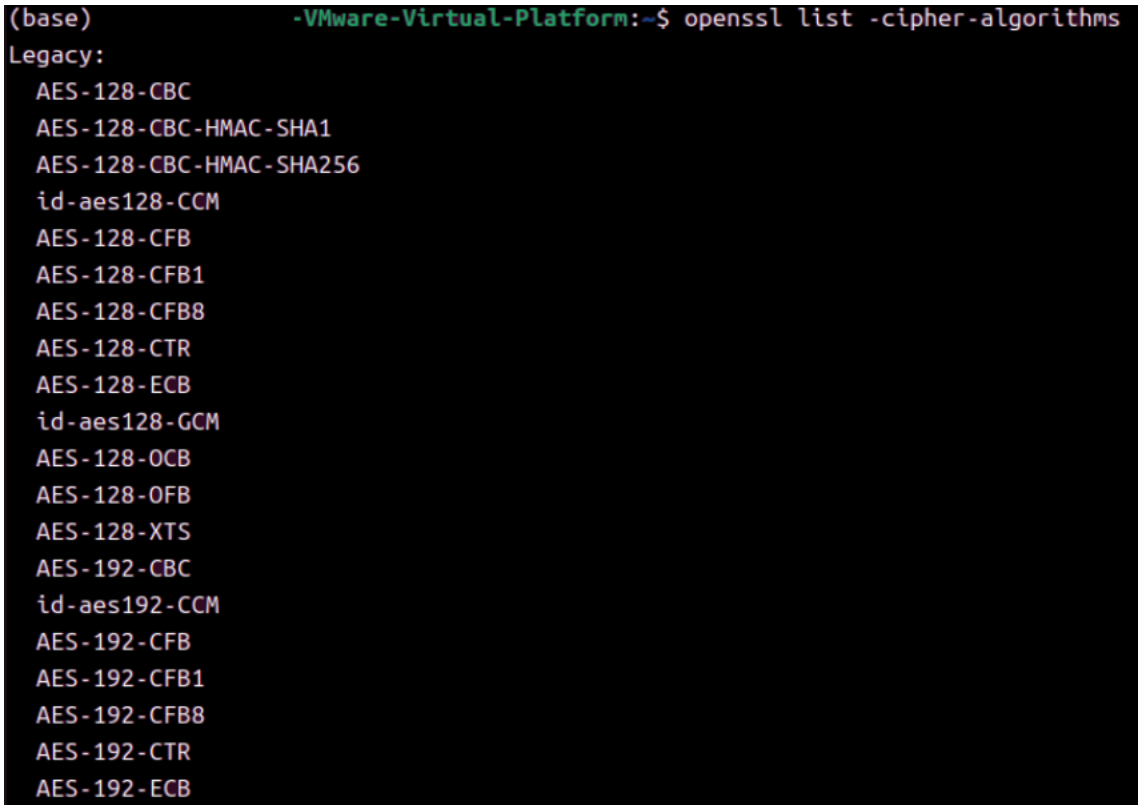


Figure 3-30 그림 제목

1.11.3 판정근거

Table 3-40 TE02.12.01 시험결과 판정근거

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

1.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.12 TE02.13.01

1.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.13.01	경계 외부 구성요소의 검증대상 동작모드 방해 여부	개발문서 검토

1.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-41 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

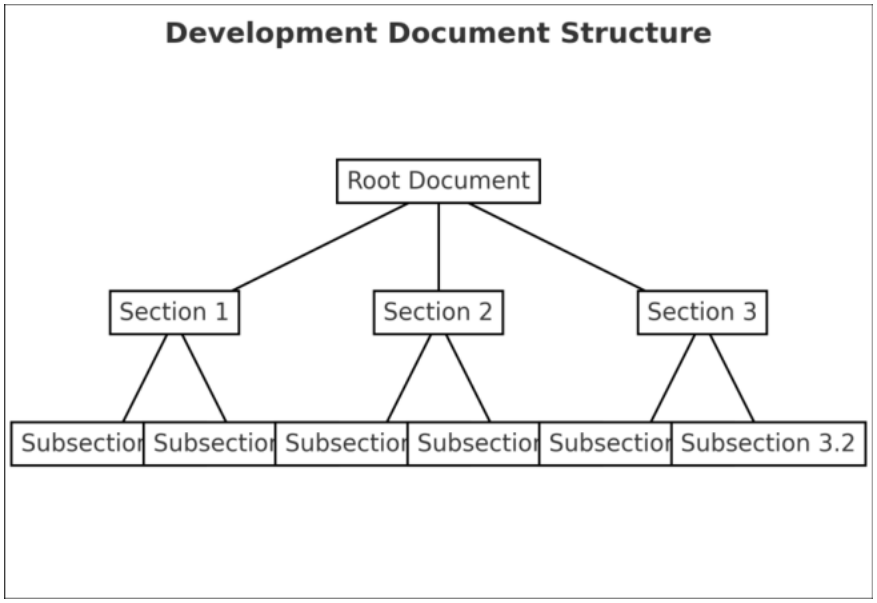


Figure 3-31 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-42 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

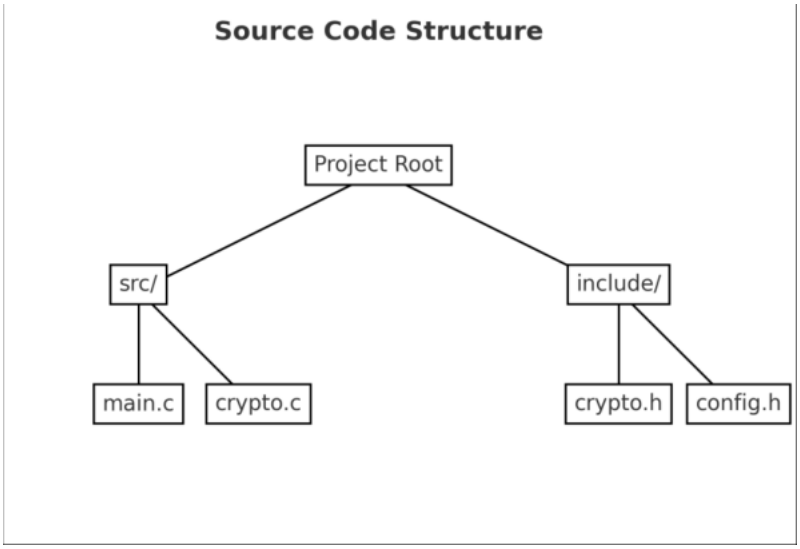


Figure 3-32 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-43 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

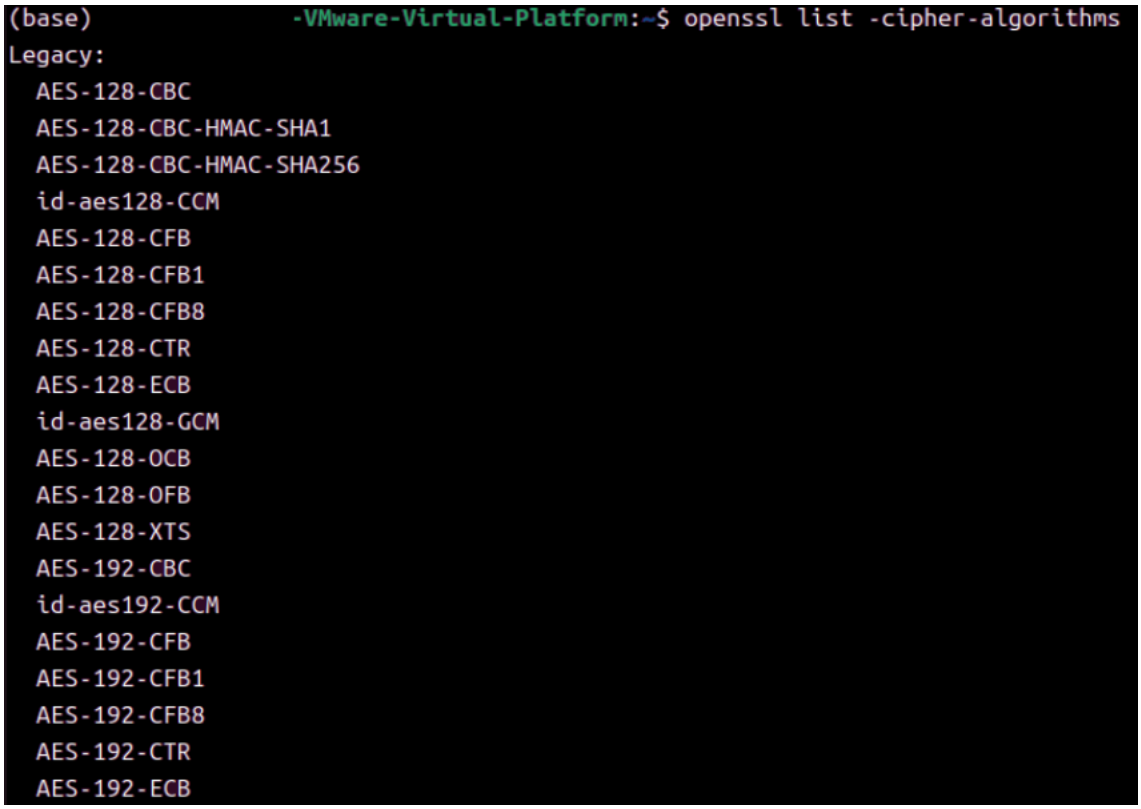


Figure 3-33 그림 제목

1.12.3 판정근거

Table 3-44 TE02.13.01 시험결과 판정근거

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

1.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.13 TE02.14.01

1.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.14.01	보안요구사항 적용받지 않는 구성요소 존재 여부	개발문서 검토

1.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-45 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

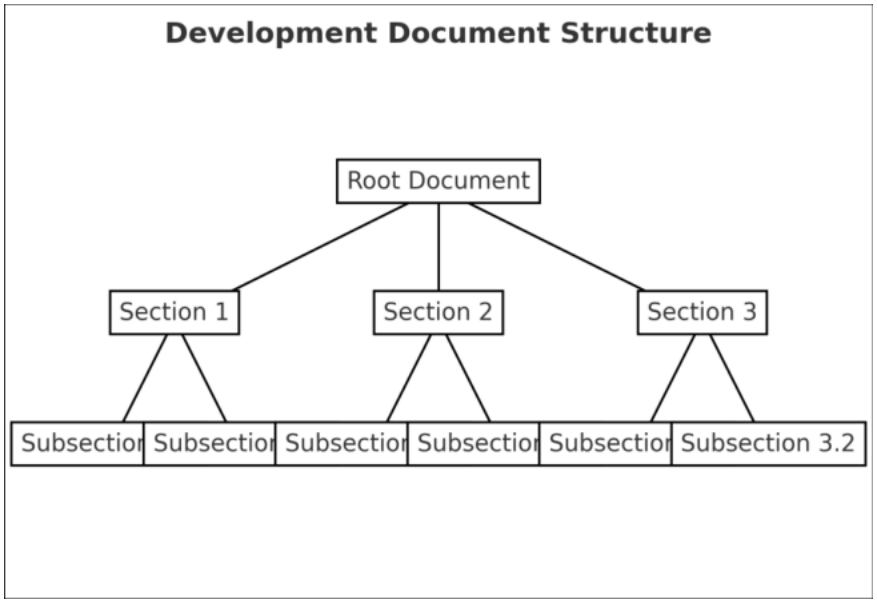


Figure 3-34 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-46 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

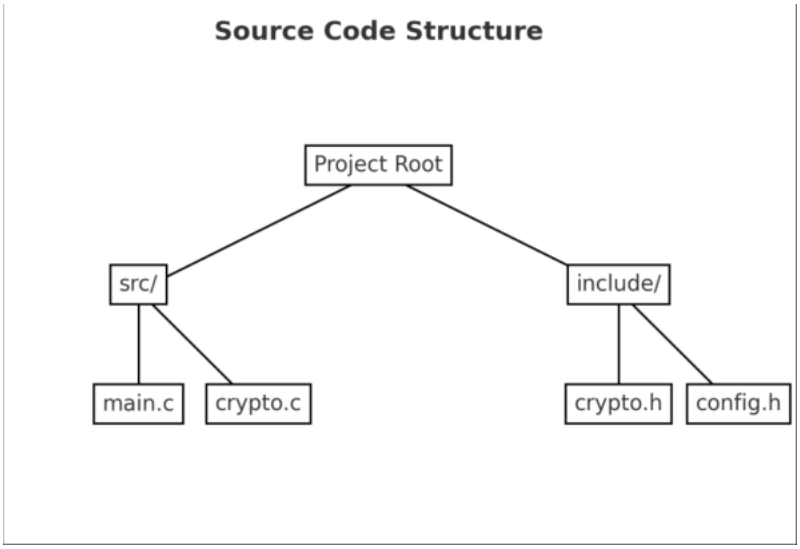


Figure 3-35 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-47 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

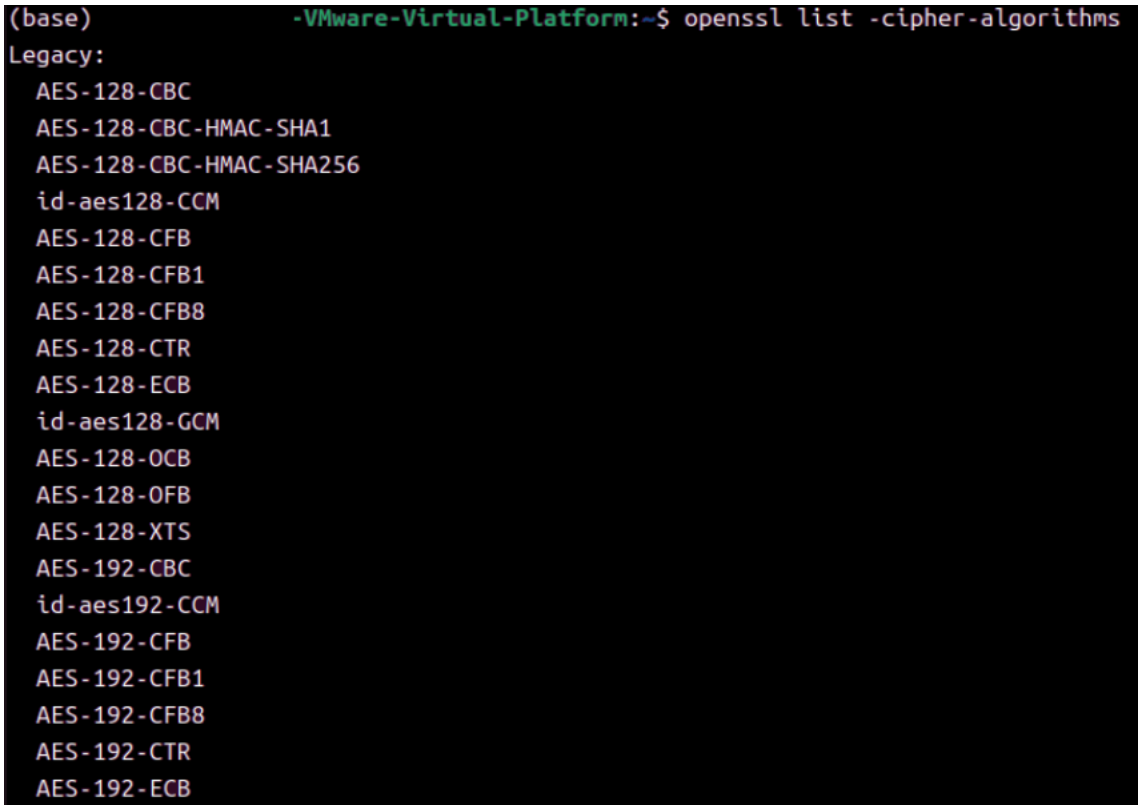


Figure 3-36 그림 제목

1.13.3 판정근거

Table 3-48 TE02.14.01 시험결과 판정근거

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

1.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.14 TE02.14.02

1.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.14.02	보안요구사항 적용받지 않는 구성요소 근거	개발문서 검토

1.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-49 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

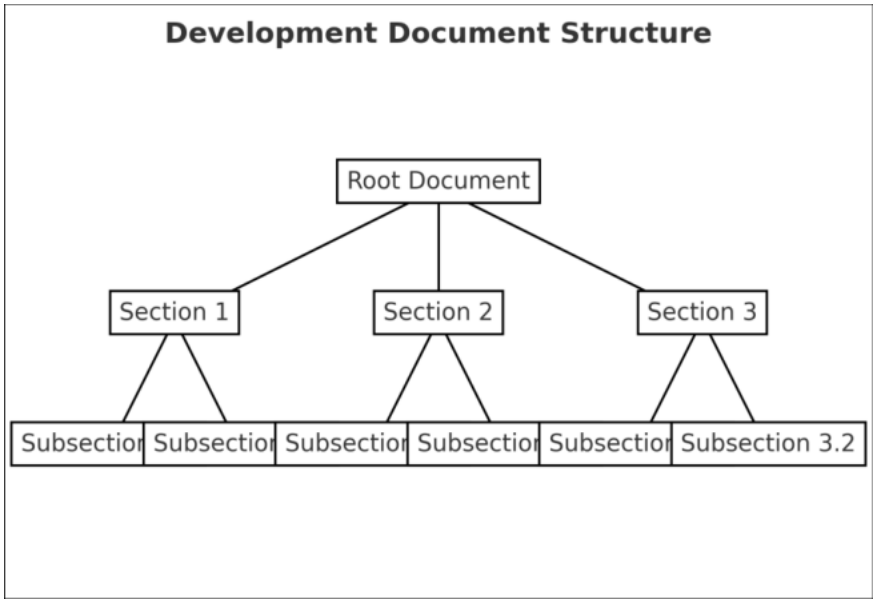


Figure 3-37 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-50 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

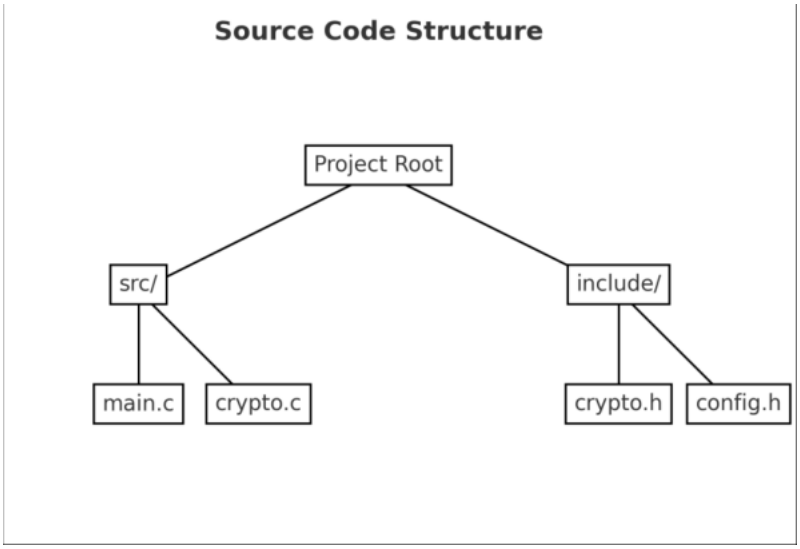


Figure 3-38 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-51 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

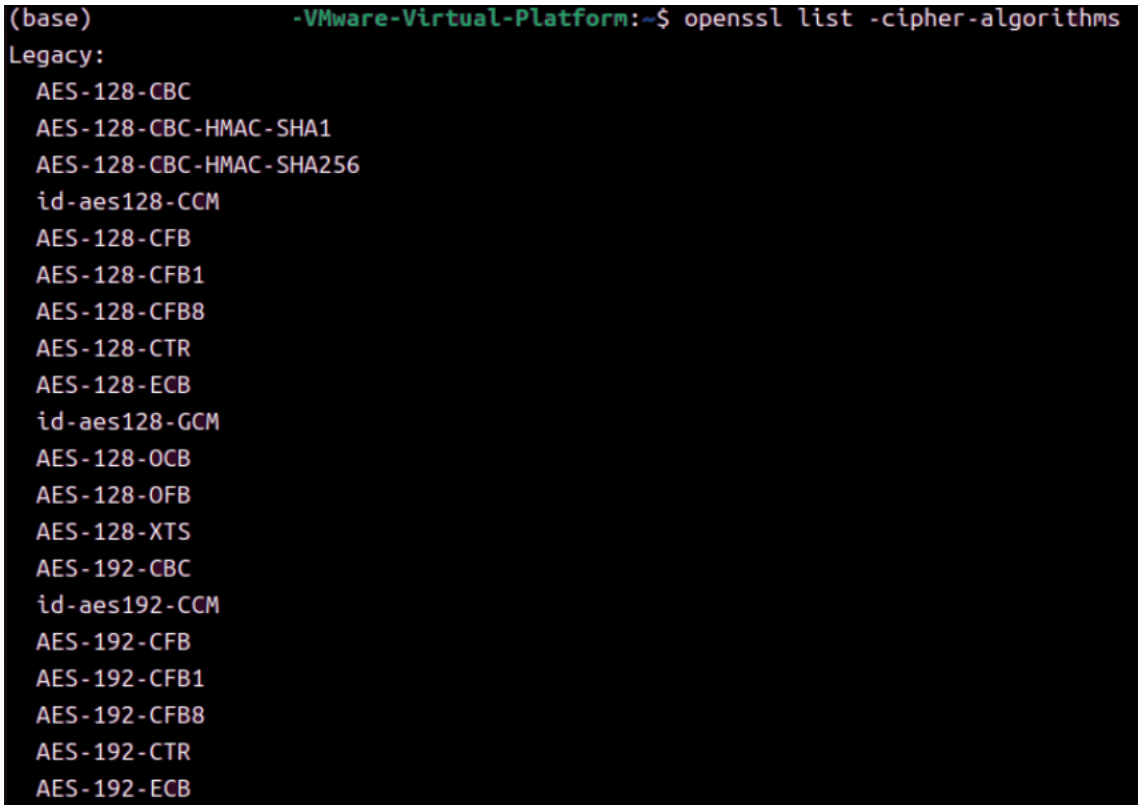


Figure 3-39 그림 제목

1.14.3 판정근거

Table 3-52 TE02.14.02 시험결과 판정근거

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

1.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.15 TE02.16.01

1.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.16.01	구성요소 목록 서술	개발문서 검토

1.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-53 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

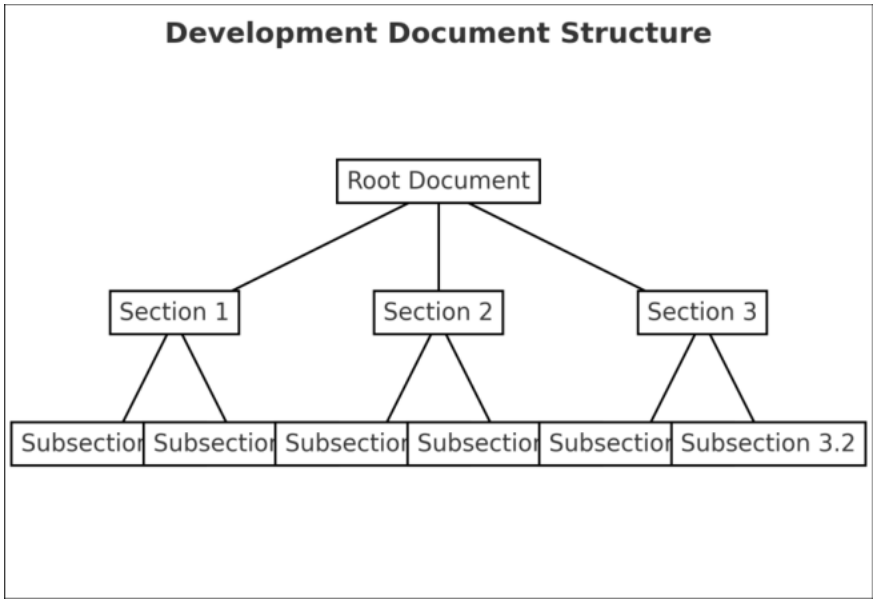


Figure 3-40 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-54 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

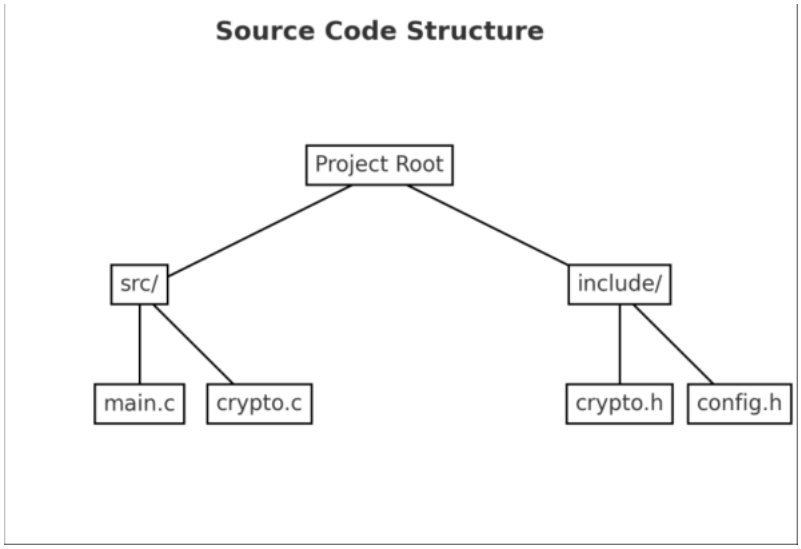


Figure 3-41 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-55 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

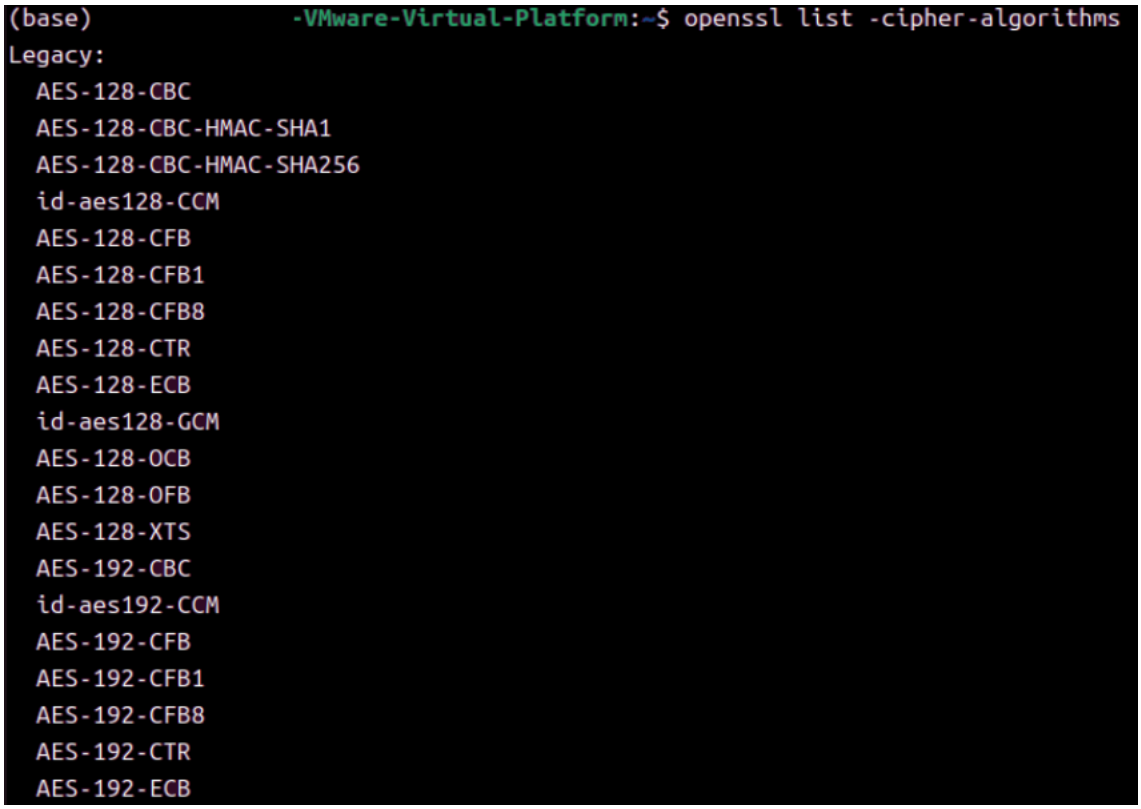


Figure 3-42 그림 제목

1.15.3 판정근거

Table 3-56 TE02.16.01 시험결과 판정근거

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

1.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.16 TE02.16.02

1.16.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.16.02	구성요소 목록 확인	암호모듈 검사

1.16.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-57 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

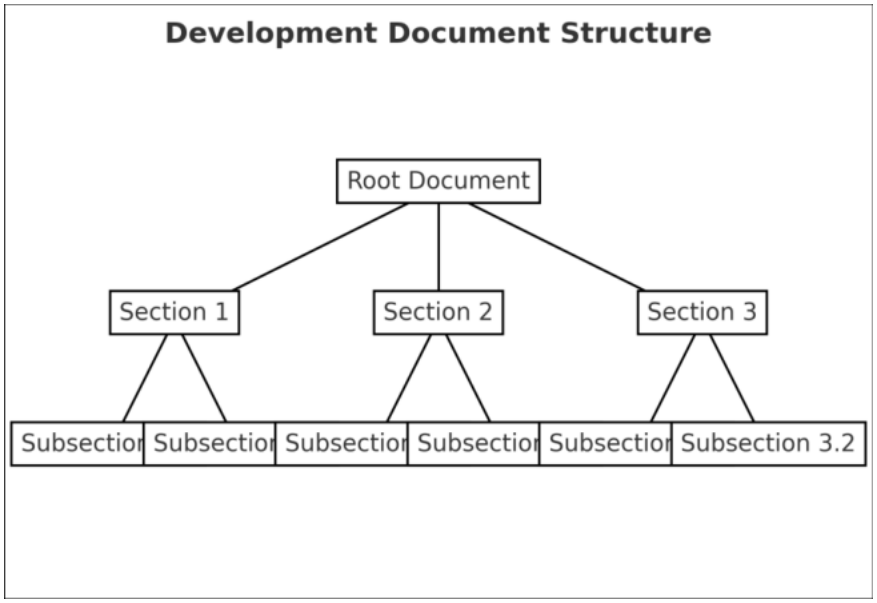


Figure 3-43 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-58 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

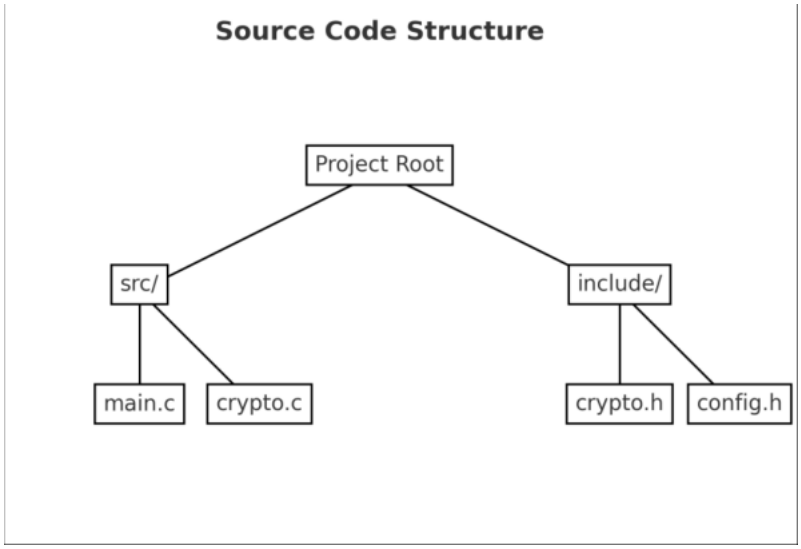


Figure 3-44 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-59 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

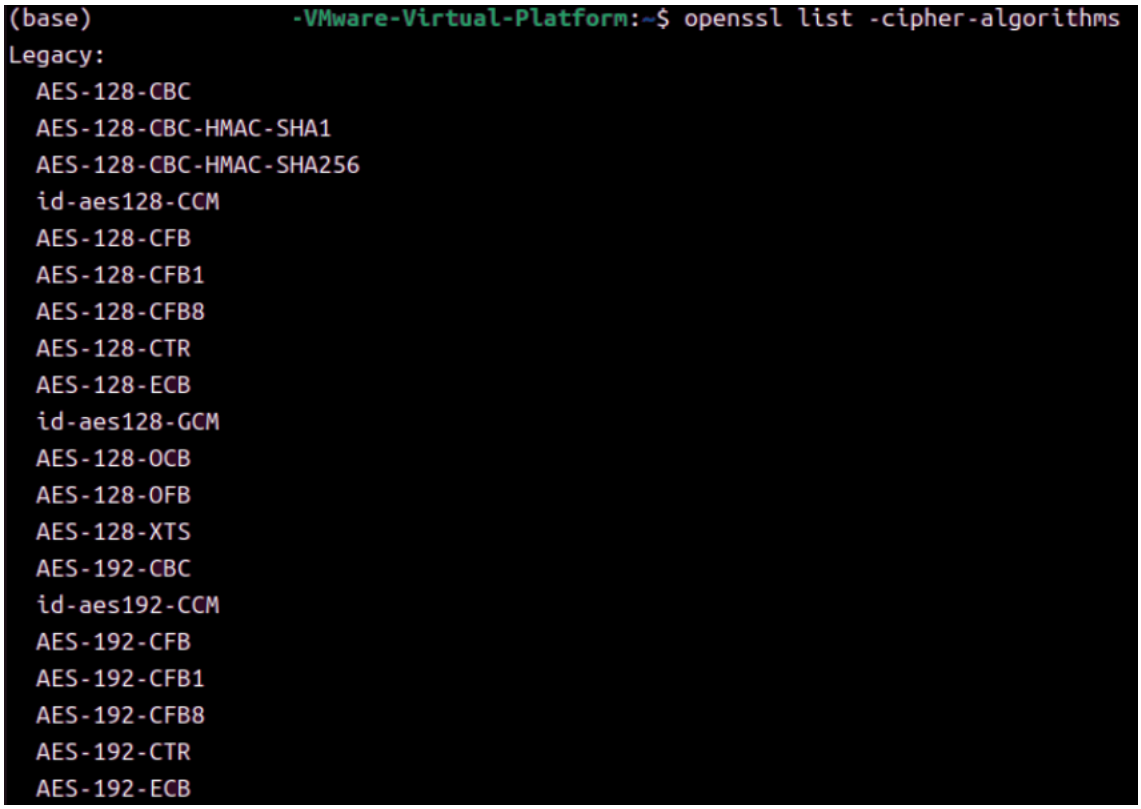


Figure 3-45 그림 제목

1.16.3 판정근거

Table 3-60 TE02.16.02 시험결과 판정근거

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

1.16.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.17 TE02.16.03

1.17.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.16.03	다른 절의 명세들과 구성요소 목록 일치 확인	개발문서 검토

1.17.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-61 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

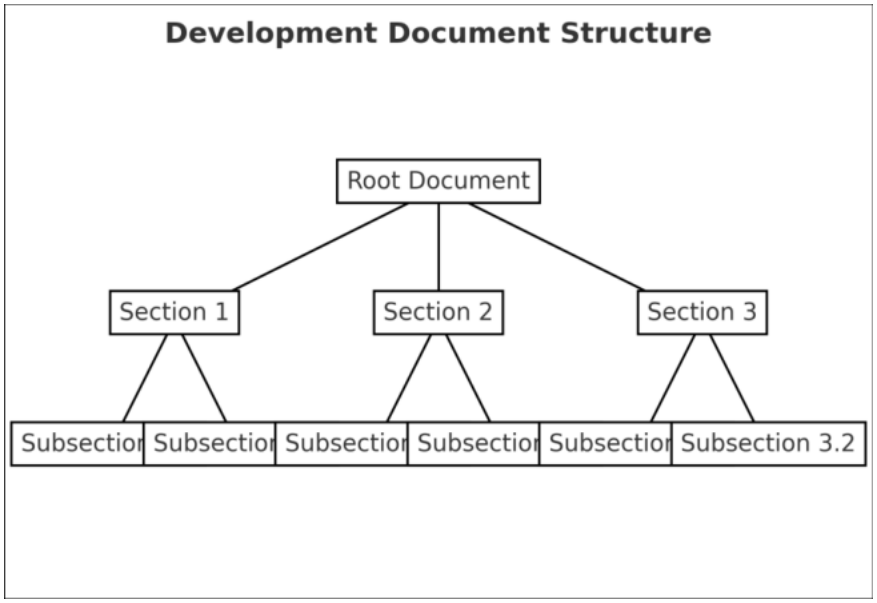


Figure 3-46 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-62 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

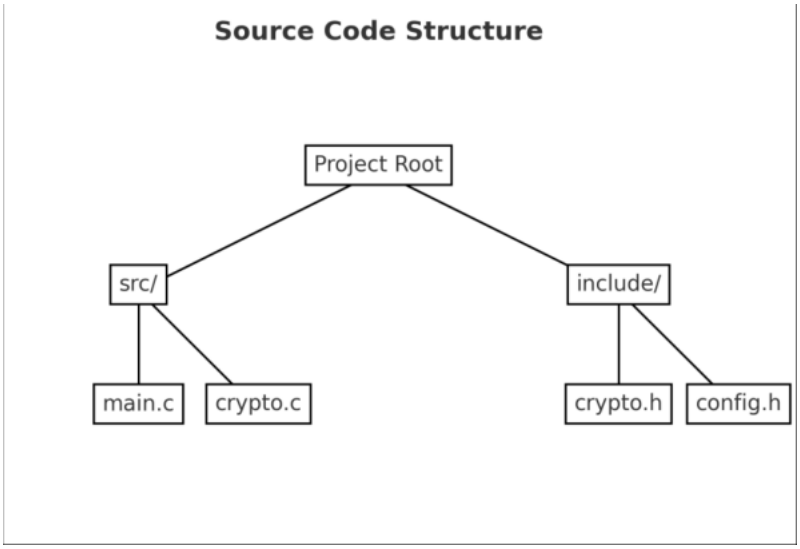


Figure 3-47 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-63 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

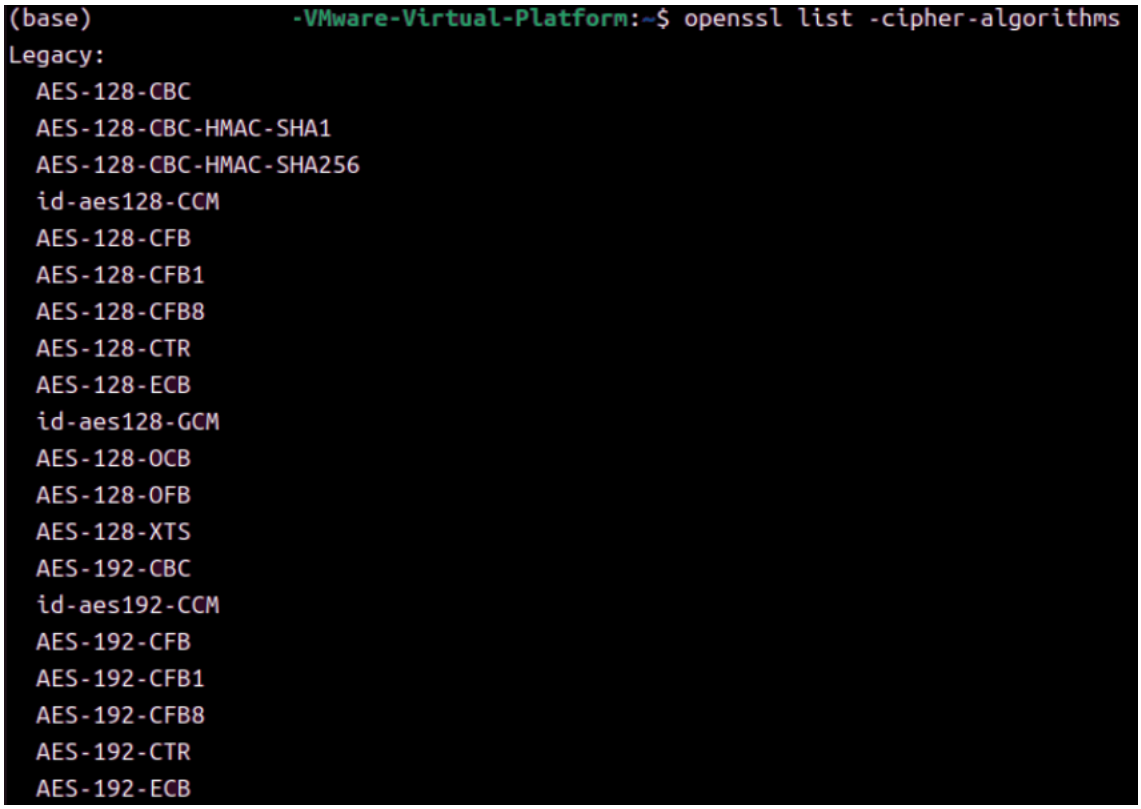


Figure 3-48 그림 제목

1.17.3 판정근거

Table 3-64 TE02.16.03 시험결과 판정근거

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

1.17.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.18 TE02.16.04

1.18.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.16.04	경계 외부 구성요소 목록	개발문서 검토

1.18.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-65 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

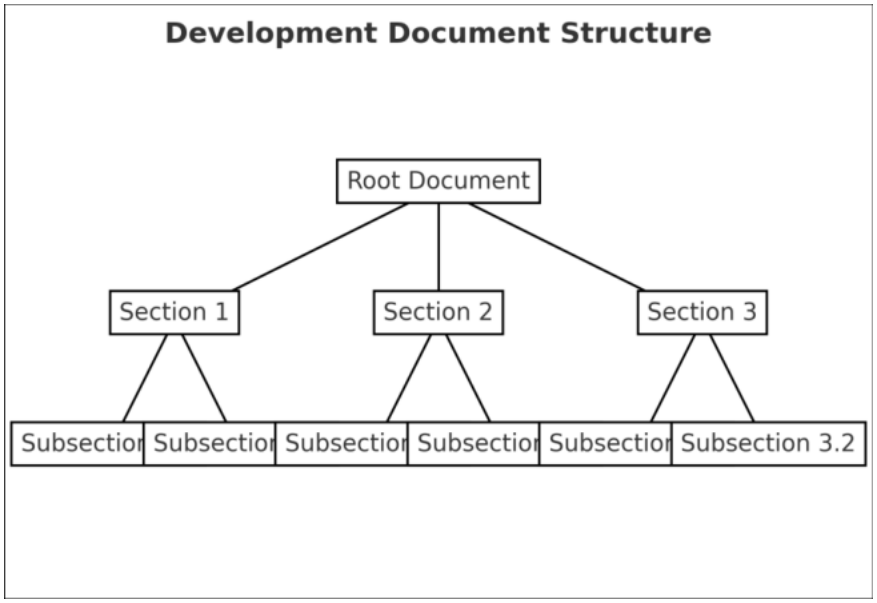


Figure 3-49 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-66 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

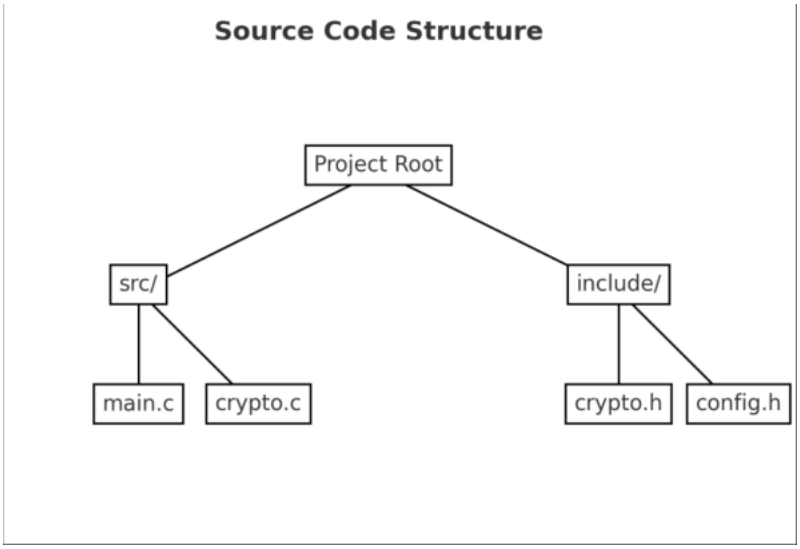


Figure 3-50 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-67 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

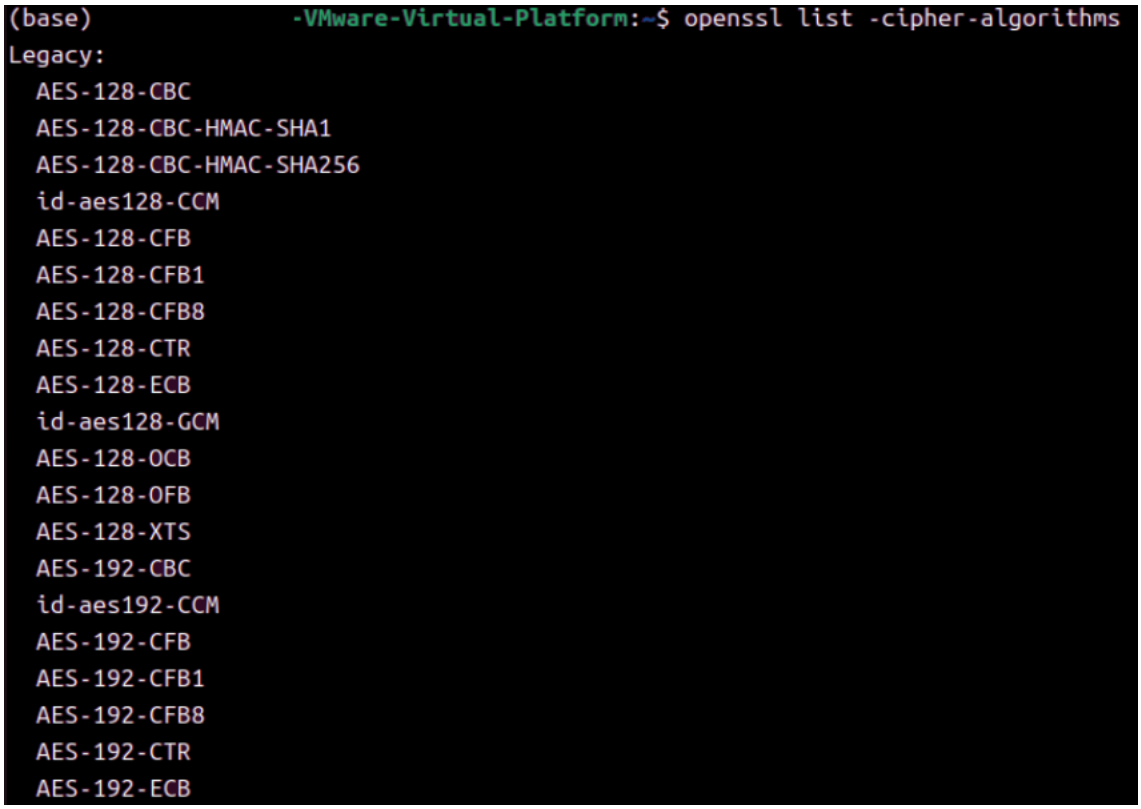


Figure 3-51 그림 제목

1.18.3 판정근거

Table 3-68 TE02.16.04 시험결과 판정근거

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

1.18.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.19 TE02.16.05

1.19.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.16.05	구성요소들의 연결 관계	개발문서 검토

1.19.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-69 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

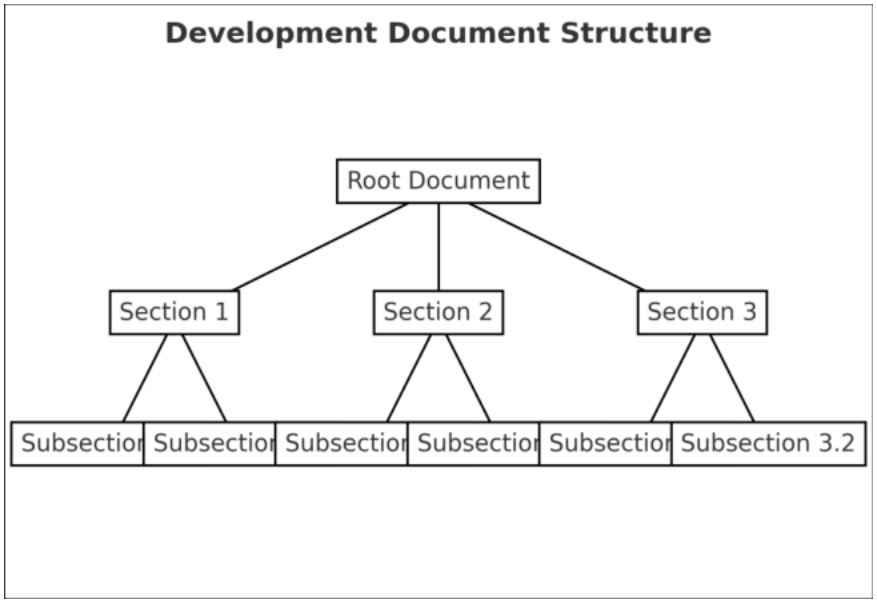


Figure 3-52 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-70 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

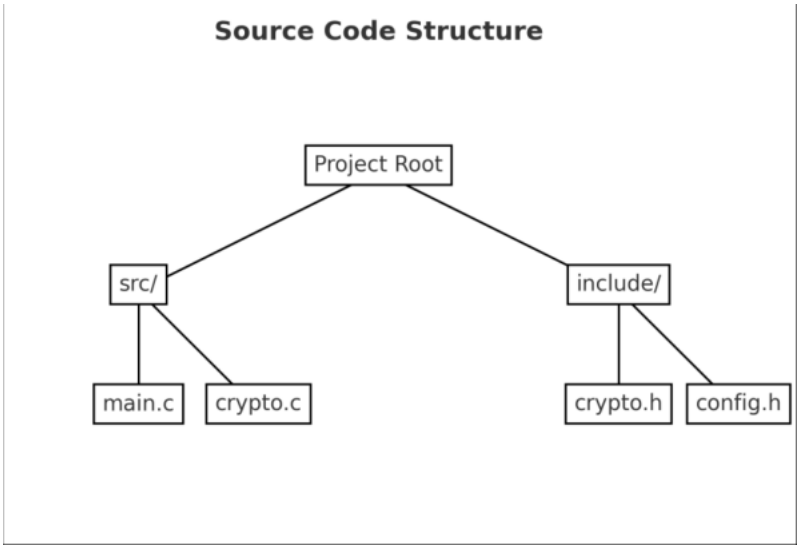


Figure 3-53 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-71 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

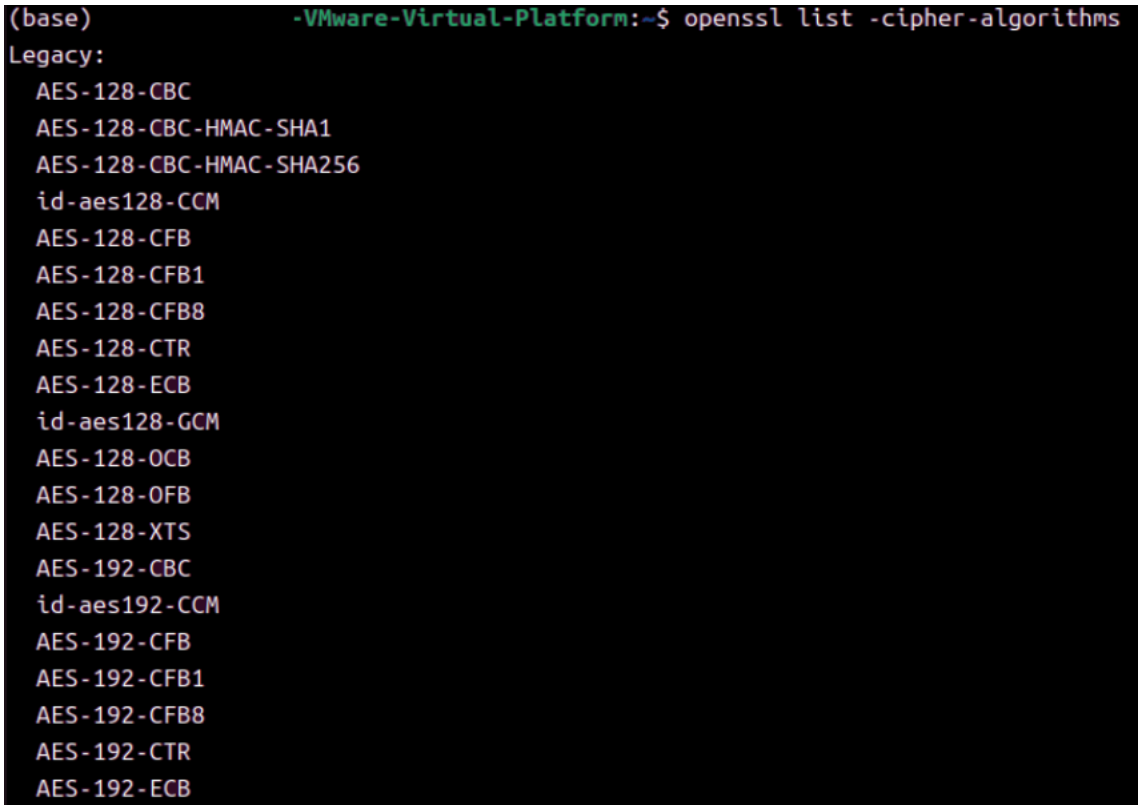


Figure 3-54 그림 제목

1.19.3 판정근거

Table 3-72 TE02.16.05 시험결과 판정근거

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

1.19.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.20 TE02.19.01

1.20.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.19.01	보안정책서에 검증대상 동작모드 서술	개발문서 검토

1.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-73 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

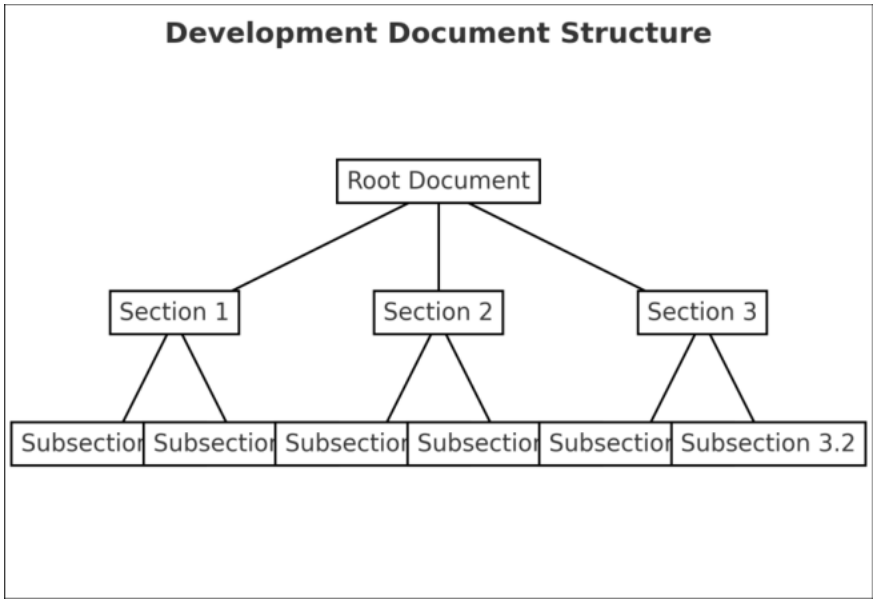


Figure 3-55 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-74 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

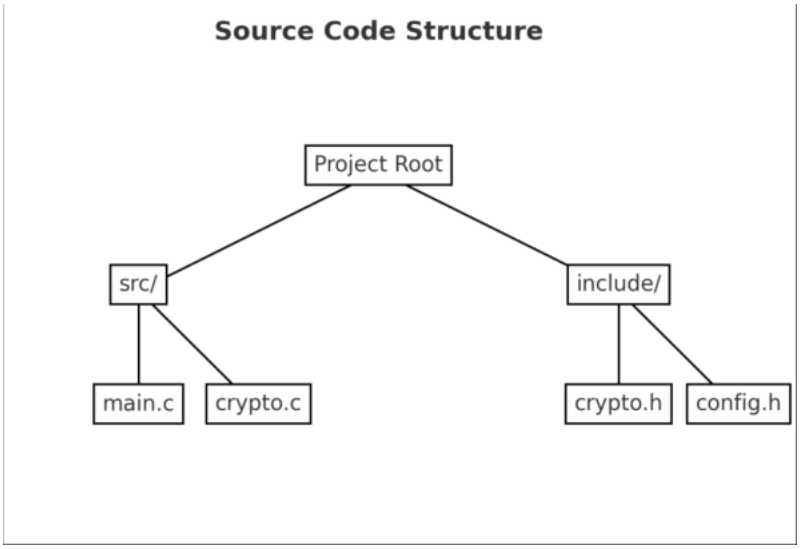


Figure 3-56 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-75 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

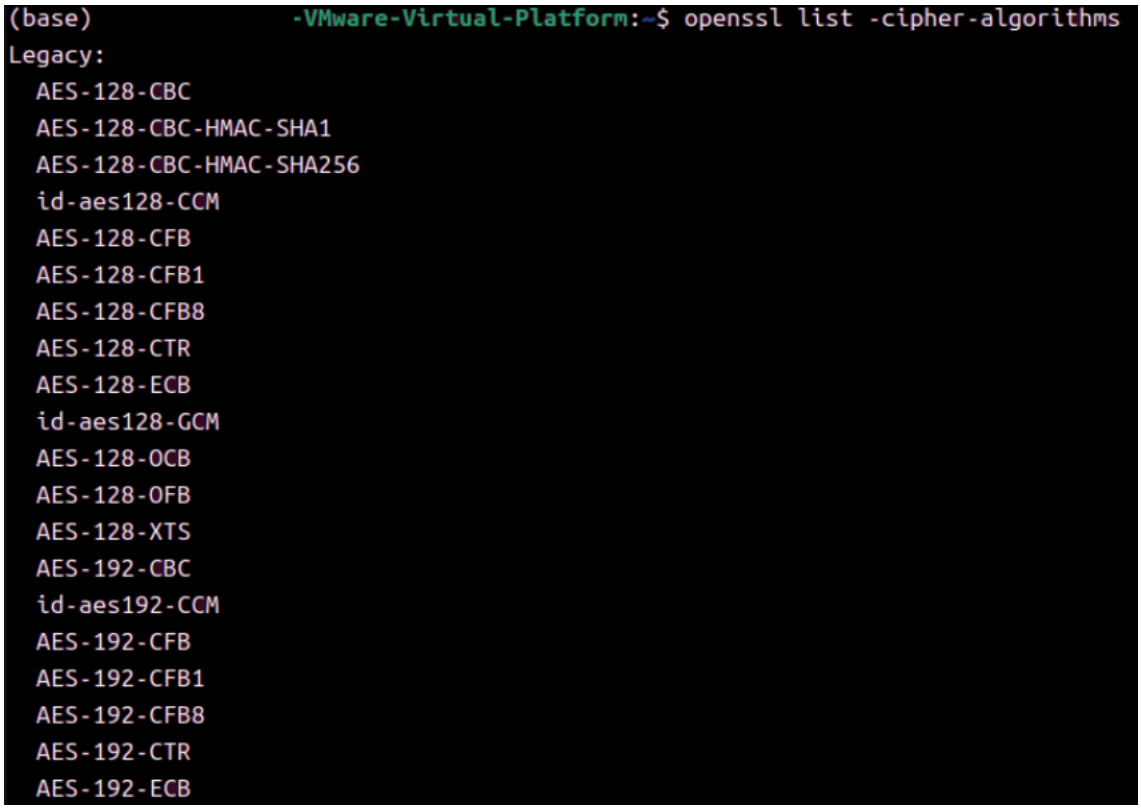


Figure 3-57 그림 제목

1.20.3 판정근거

Table 3-76 TE02.19.01 시험결과 판정근거

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

1.20.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.21 TE02.19.02

1.21.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.19.02	검증대상 동작모드 동작	동작시험

1.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-77 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

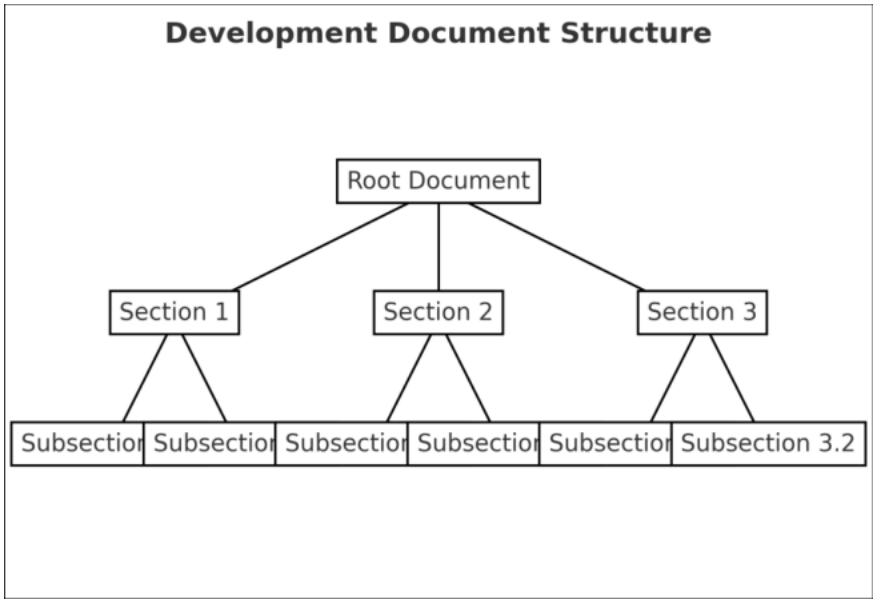


Figure 3-58 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-78 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

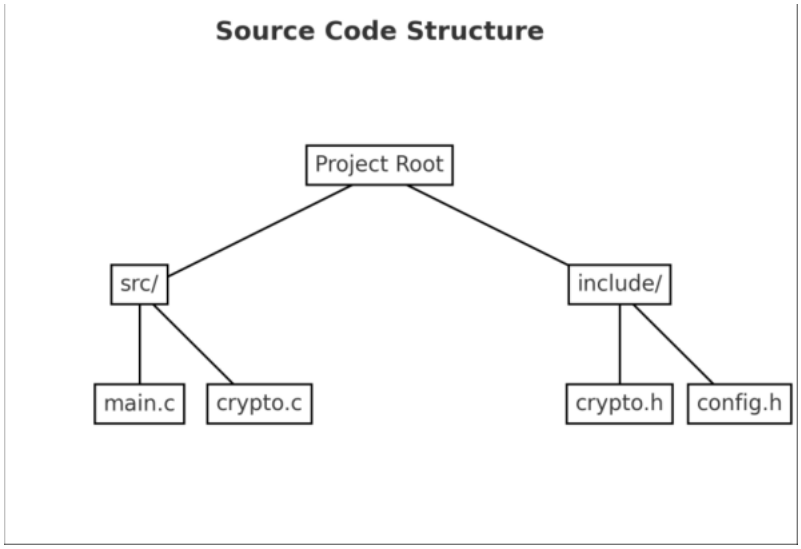


Figure 3-59 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-79 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

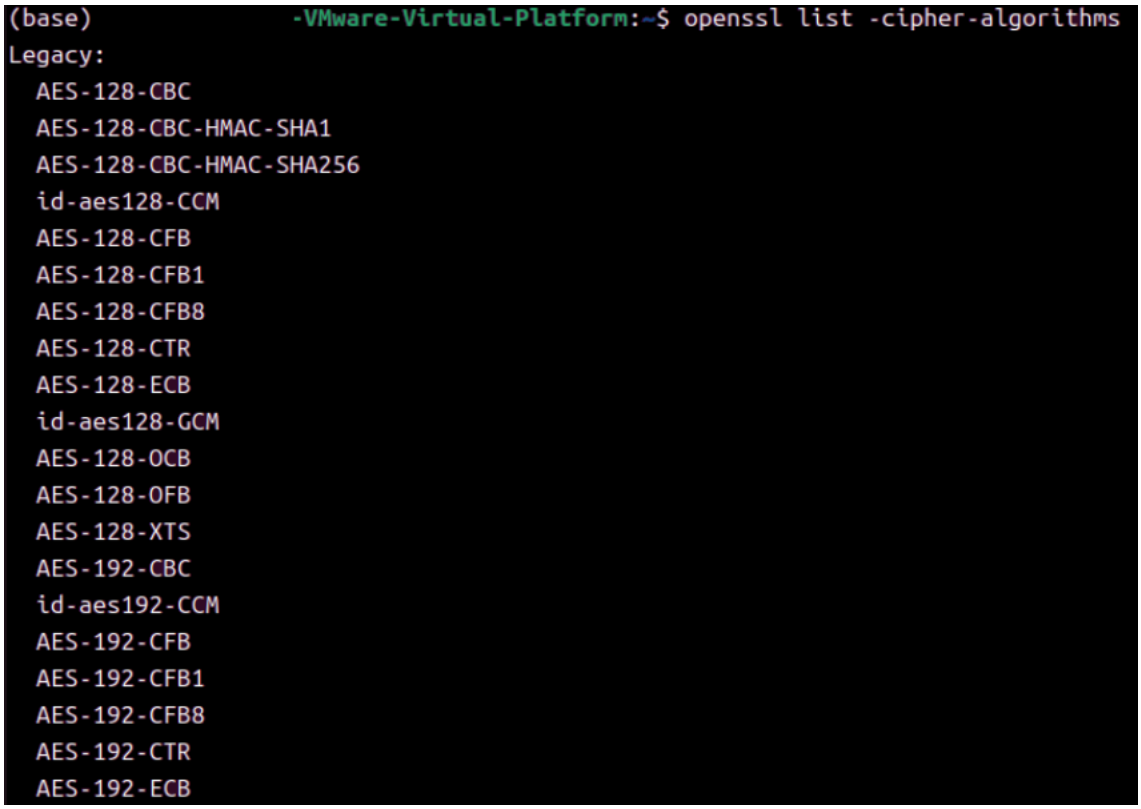


Figure 3-60 그림 제목

1.21.3 판정근거

Table 3-80 TE02.19.02 시험결과 판정근거

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

1.21.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.22 TE02.20.01

1.22.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.20.01	암호알고리즘 구현적합성	검증도구 수행

1.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-81 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

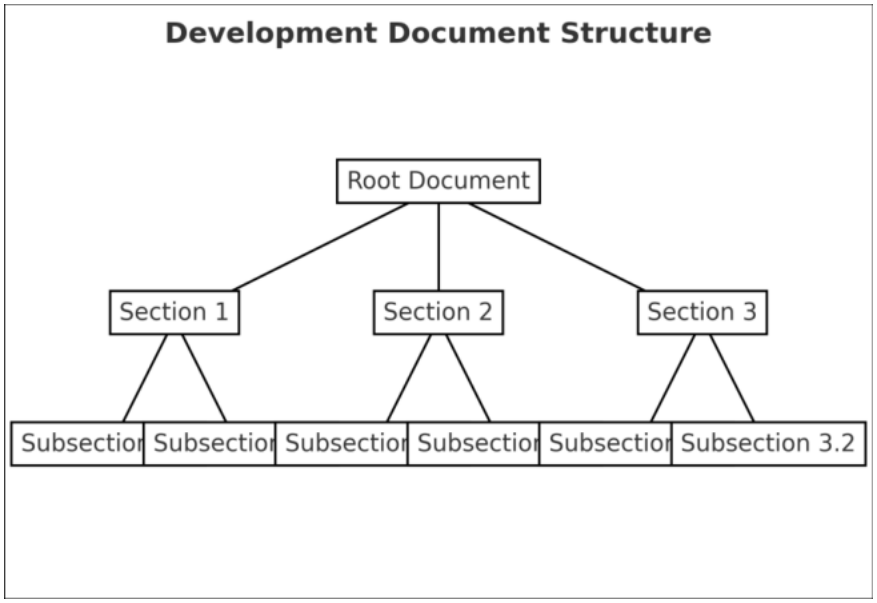


Figure 3-61 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-82 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

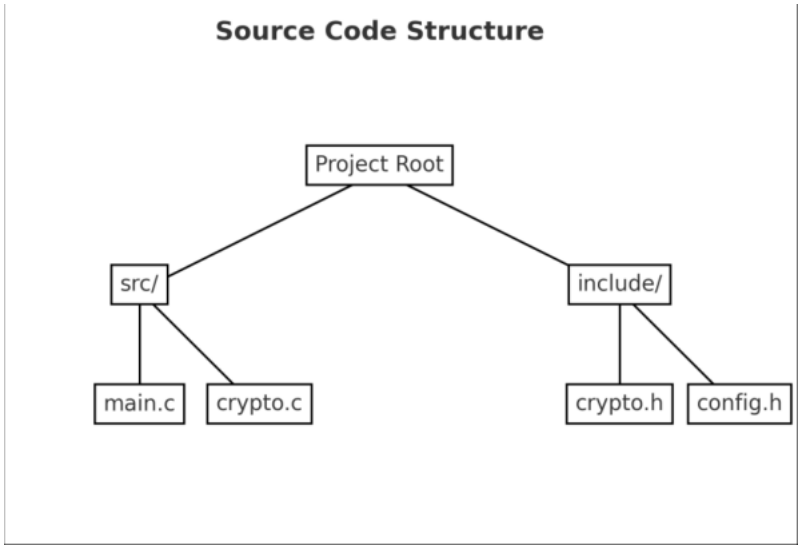


Figure 3-62 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-83 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

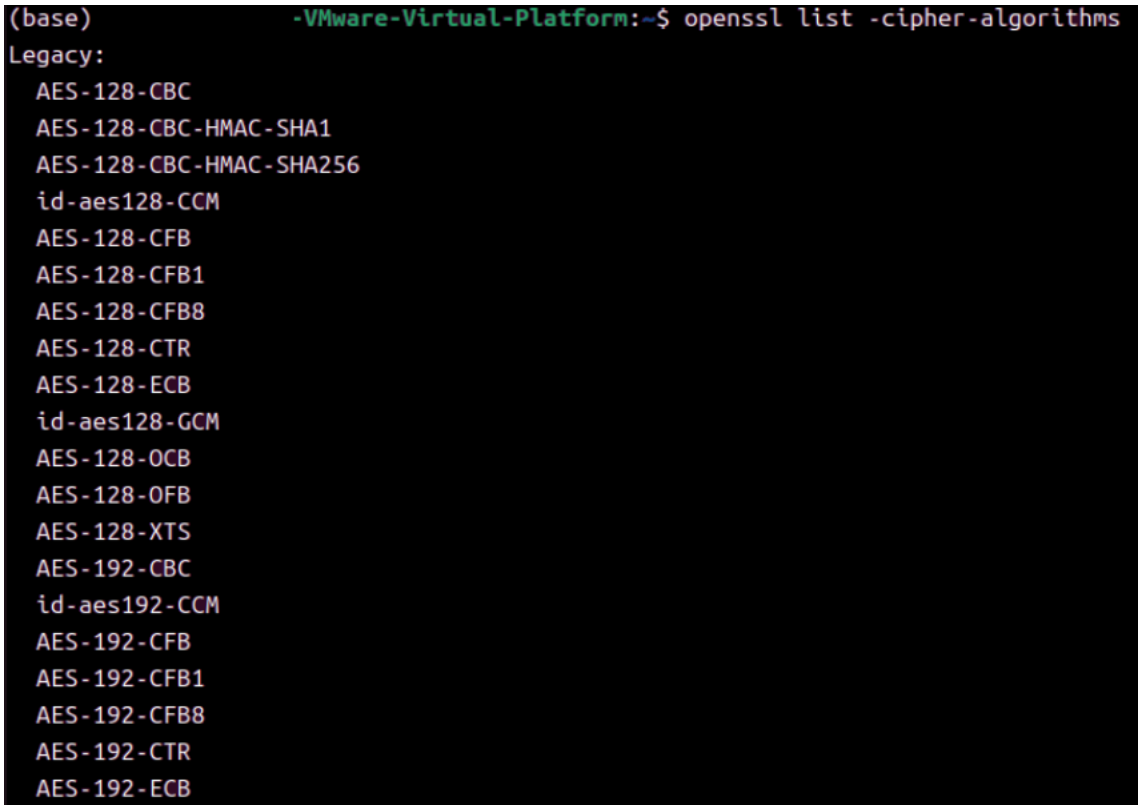


Figure 3-63 그림 제목

1.22.3 판정근거

Table 3-84 TE02.20.01 시험결과 판정근거

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

1.22.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.23 TE02.20.02

1.23.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.20.02	비검증대상 암호알고리즘 목록	개발문서 검토

1.23.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-85 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

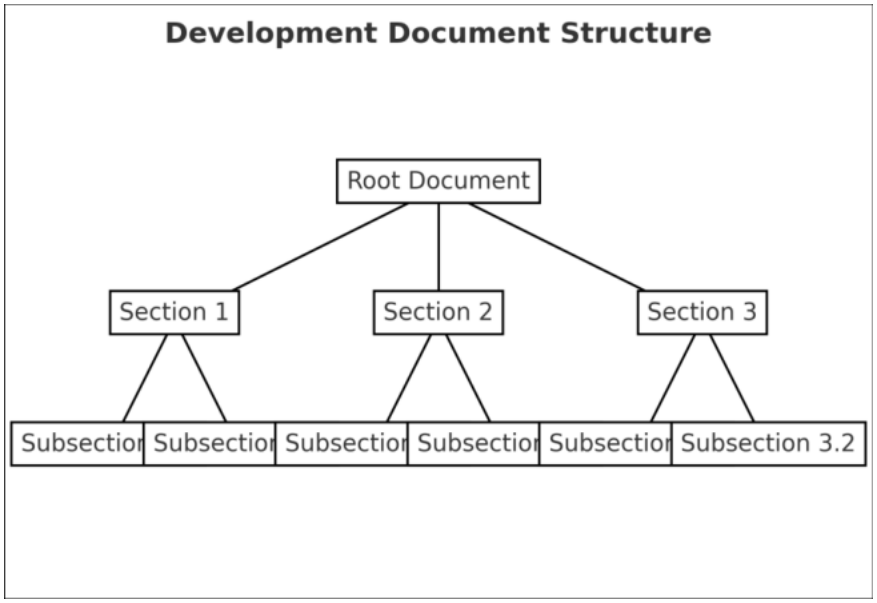


Figure 3-64 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-86 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

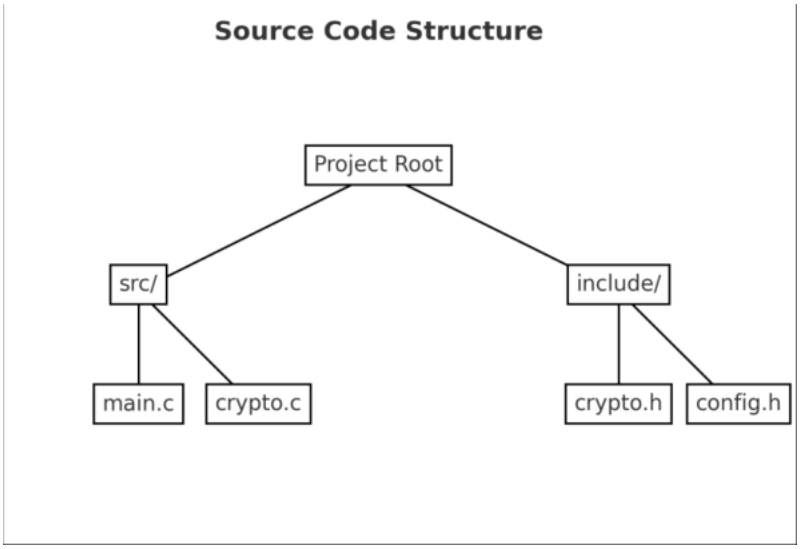


Figure 3-65 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-87 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

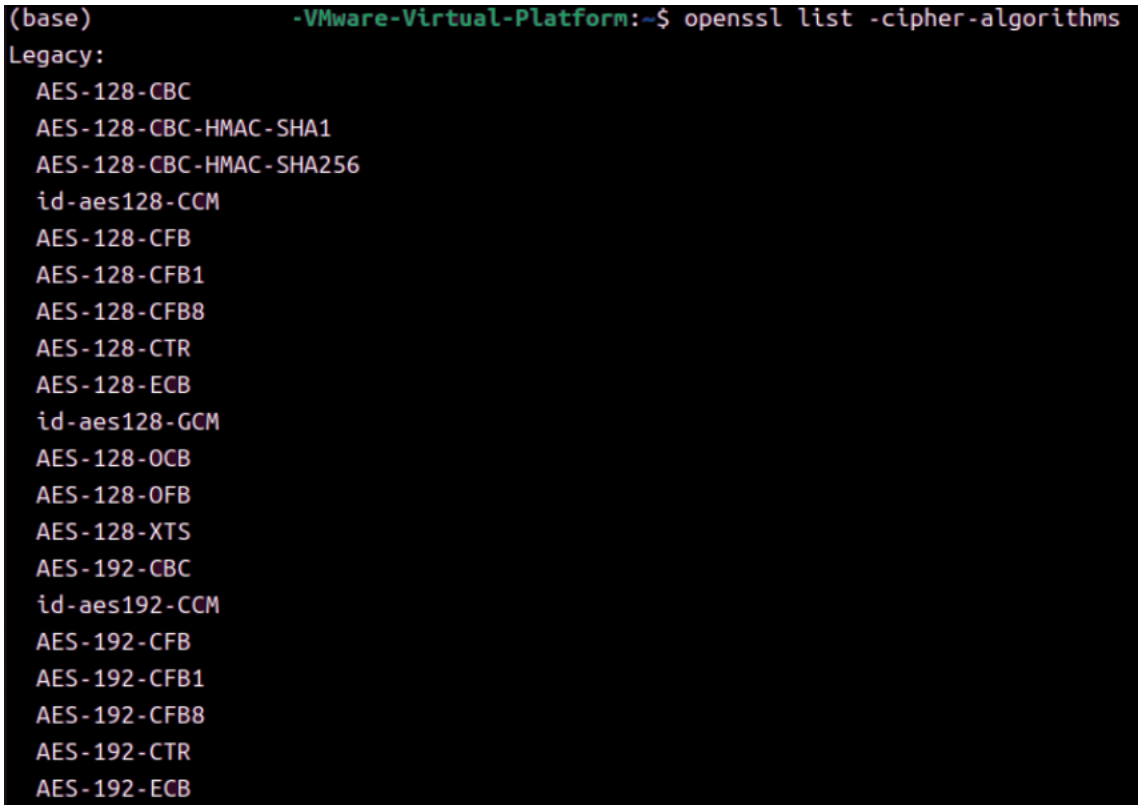


Figure 3-66 그림 제목

1.23.3 판정근거

Table 3-88 TE02.20.02 시험결과 판정근거

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

1.23.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.24 TE02.21.01

1.24.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.21.01	검증대상 동작모드에서 사용되는 비검증대상 요소	개발문서 검토

1.24.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-89 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

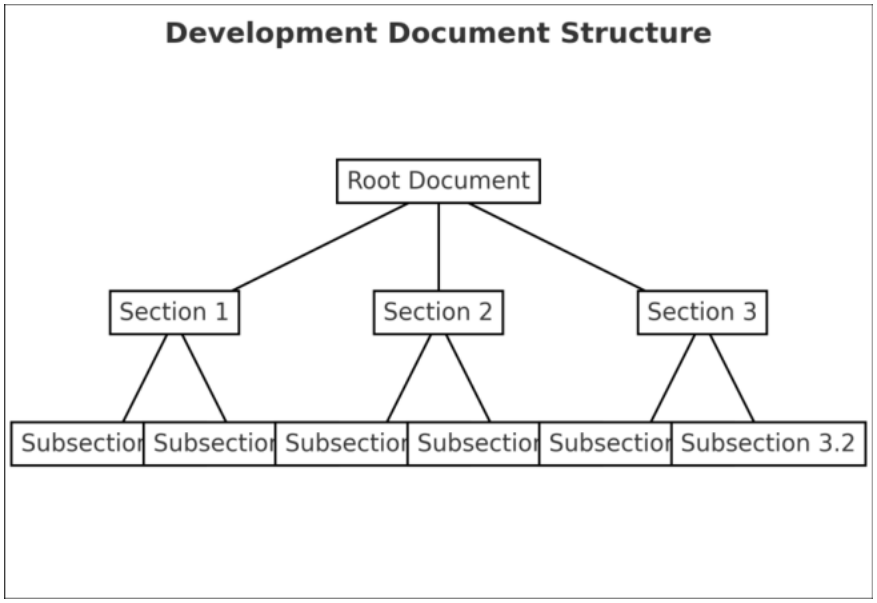


Figure 3-67 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-90 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

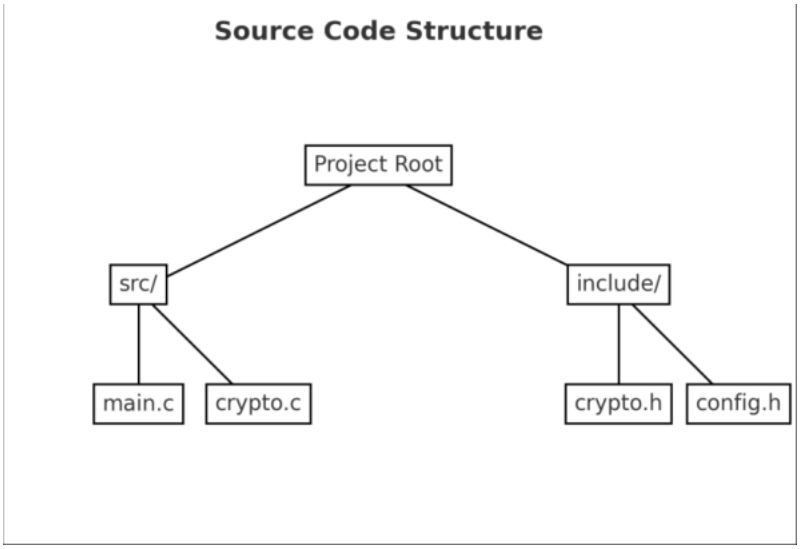


Figure 3-68 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-91 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

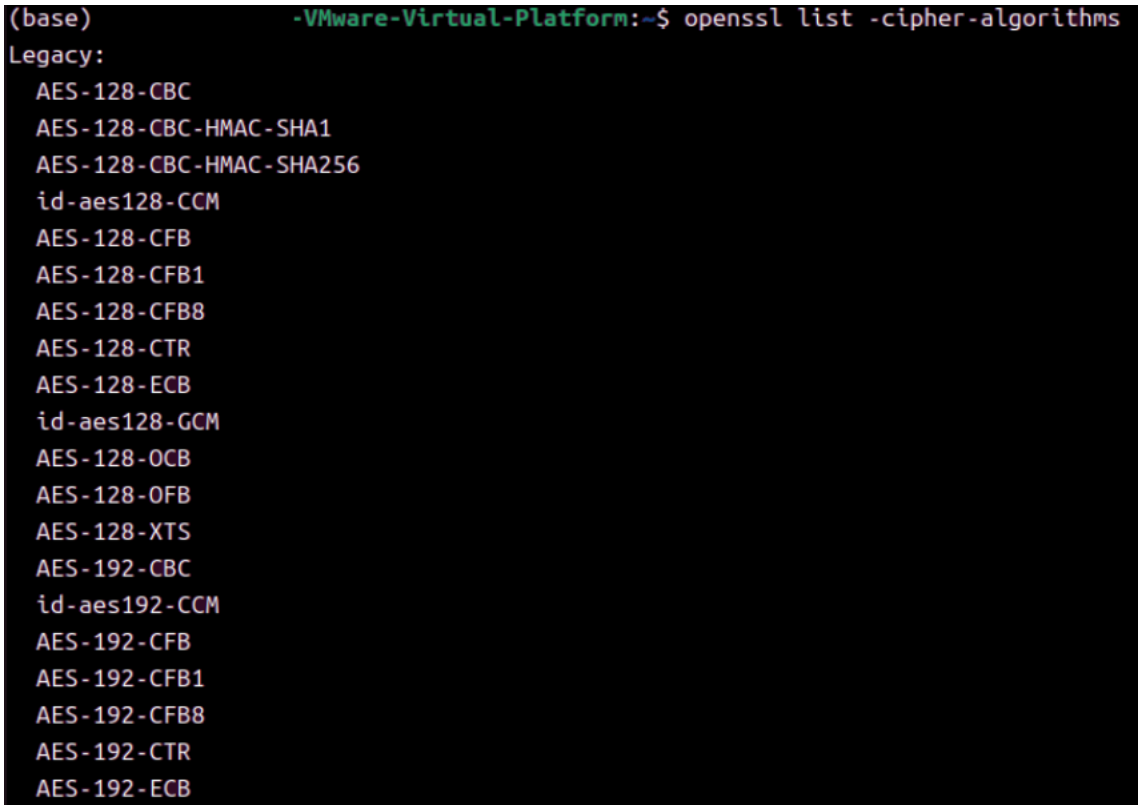


Figure 3-69 그림 제목

1.24.3 판정근거

Table 3-92 TE02.21.01 시험결과 판정근거

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

1.24.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.25 TE02.21.02

1.25.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.21.02	비검증대상 요소의 보안 관련성 없음에 대한 근거	개발문서 검토

1.25.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-93 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

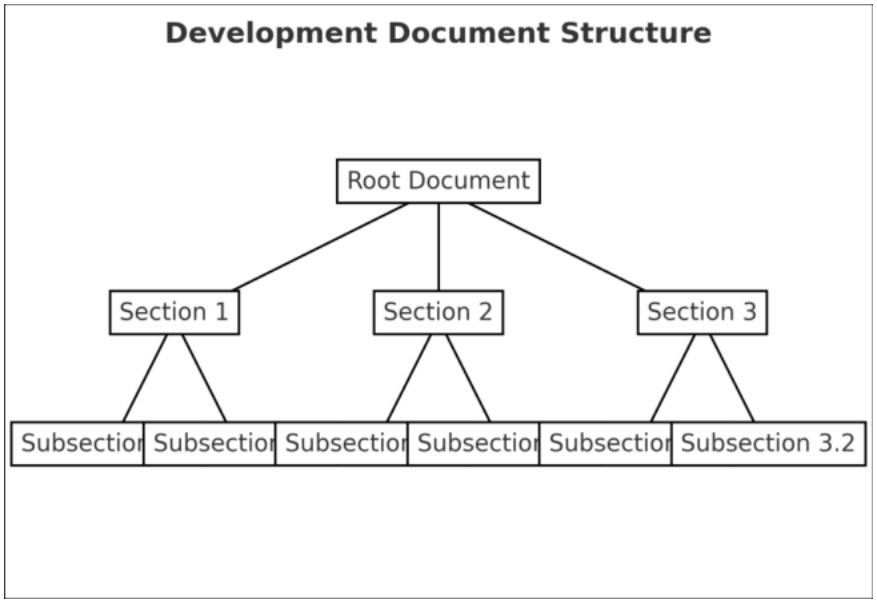


Figure 3-70 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-94 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

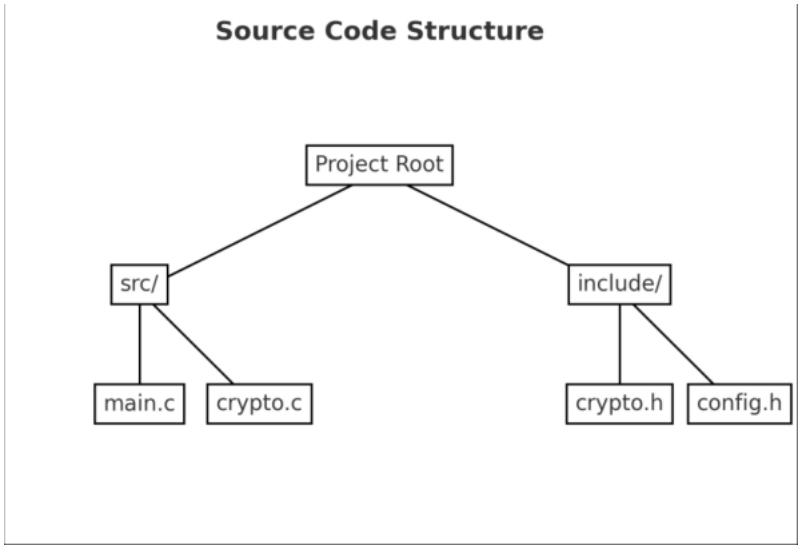


Figure 3-71 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-95 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

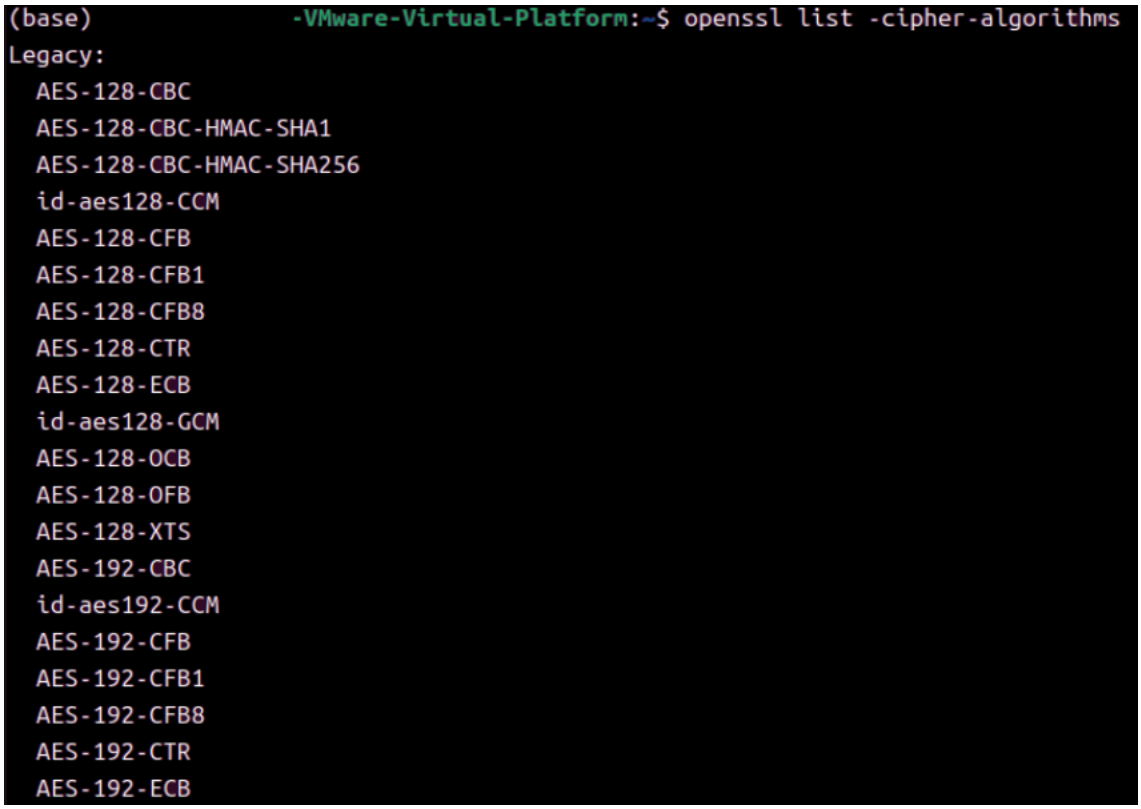


Figure 3-72 그림 제목

1.25.3 판정근거

Table 3-96 TE02.21.02 시험결과 판정근거

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

1.25.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.26 TE02.22.01

1.26.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.22.01	핵심보안매개변수 목록	개발문서 검토

1.26.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-97 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

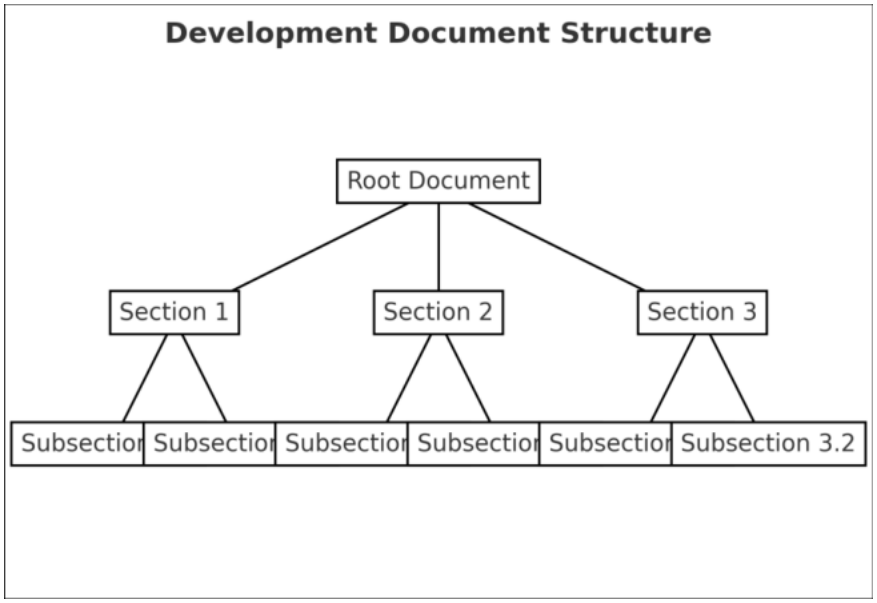


Figure 3-73 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-98 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

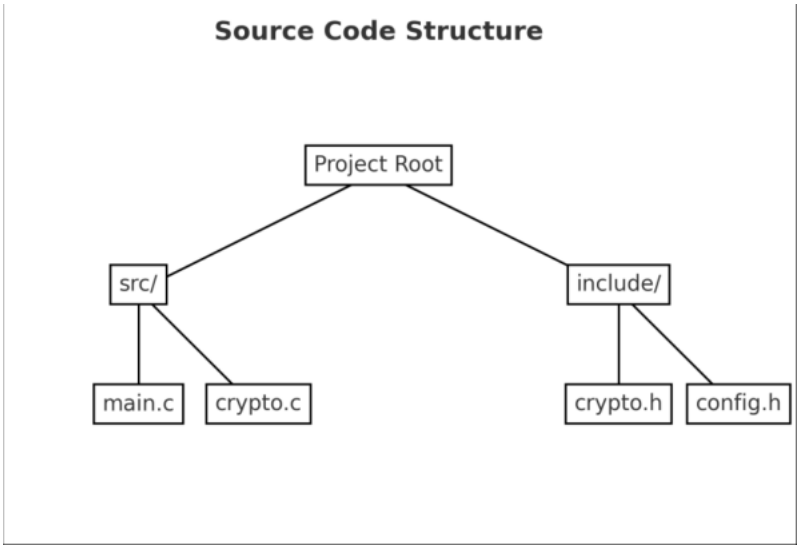


Figure 3-74 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-99 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

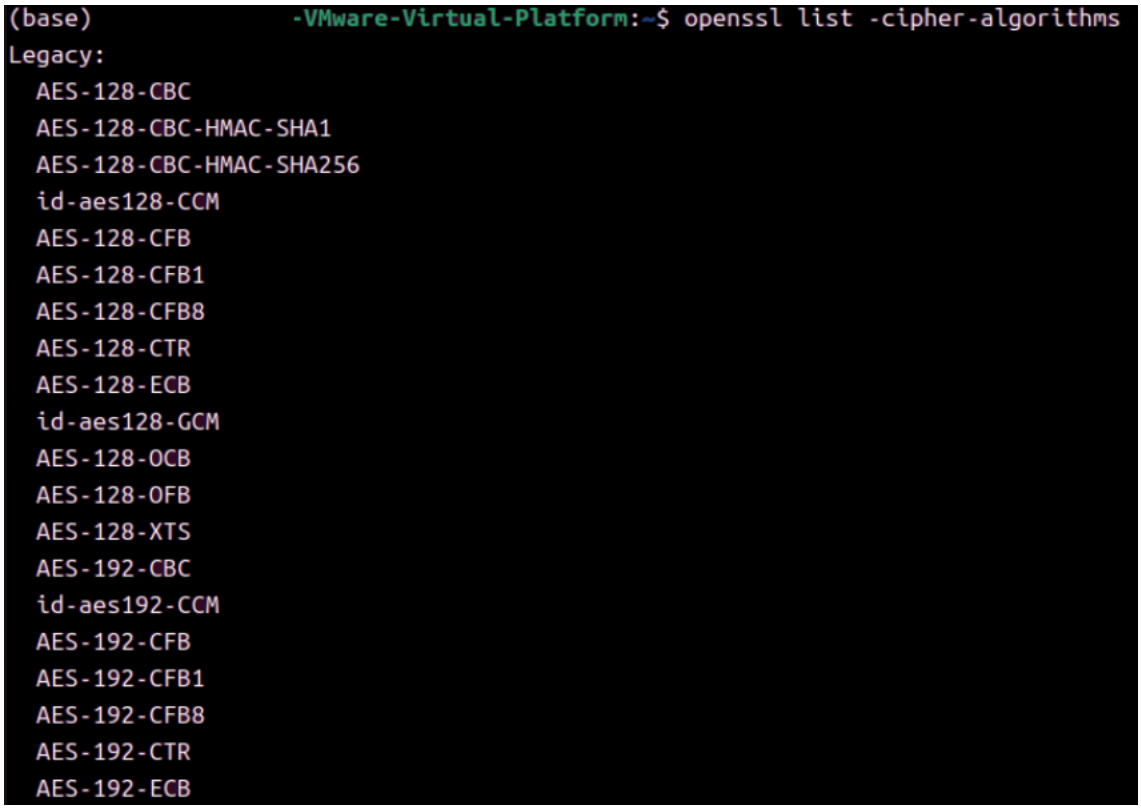


Figure 3-75 그림 제목

1.26.3 판정근거

Table 3-100 TE02.22.01 시험결과 판정근거

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

1.26.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.27 TE02.22.02

1.27.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.22.02	동작모드 간 핵심보안매개변수 분리	암호모듈 검사

1.27.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-101 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

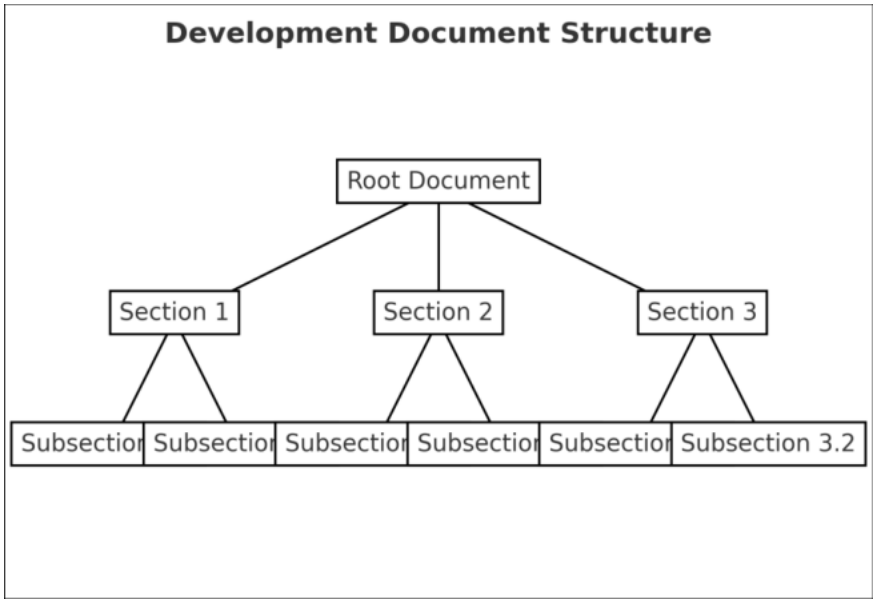


Figure 3-76 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-102 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

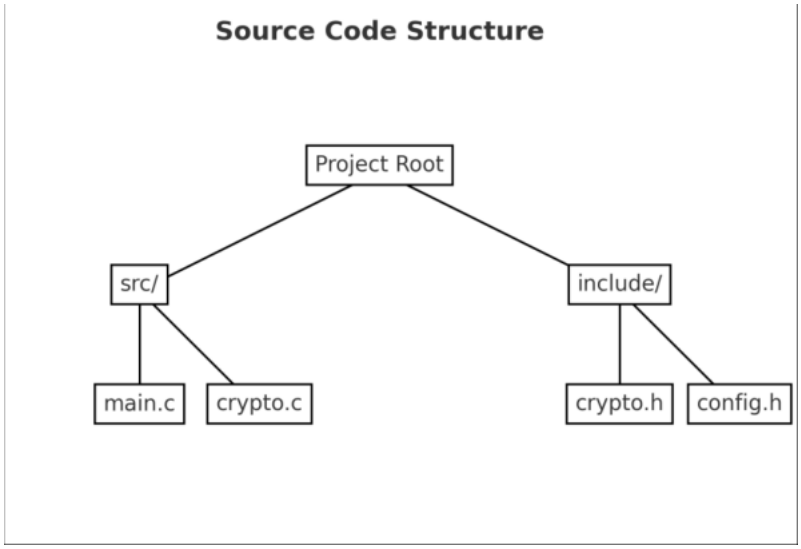


Figure 3-77 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-103 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

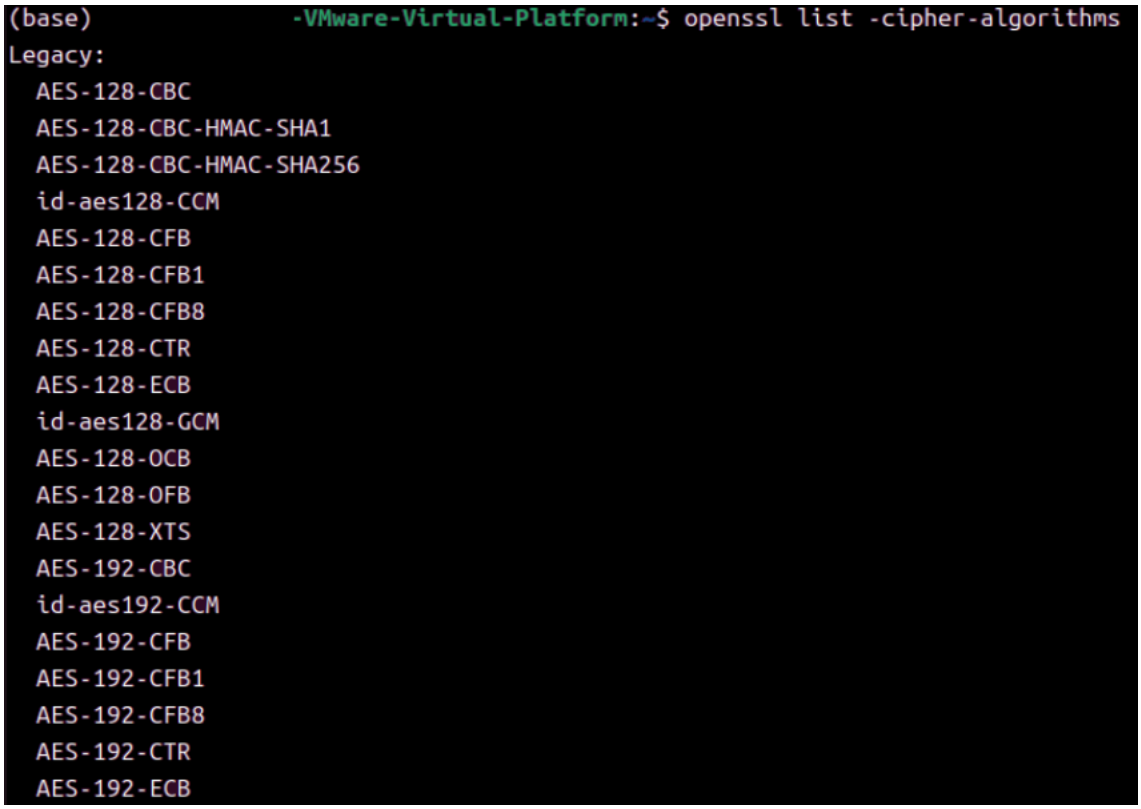


Figure 3-78 그림 제목

1.27.3 판정근거

Table 3-104 TE02.22.02 시험결과 판정근거

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

1.27.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.28 TE02.24.01

1.28.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.24.01	검증대상 동작모드 서비스 사용 시 표시기 제공 목록	개발문서 검토

1.28.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-105 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

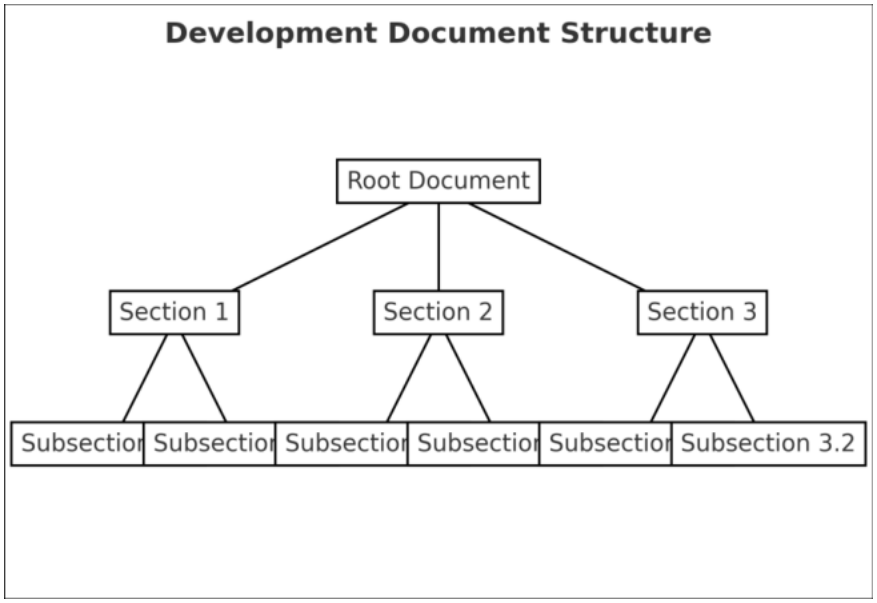


Figure 3-79 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-106 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

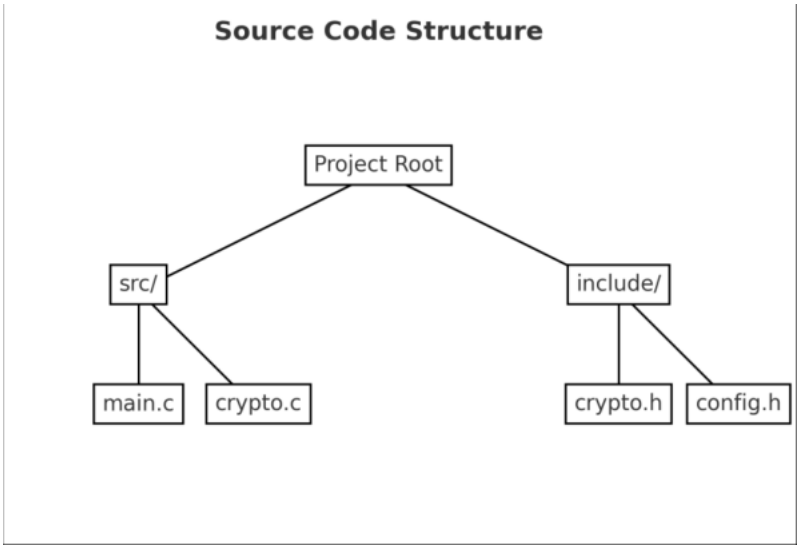


Figure 3-80 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-107 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

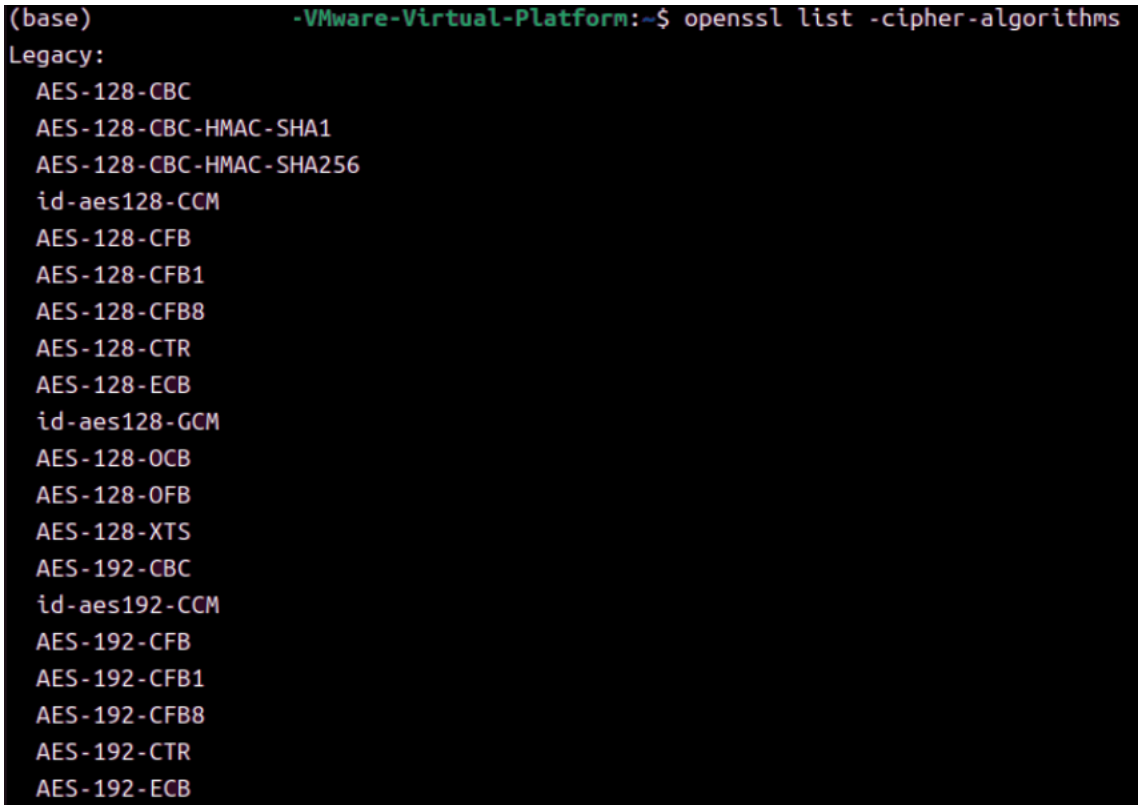


Figure 3-81 그림 제목

1.28.3 판정근거

Table 3-108 TE02.24.01 시험결과 판정근거

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

1.28.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

1.29 TE02.24.02

1.29.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.24.02	서비스 별 표시기 정상동작 확인	암호모듈 검사

1.29.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-109 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

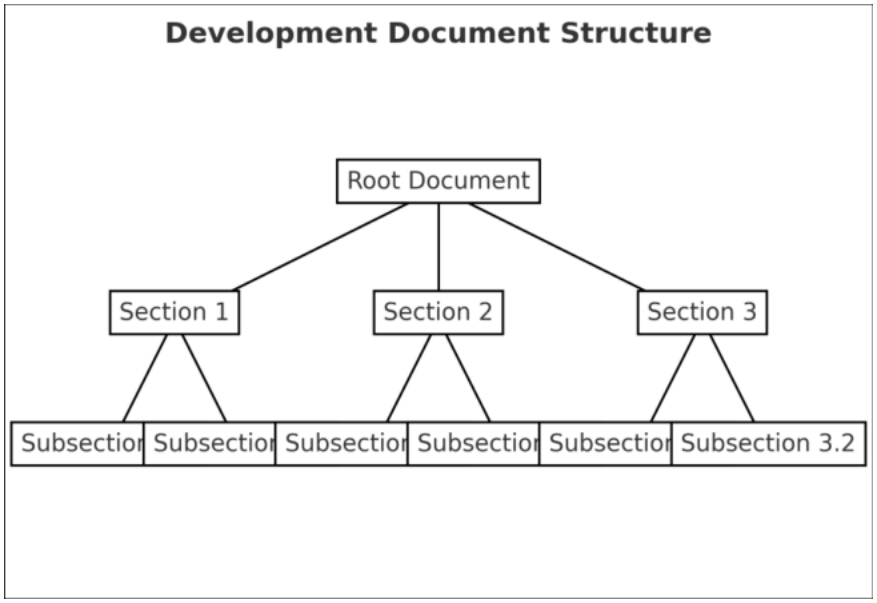


Figure 3-82 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-110 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

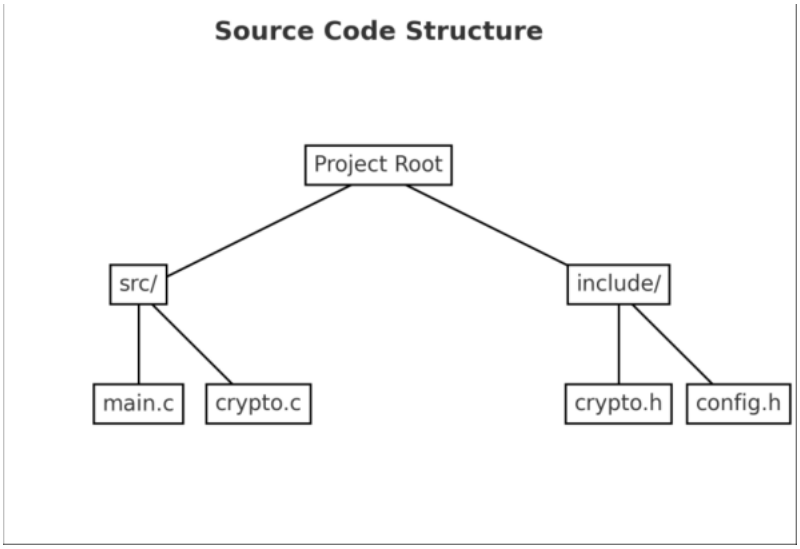


Figure 3-83 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-111 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

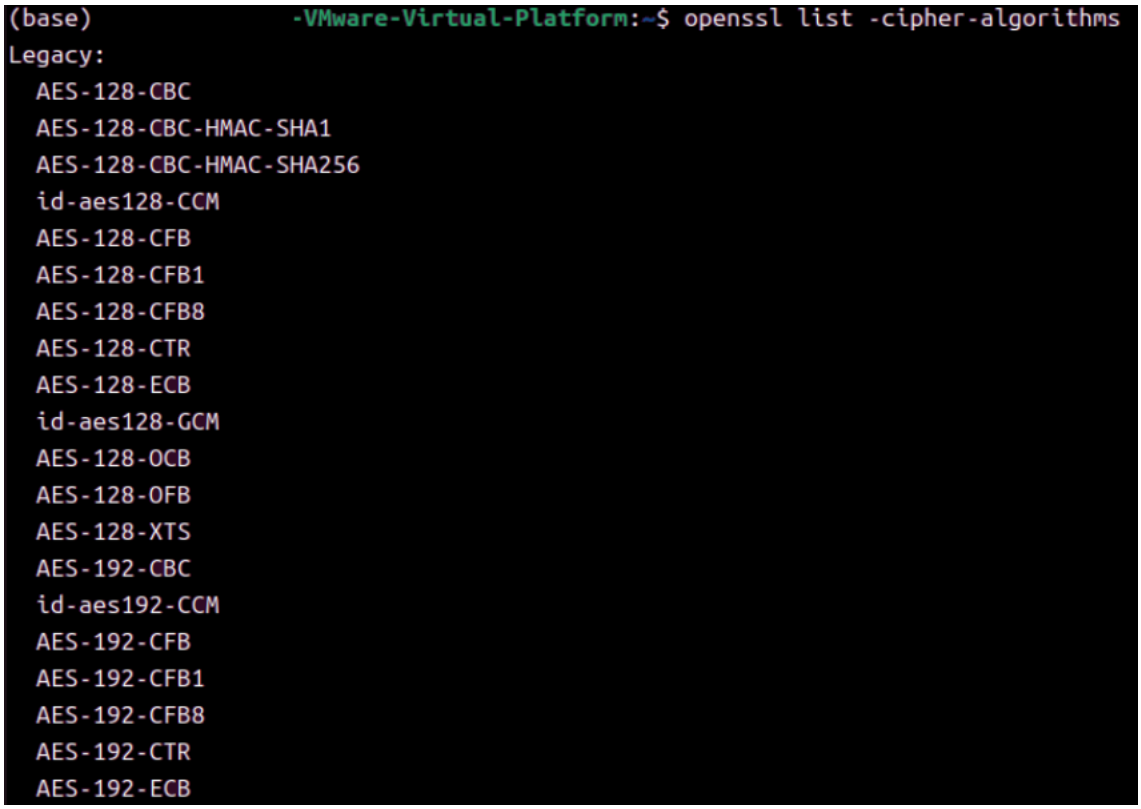


Figure 3-84 그림 제목

1.29.3 판정근거

Table 3-112 TE02.24.02 시험결과 판정근거

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

1.29.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2. 암호모듈 인터페이스 (AS03)

□ 암호모듈의 모든 논리적 정보흐름은 암호경계의 입 / 출구로 식별되는 물리적 접근 지점과 논리적 인터페이스에 제한되어야 한다 .

2.1 AS03 시험항목

AS	TE	확인사항
AS03.01	1, 2, 3, 4	암호경계의 물리적 접근 지점과 인터페이스를 통한 정보의 흐름
AS03.04	1	5 개의 논리적 인터페이스 구분
AS03.05	1	데이터 입력 인터페이스 정보
AS03.06	1	데이터 출력 인터페이스 정보
AS03.07	1, 2, 3, 4, 5	데이터 출력 금지 요건
AS03.08	1	제어 입력 인터페이스 정보
AS03.09	1, 2	제어 출력 인터페이스 정보
AS03.10	1, 2, 3, 4, 5	제어 출력 금지 요건
AS03.11	1, 2	상태 출력 인터페이스 정보
AS03.15	1, 2, 3, 4, 5, 6	입력 데이터 및 제어 정보 형식

2.2 TE03.01.01

2.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.01.01	암호모듈의 논리적 인터페이스 정보	개발문서 검토

2.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-113 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

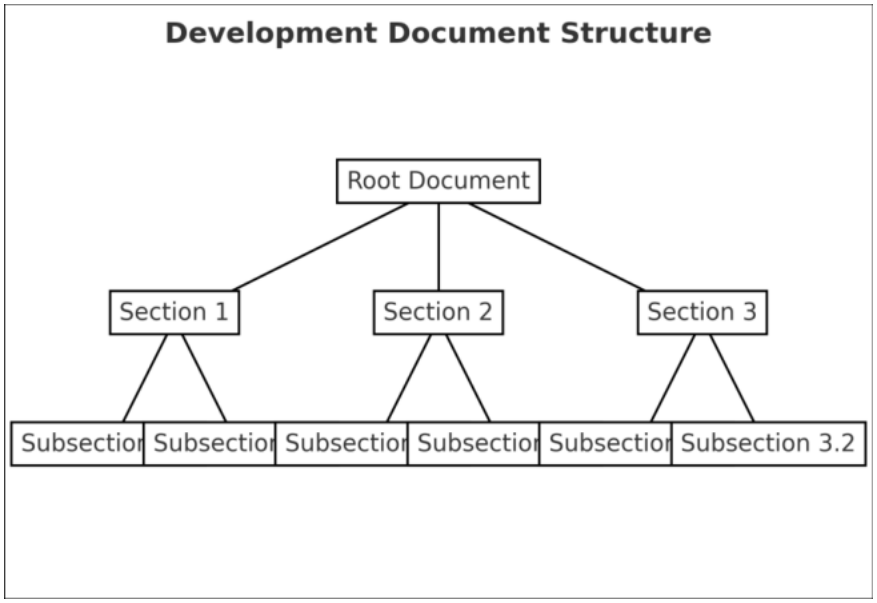


Figure 3-85 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-114 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

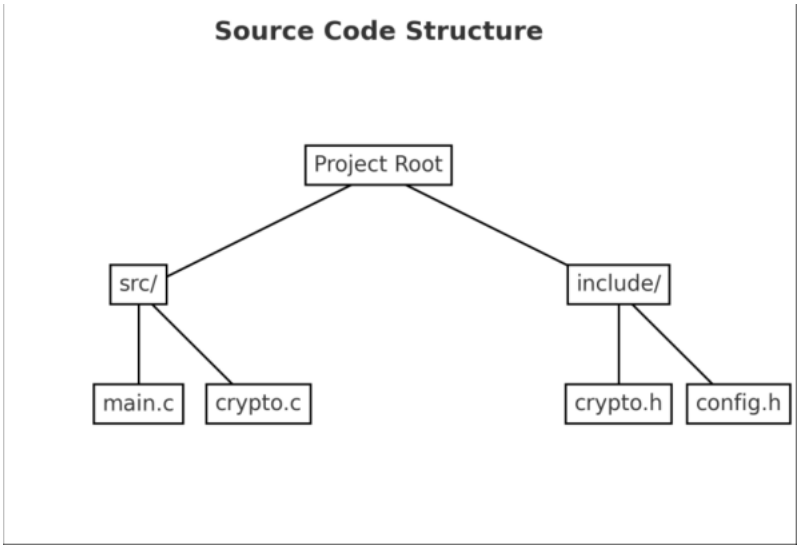


Figure 3-86 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-115 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

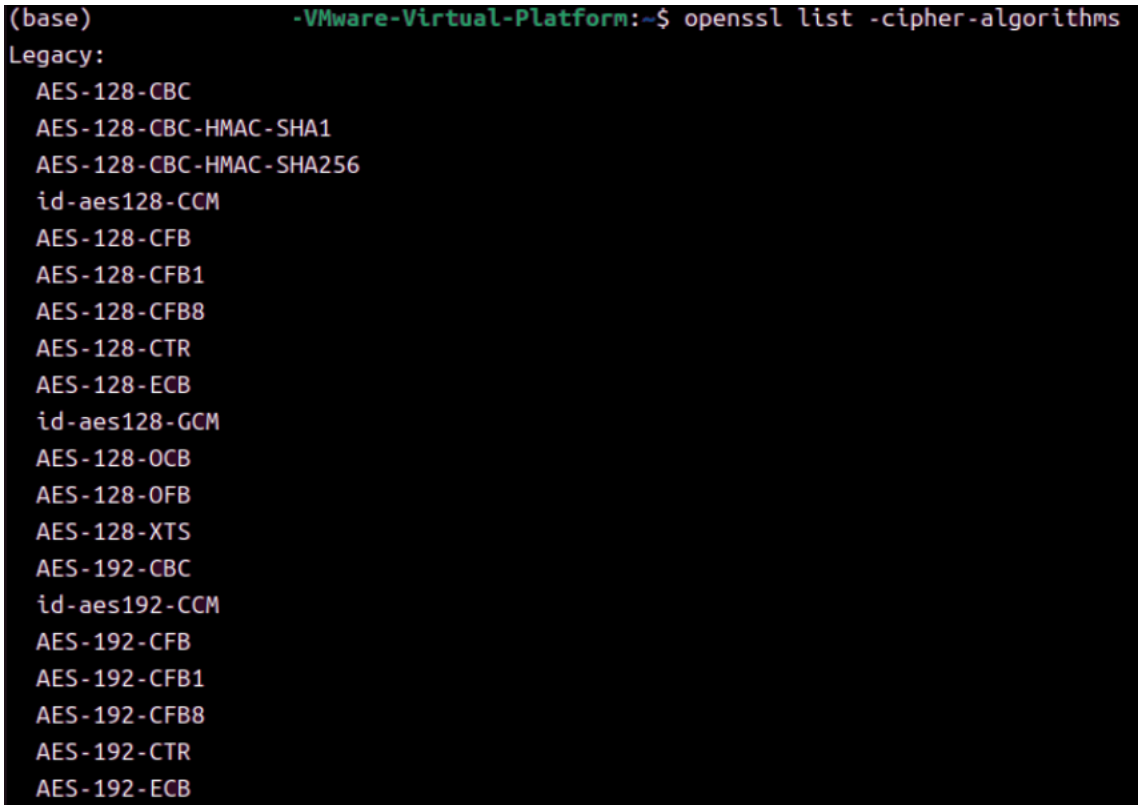


Figure 3-87 그림 제목

2.2.3 판정근거

Table 3-116 TE03.01.01 시험결과 판정근거

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

2.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.3 TE03.01.02

2.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.01.02	암호모듈의 모든 정보 흐름 및 물리적 접근 지점 명세	개발문서 검토

2.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-117 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

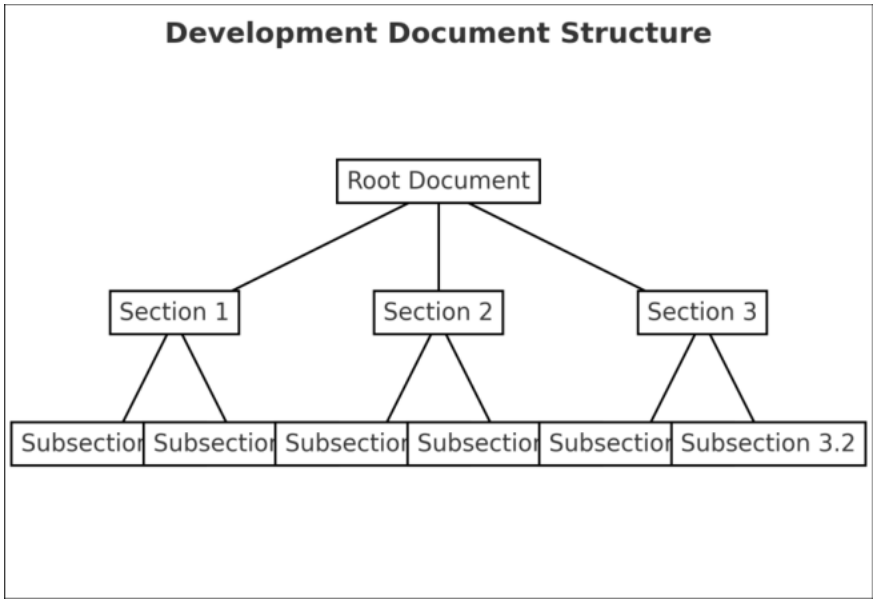


Figure 3-88 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-118 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

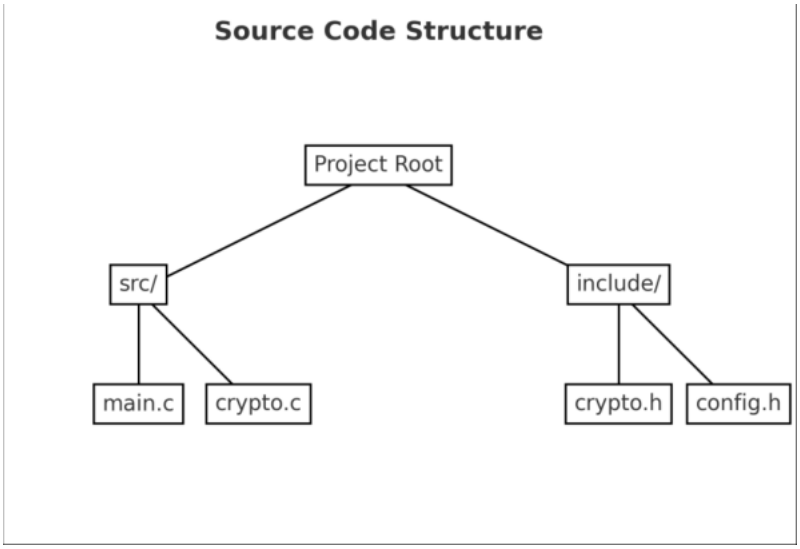


Figure 3-89 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-119 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

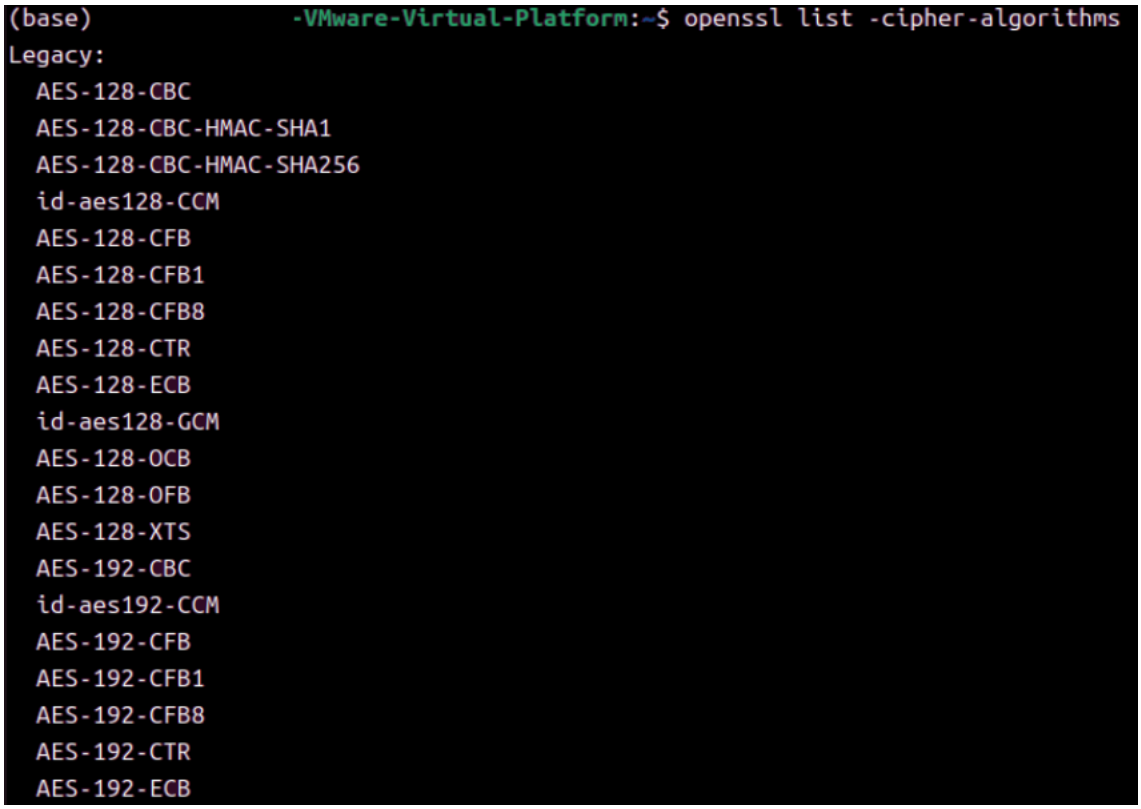


Figure 3-90 그림 제목

2.3.3 판정근거

Table 3-120 TE03.01.02 시험결과 판정근거

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

2.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.4 TE03.01.03

2.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.01.03	논리적 인터페이스 및 물리적 포트 명세	개발문서 검토

2.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-121 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

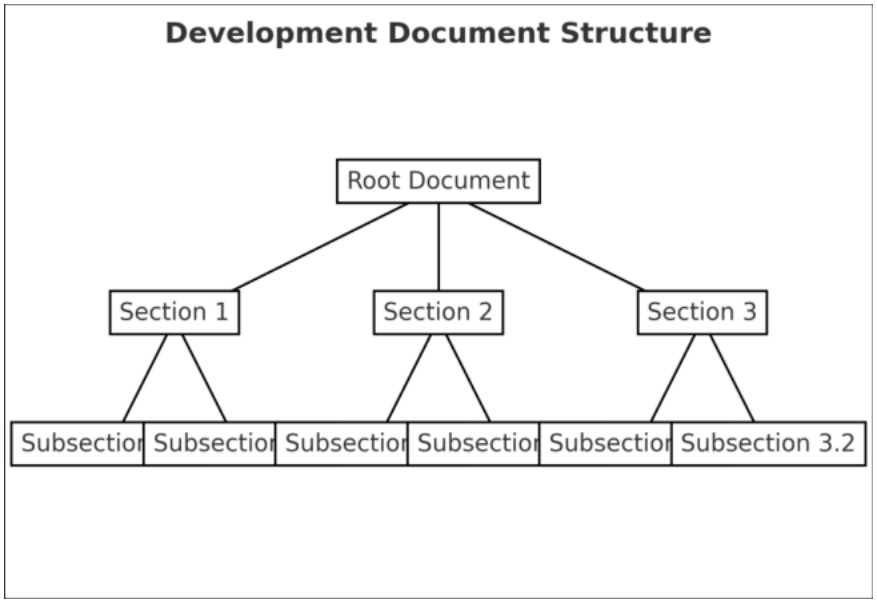


Figure 3-91 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-122 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

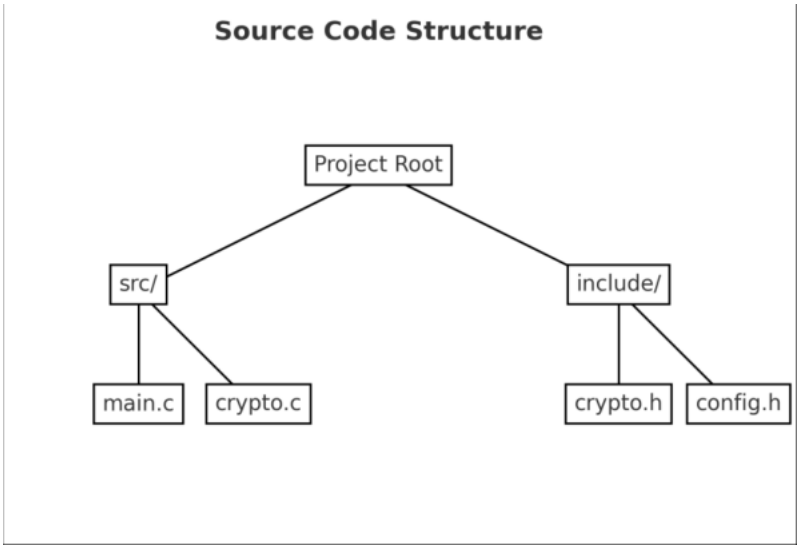


Figure 3-92 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-123 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

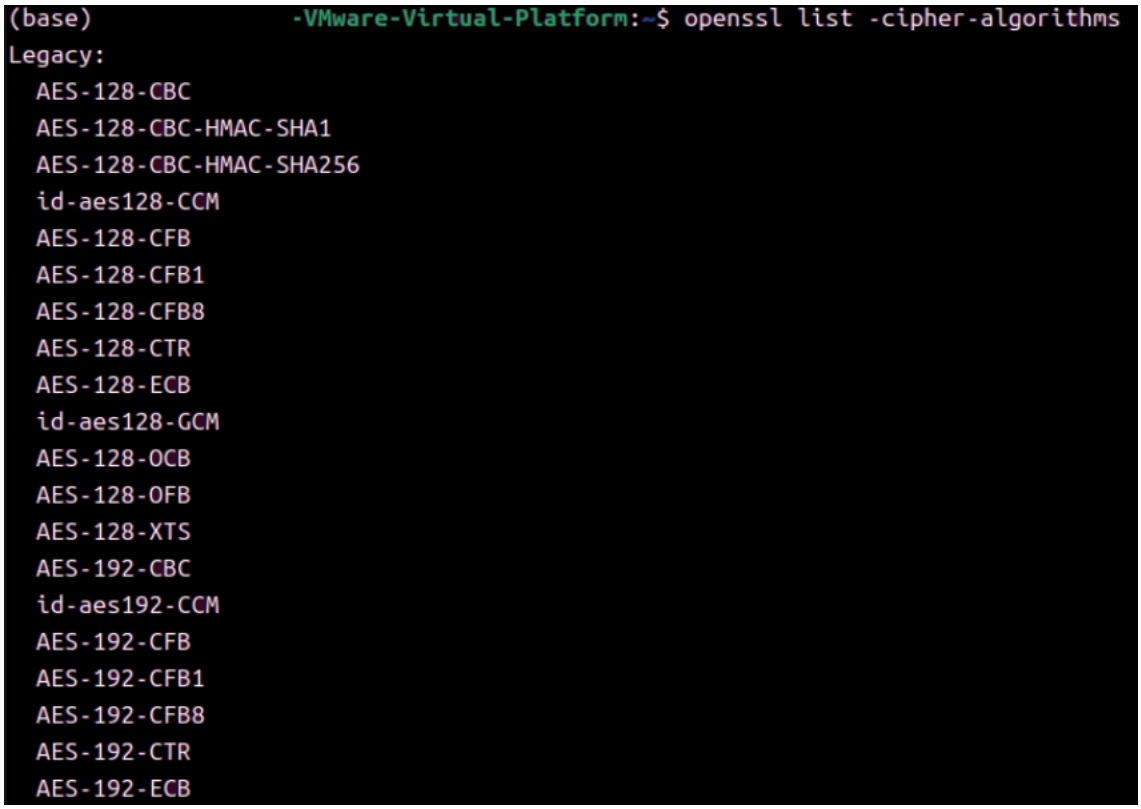


Figure 3-93 그림 제목

2.4.3 판정근거

Table 3-124 TE03.01.03 시험결과 판정근거

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

2.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.5 TE03.01.04

2.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.01.04	실제 설계된 암호모듈 인터페이스 정보와 개발문서 정보 사이의 일치 여부	소스코드 검토

2.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-125 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

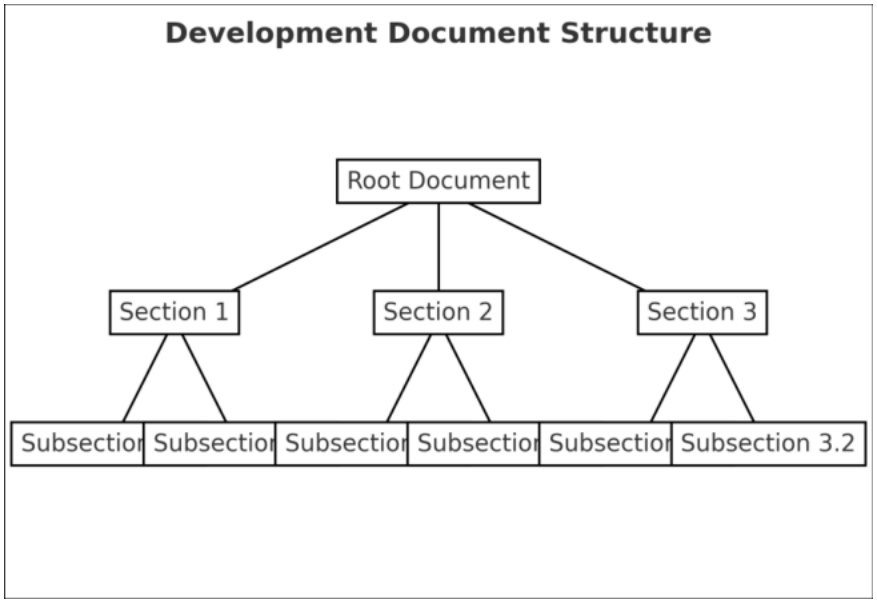


Figure 3-94 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-126 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

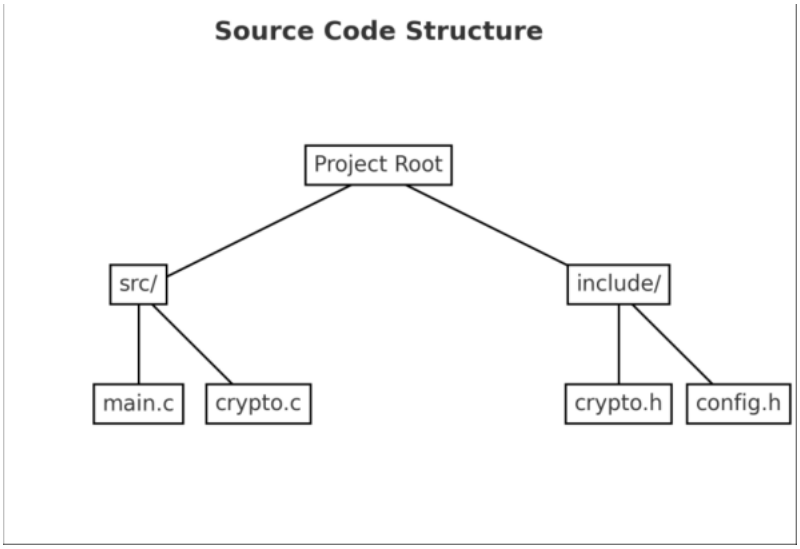


Figure 3-95 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-127 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

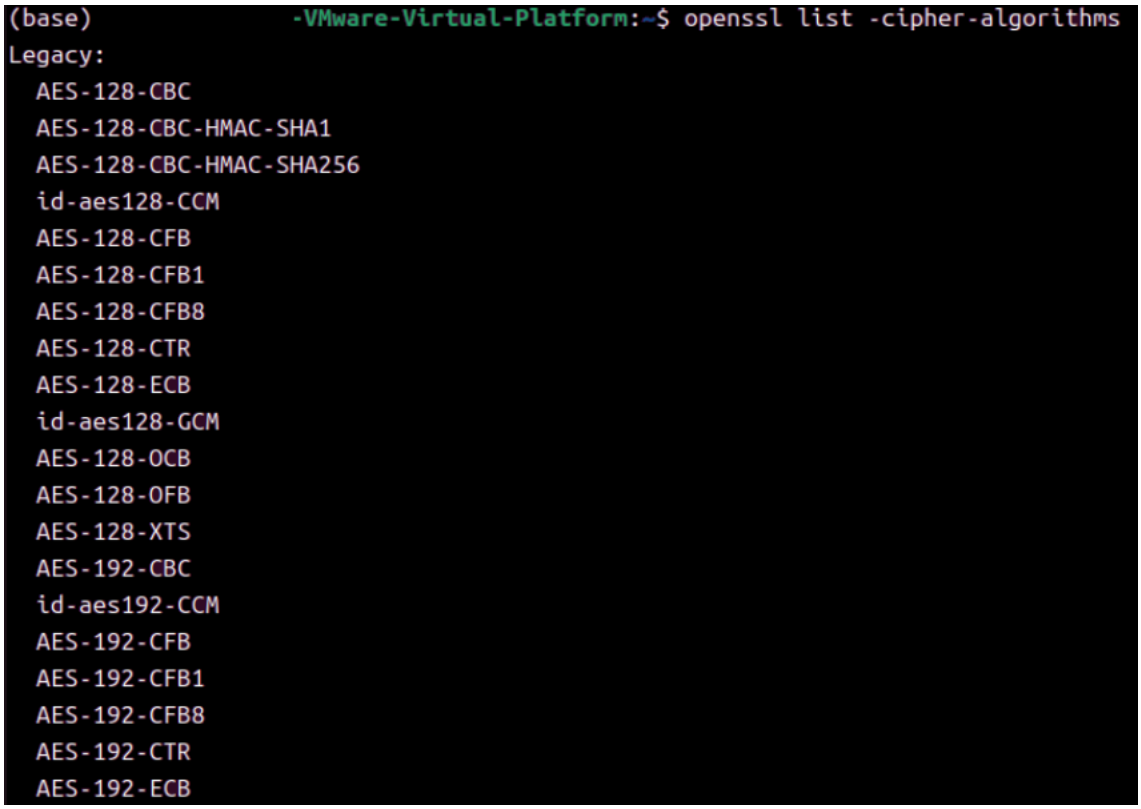


Figure 3-96 그림 제목

2.5.3 판정근거

Table 3-128 TE03.01.04 시험결과 판정근거

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

2.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.6 TE03.04.01

2.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.04.01	5 개의 논리적 인터페이스 (데이터 입력 , 데이터 출력 , 제어 입력 , 제어 출력 , 상태 출력) 서술 여부	개발문서 검토

2.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-129 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

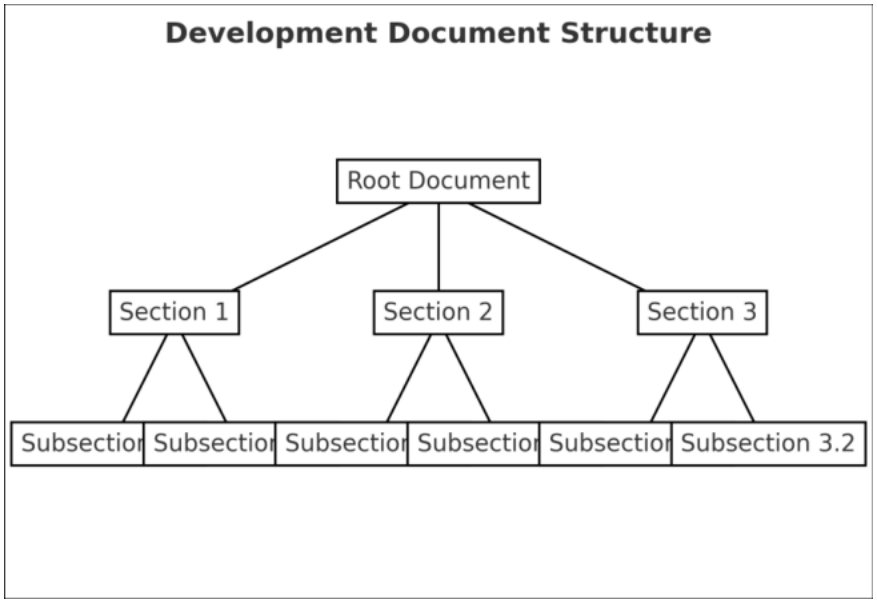


Figure 3-97 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-130 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

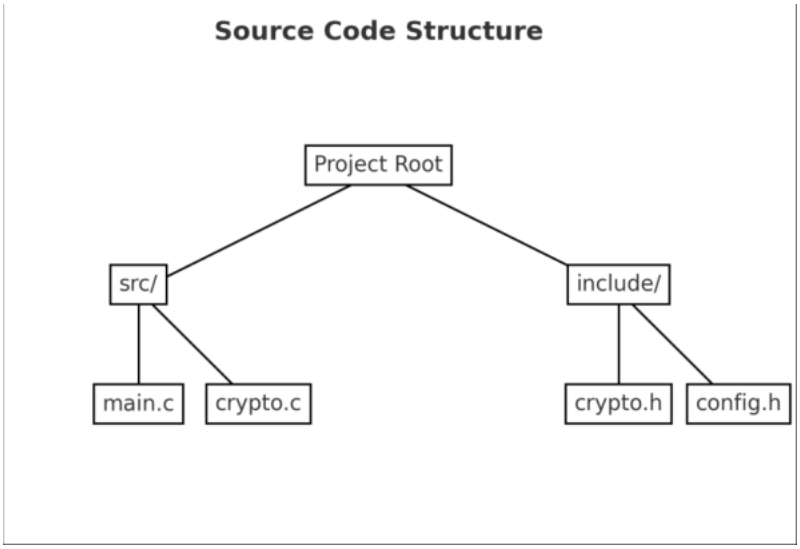


Figure 3-98 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

■

Table 3-131 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

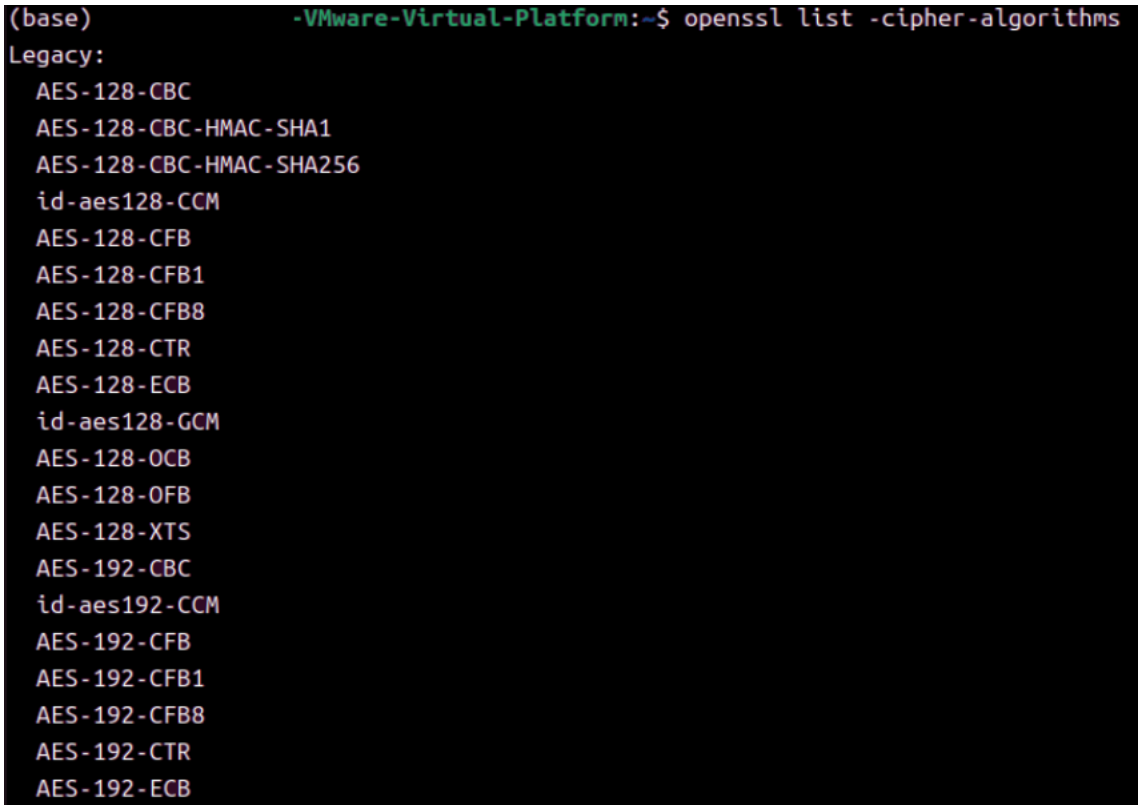


Figure 3-99 그림 제목

2.6.3 판정근거

Table 3-132 TE03.04.01 시험결과 판정근거

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

2.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.7 TE03.05.01

2.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.05.01	입력되는 모든 데이터가 데이터 입력 인터페이스를 통해 입력되는 지 확인)	암호모듈 검사

2.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-133 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

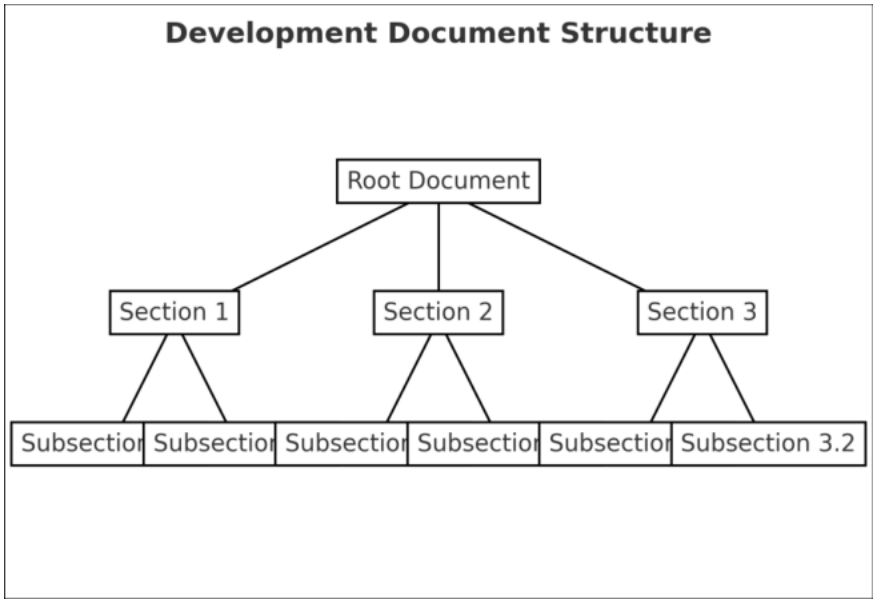


Figure 3-100 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-134 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

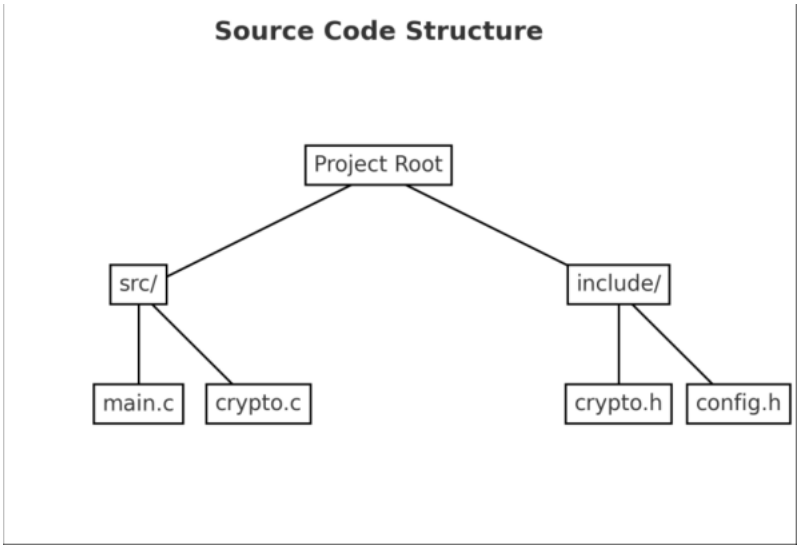


Figure 3-101 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-135 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

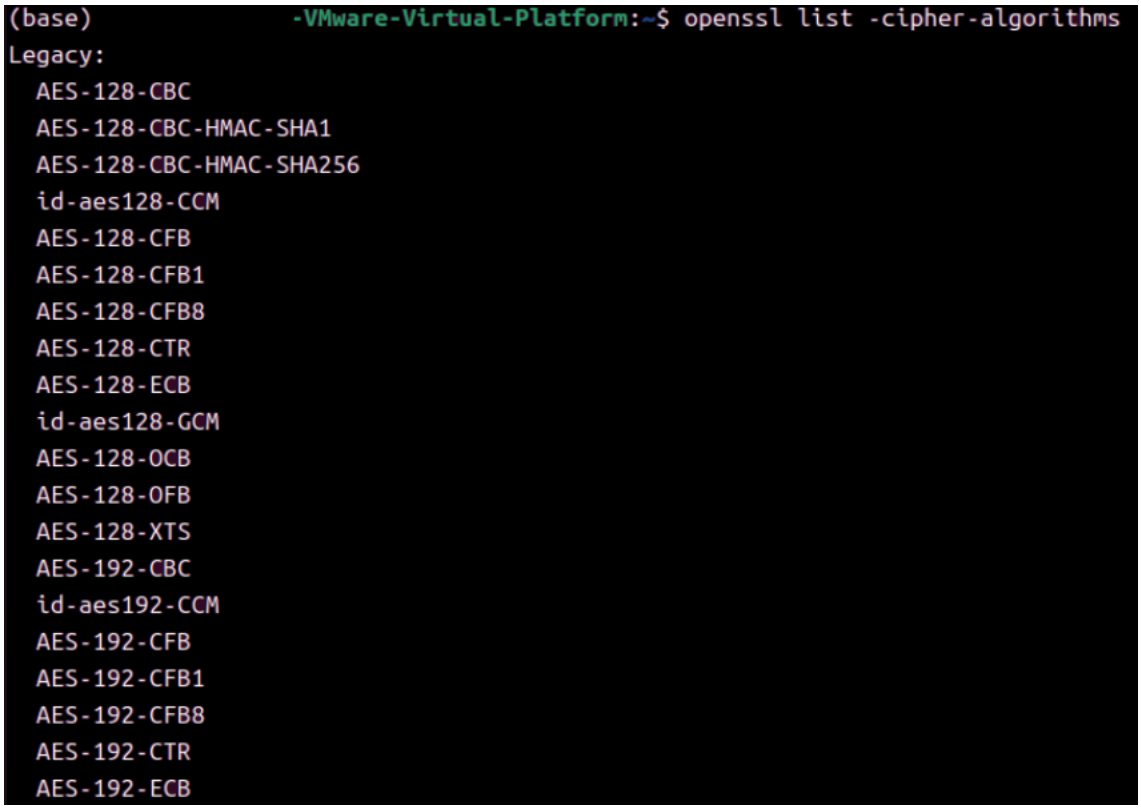


Figure 3-102 그림 제목

2.7.3 판정근거

Table 3-136 TE03.05.01 시험결과 판정근거

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

2.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.8 TE03.06.01

2.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.06.01	출력되는 모든 데이터가 데이터 출력 인터페이스를 통해 출력되는 지 확인	암호모듈 검사

2.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-137 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

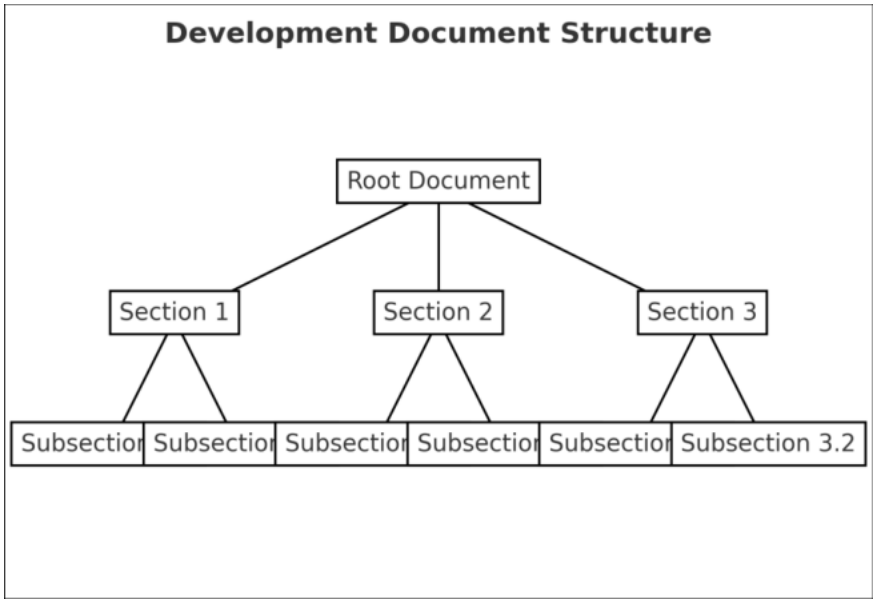


Figure 3-103 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-138 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

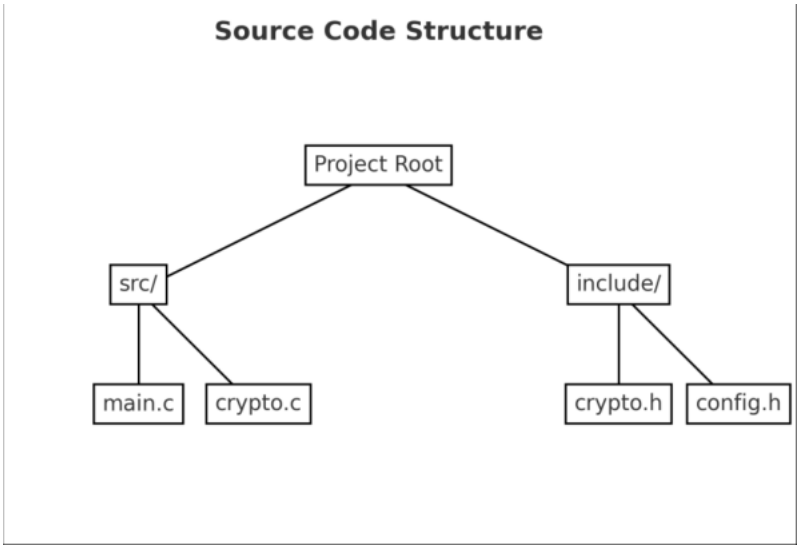


Figure 3-104 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-139 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

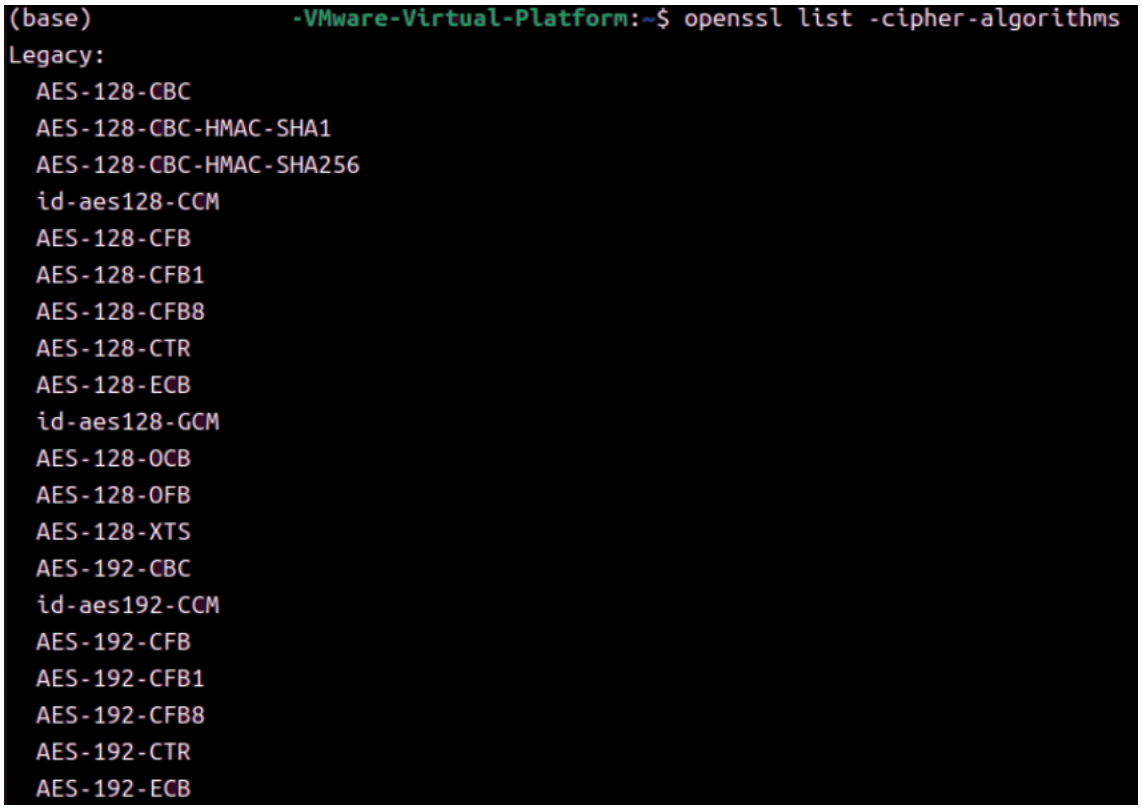


Figure 3-105 그림 제목

2.8.3 판정근거

Table 3-140 TE03.06.01 시험결과 판정근거

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

2.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.9 TE03.07.01

2.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.07.01	수동 SSP 주입 , 동작 전 자가시험 , 소프트웨어 로딩 , 제로화 동작 , 오류 상태인 경우 데이터 출력 금지	개발문서 검토

2.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-141 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

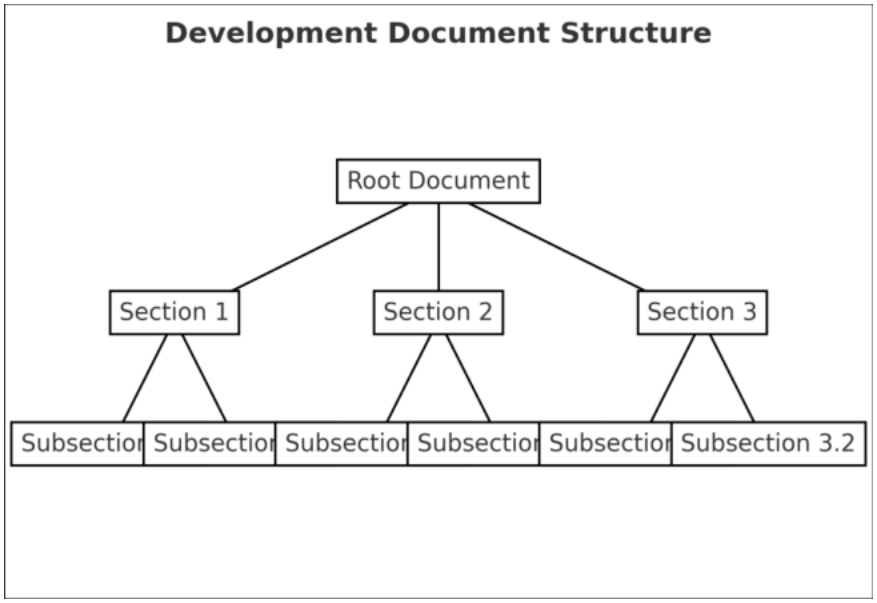


Figure 3-106 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-142 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

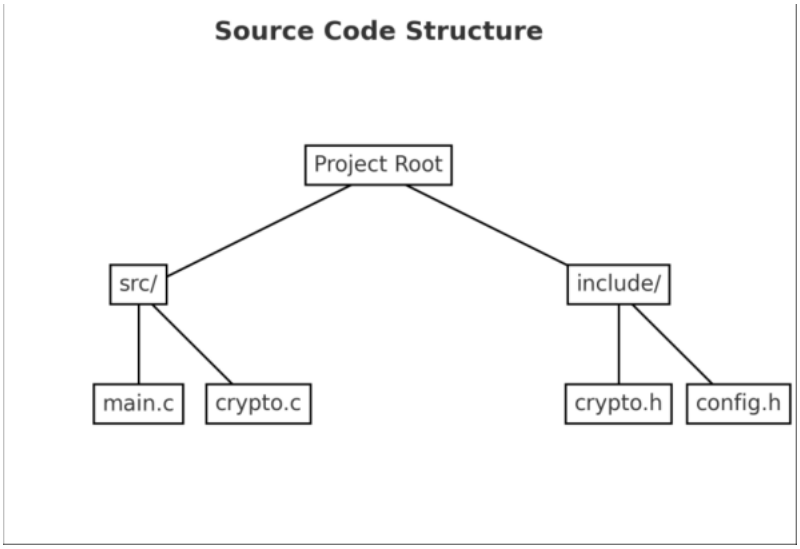


Figure 3-107 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-143 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

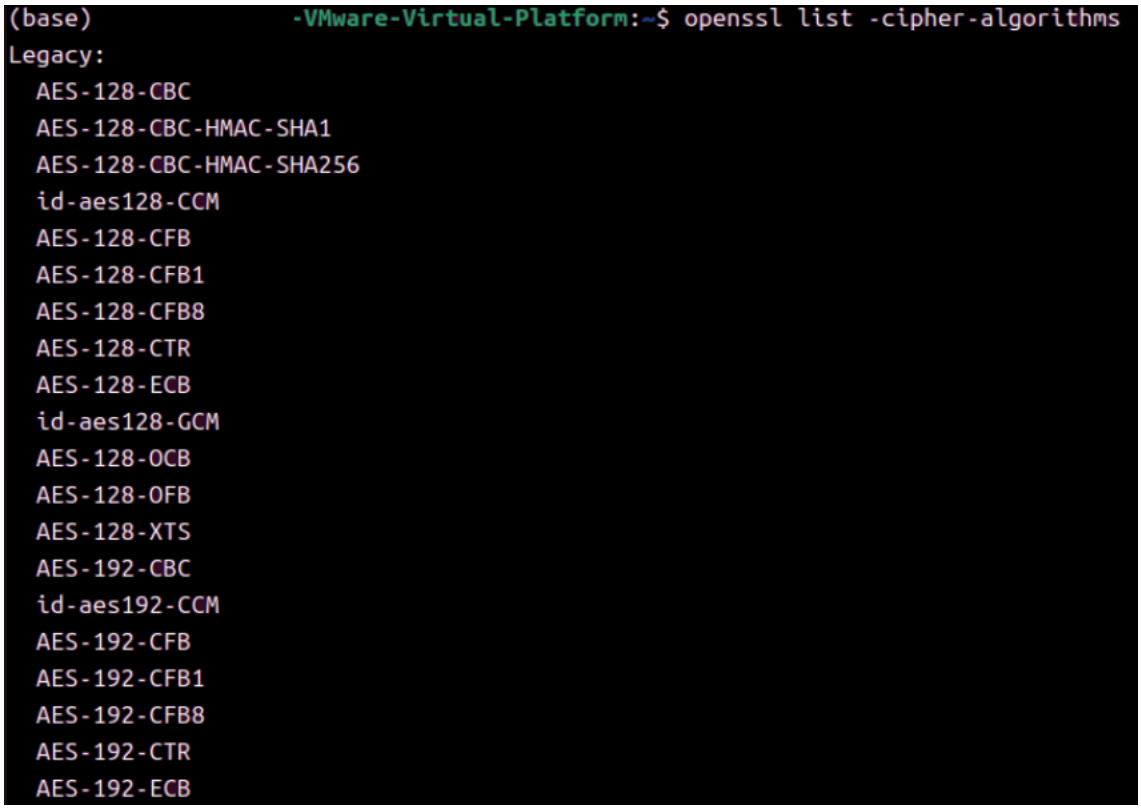


Figure 3-108 그림 제목

2.9.3 판정근거

Table 3-144 TE03.07.01 시험결과 판정근거

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

2.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.10 TE03.07.02

2.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.07.02	TE03.07.01 에 명세된 상태로 진입하여 데이터 출력 금지 확인	암호모듈 검사

2.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-145 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

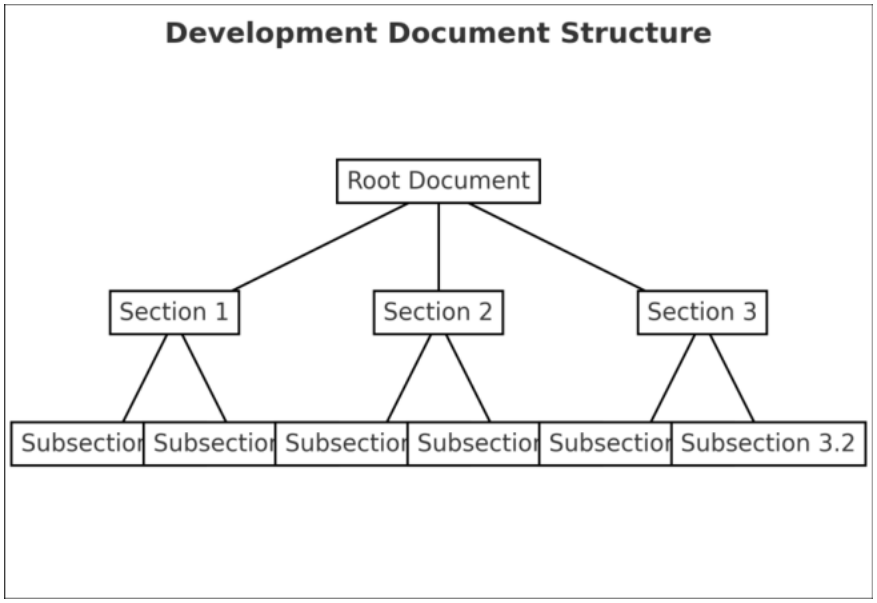


Figure 3-109 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-146 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

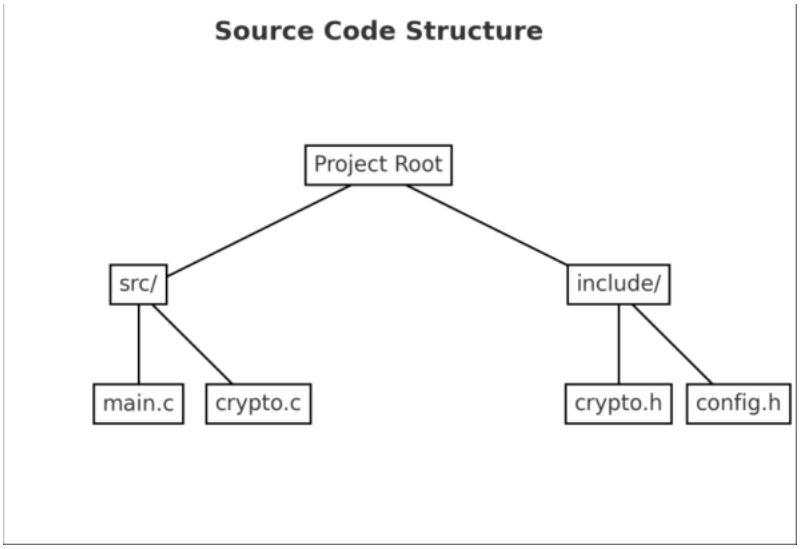


Figure 3-110 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-147 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

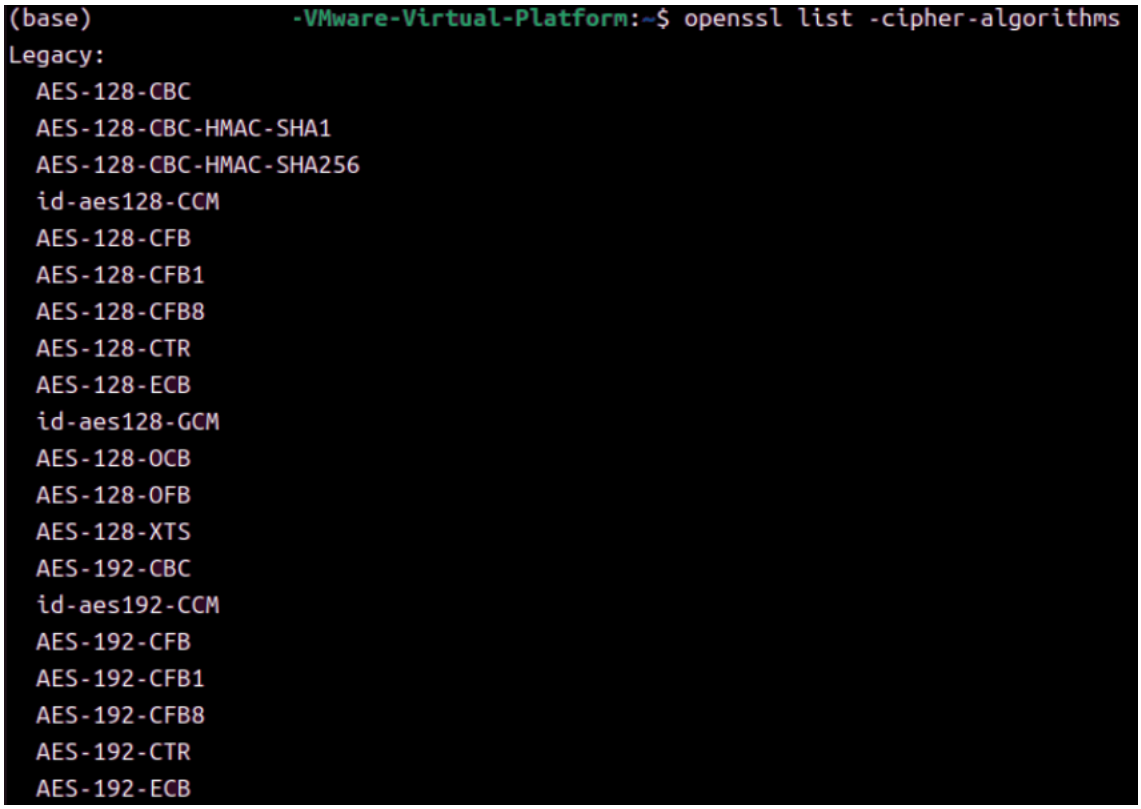


Figure 3-111 그림 제목

2.10.3 판정근거

Table 3-148 TE03.07.02 시험결과 판정근거

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

2.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.11 TE03.07.03

2.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.07.03	자가시험 상태에서 데이터 출력 금지 및 필요 시 자가시험 결과를 표시하는 상태 출력만 허용	개발문서 검토

2.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-149 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

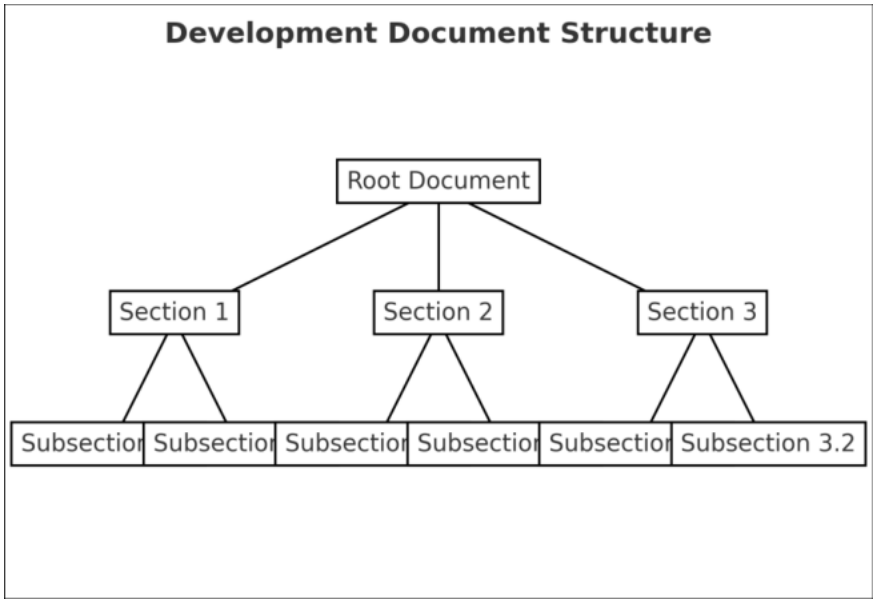


Figure 3-112 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-150 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

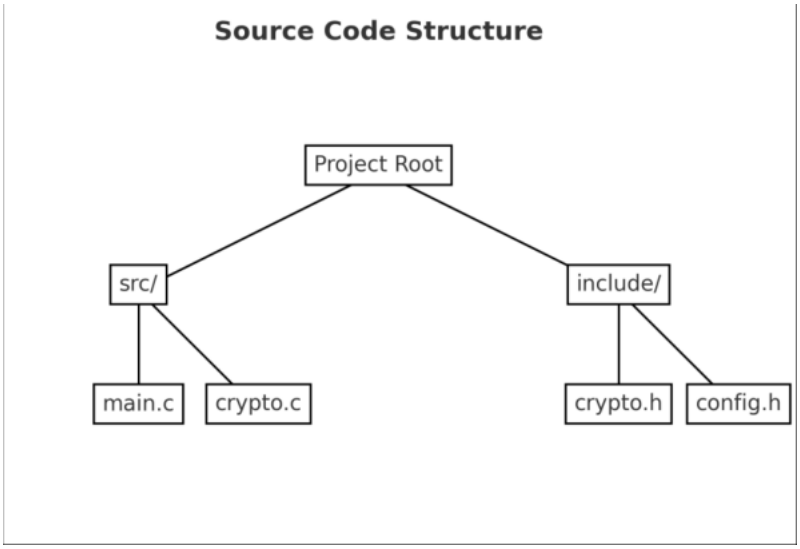


Figure 3-113 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-151 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

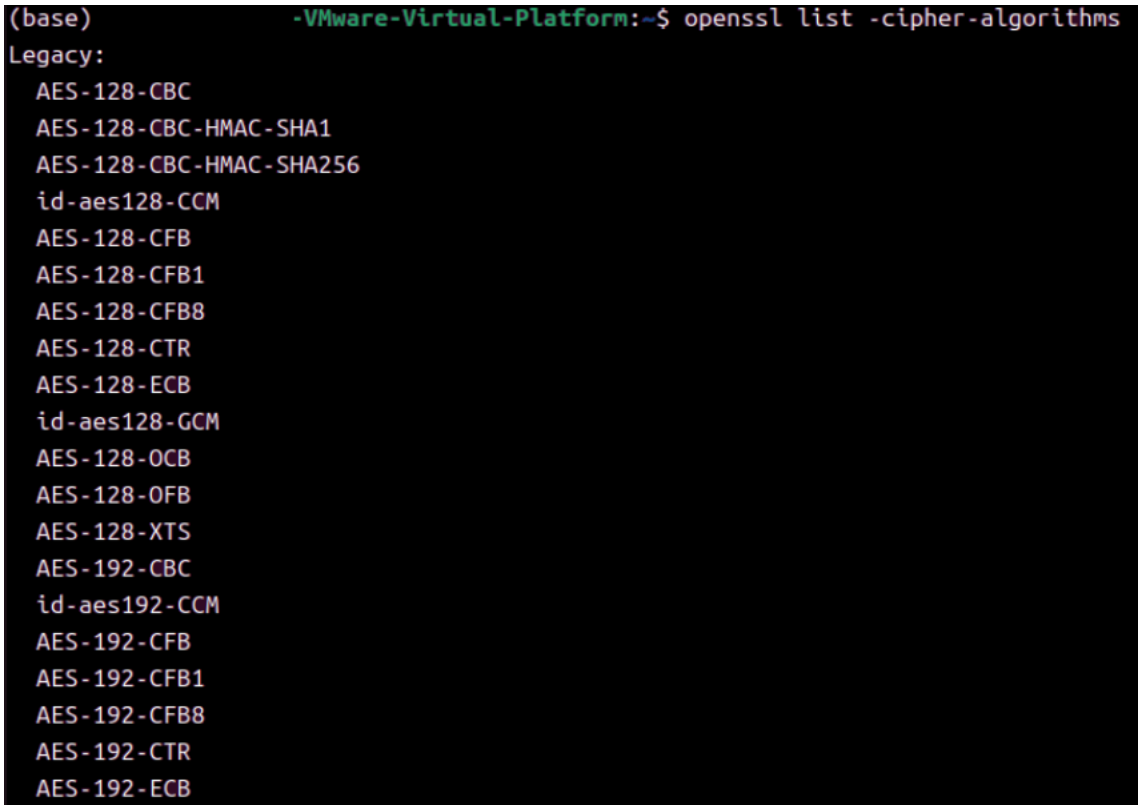


Figure 3-114 그림 제목

2.11.3 판정근거

Table 3-152 TE03.07.03 시험결과 판정근거

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

2.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.12 TE03.07.04

2.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.07.04	자가시험 동작하여 데이터 출력 금지 및 필요 시 자가시험 결과를 표시하는 상태 출력만 허용	암호모듈 검사

2.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-153 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

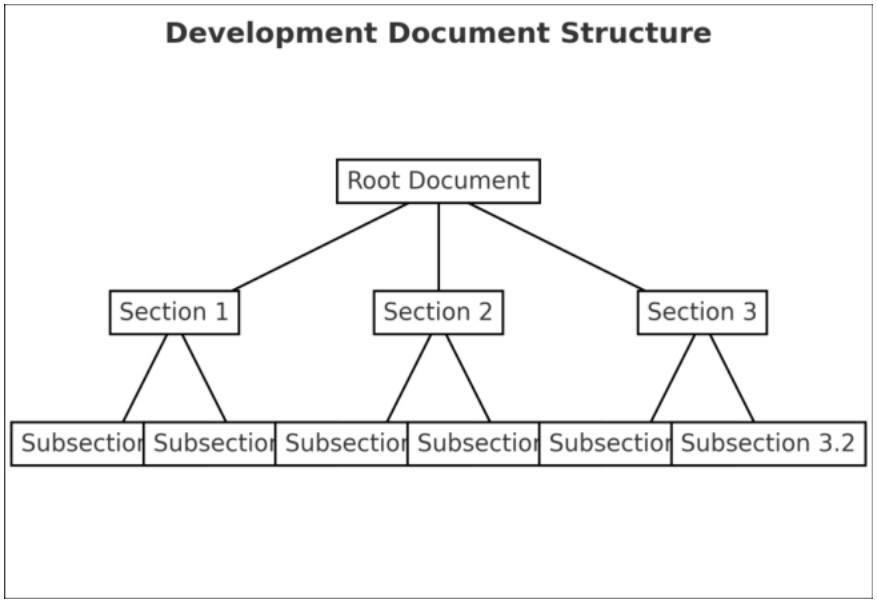


Figure 3-115 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-154 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

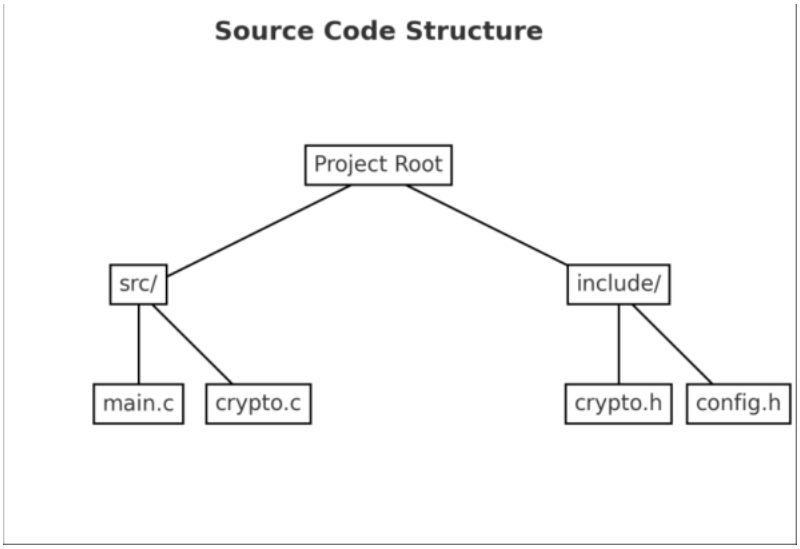


Figure 3-116 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-155 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

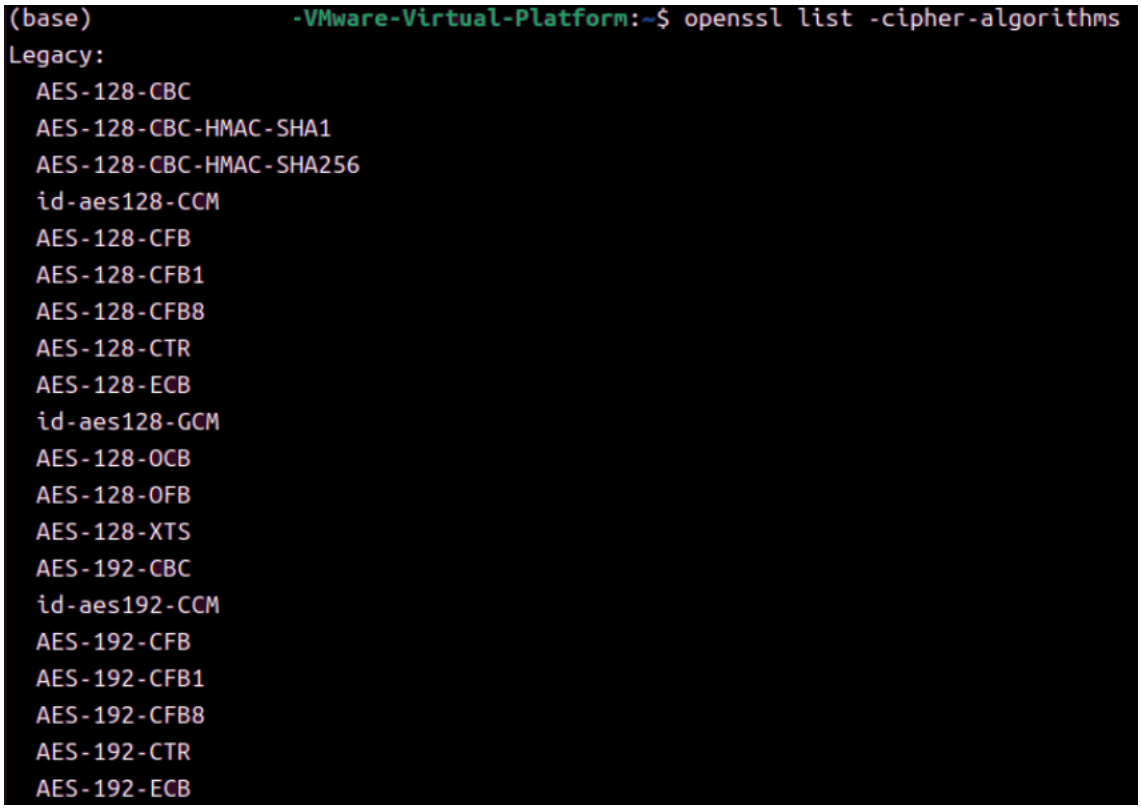


Figure 3-117 그림 제목

2.12.3 판정근거

Table 3-156 TE03.07.04 시험결과 판정근거

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

2.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.13 TE03.07.05

2.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.07.05	오류상태나 자가시험 조건에서 데이터 출력 금지	개발문서 검토

2.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-157 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

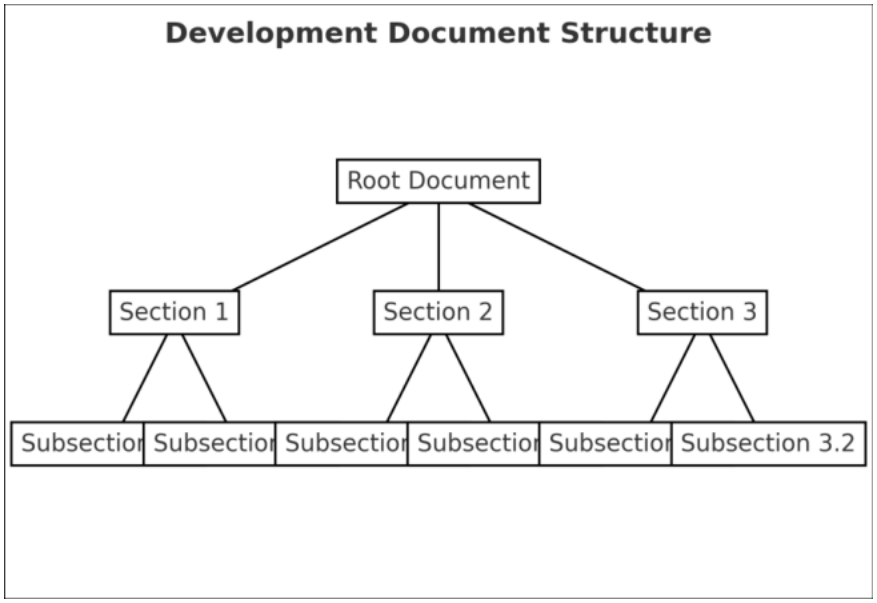


Figure 3-118 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-158 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

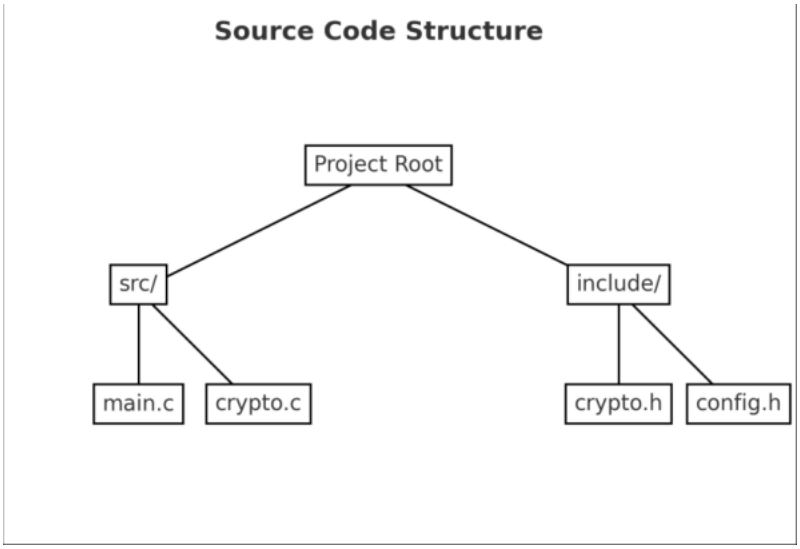


Figure 3-119 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-159 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

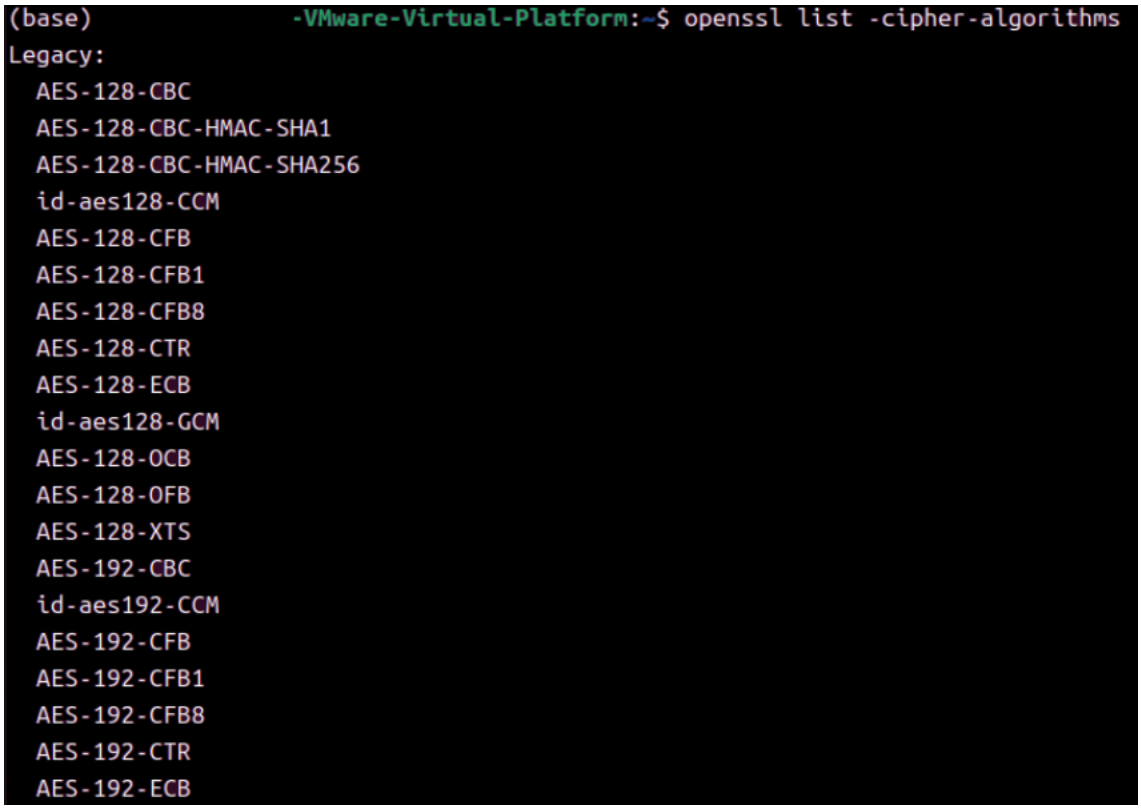


Figure 3-120 그림 제목

2.13.3 판정근거

Table 3-160 TE03.07.05 시험결과 판정근거

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

2.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.14 TE03.08.01

2.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.08.01	모든 제어 데이터가 제어 입력 인터페이스를 통해 입력되는지 여부	암호모듈 검사

2.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-161 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

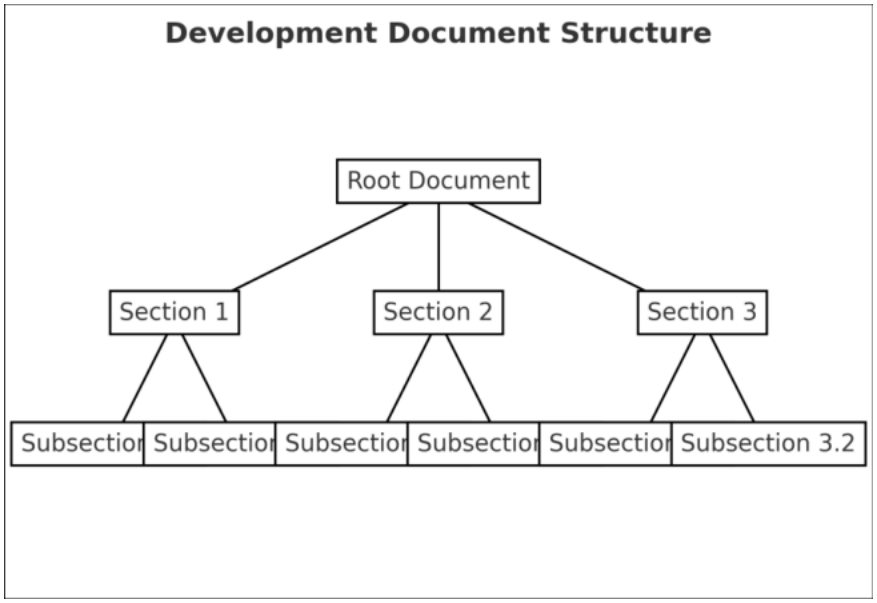


Figure 3-121 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-162 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

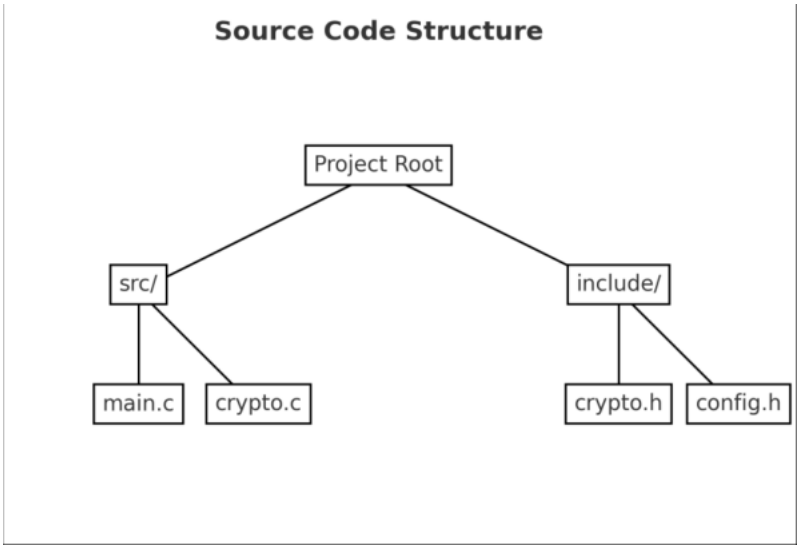


Figure 3-122 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-163 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

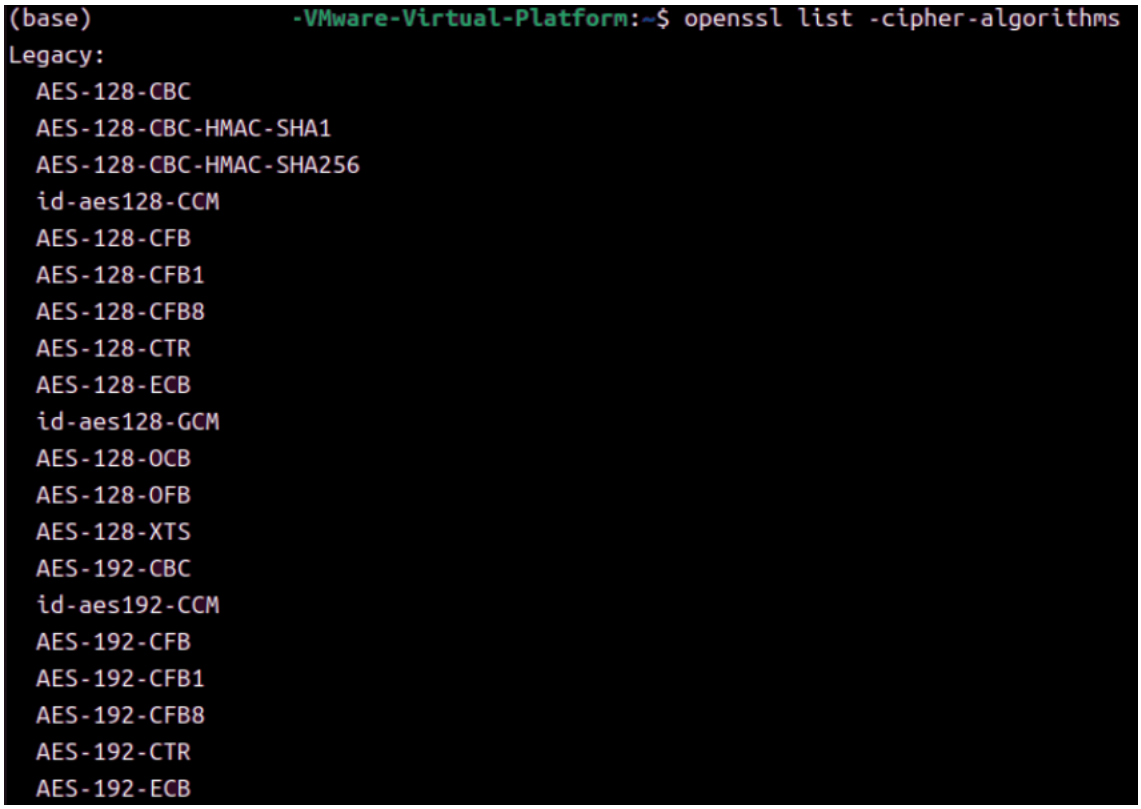


Figure 3-123 그림 제목

2.14.3 판정근거

Table 3-164 TE03.08.01 시험결과 판정근거

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

2.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.15 TE03.09.01

2.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.09.01	제어 출력 인터페이스 및 모든 출력 명령과 신호 , 제어 데이터 명세	개발문서 검토

2.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-165 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

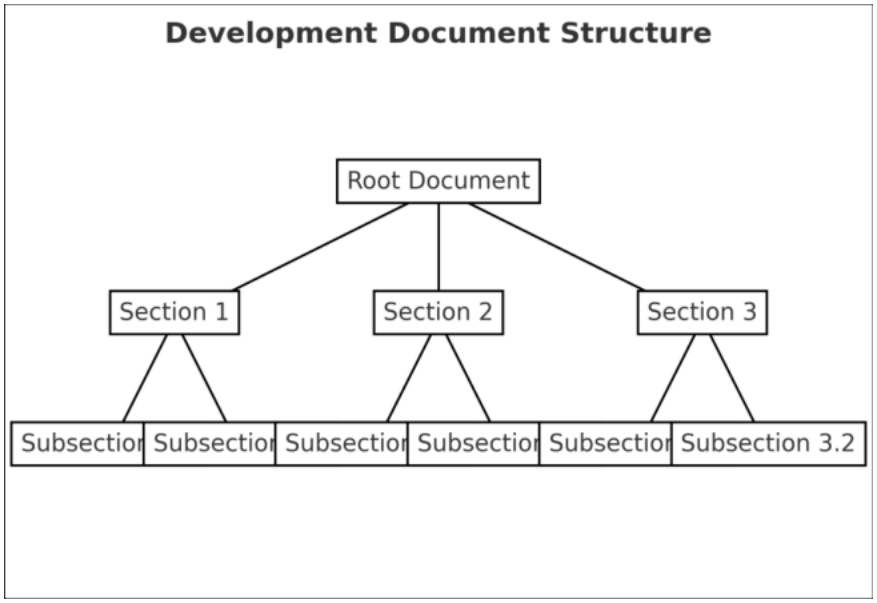


Figure 3-124 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-166 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

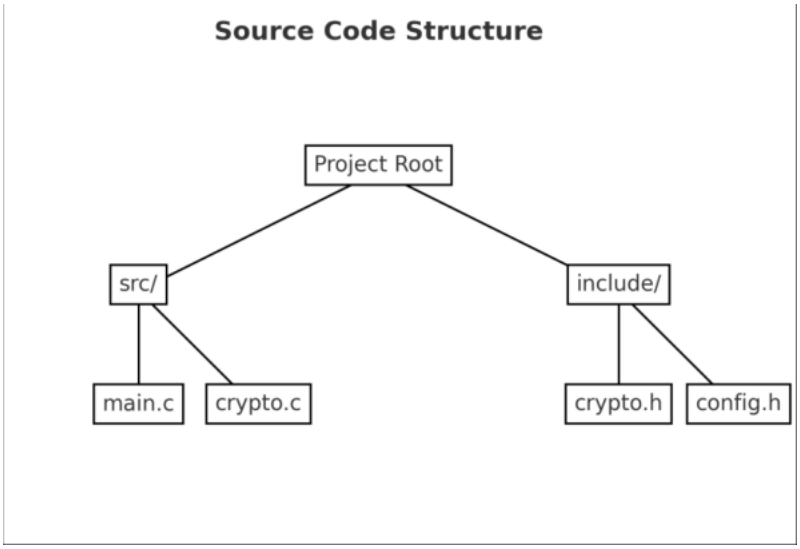


Figure 3-125 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-167 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

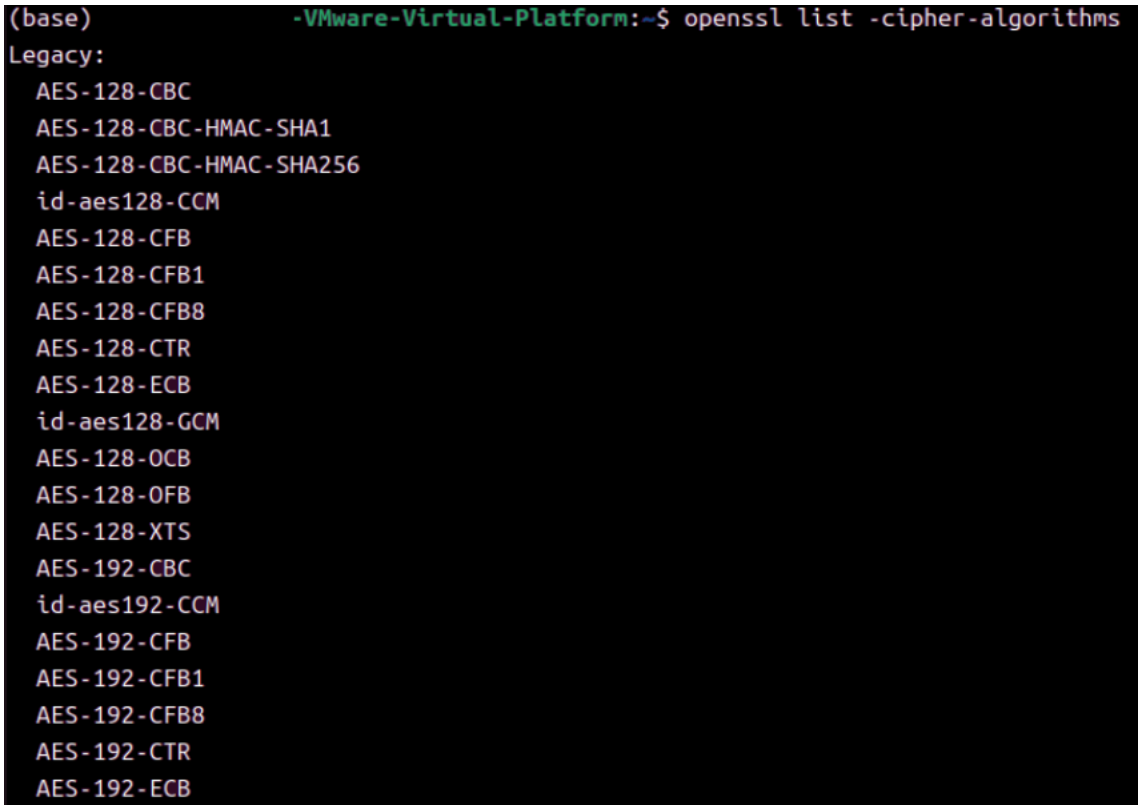


Figure 3-126 그림 제목

2.15.3 판정근거

Table 3-168 TE03.09.01 시험결과 판정근거

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

2.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.16 TE03.09.02

2.16.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.09.02	제어 출력 인터페이스가 명세대로 작동	암호모듈 검사

2.16.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-169 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

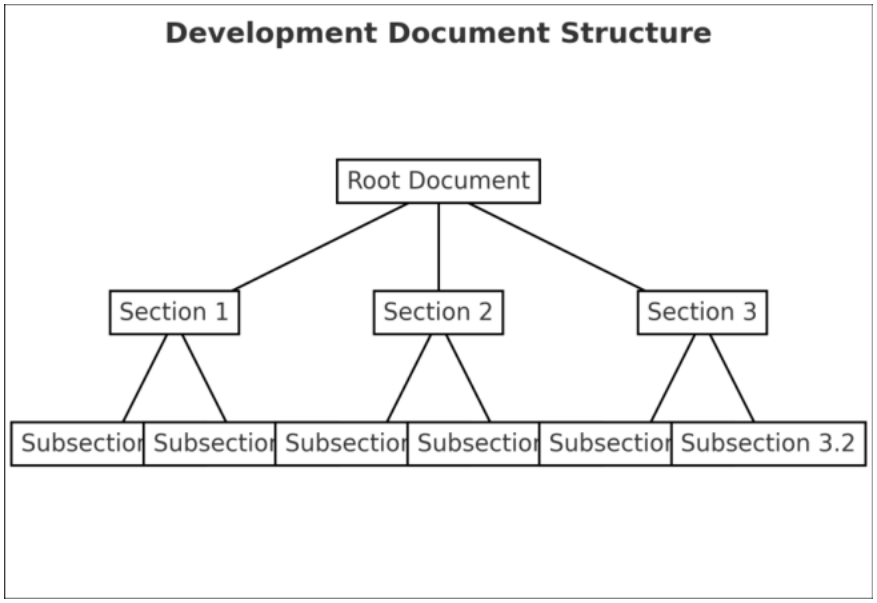


Figure 3-127 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-170 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

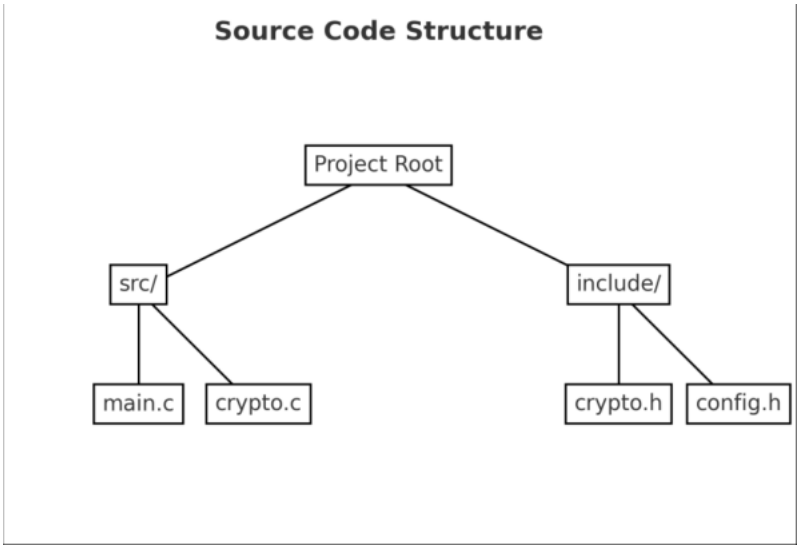


Figure 3-128 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-171 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

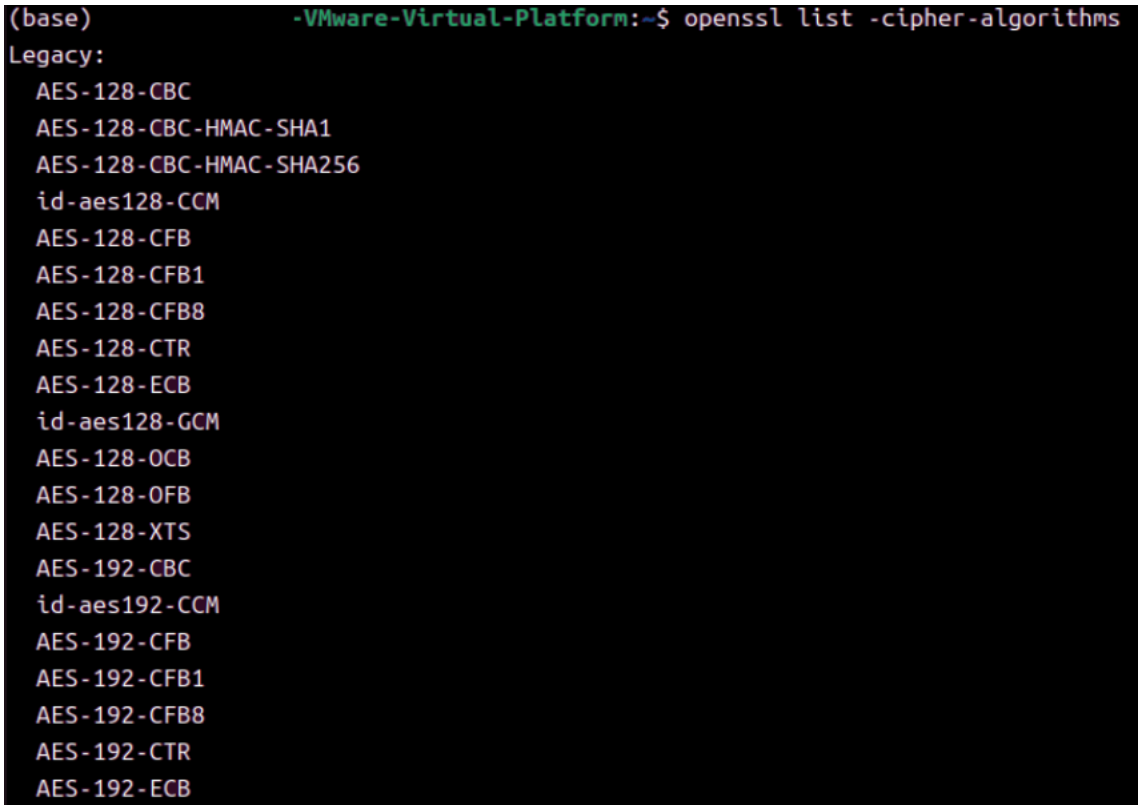


Figure 3-129 그림 제목

2.16.3 판정근거

Table 3-172 TE03.09.02 시험결과 판정근거

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

2.16.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.17 TE03.10.01

2.17.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.10.01	오류 상태에서 제어 출력 인터페이스를 통한 모든 제어 출력 금지 및 상태 정보만 출력	개발문서 검토

2.17.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-173 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

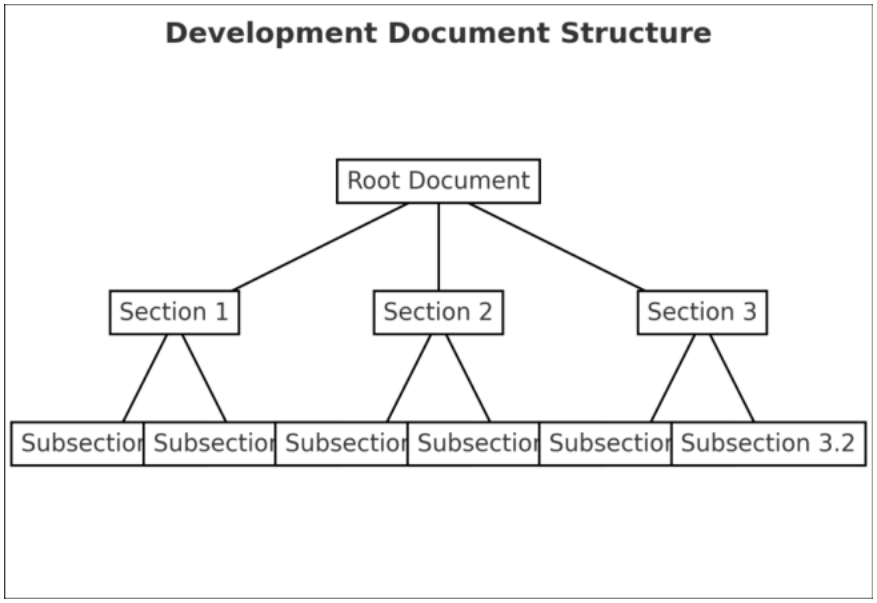


Figure 3-130 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-174 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

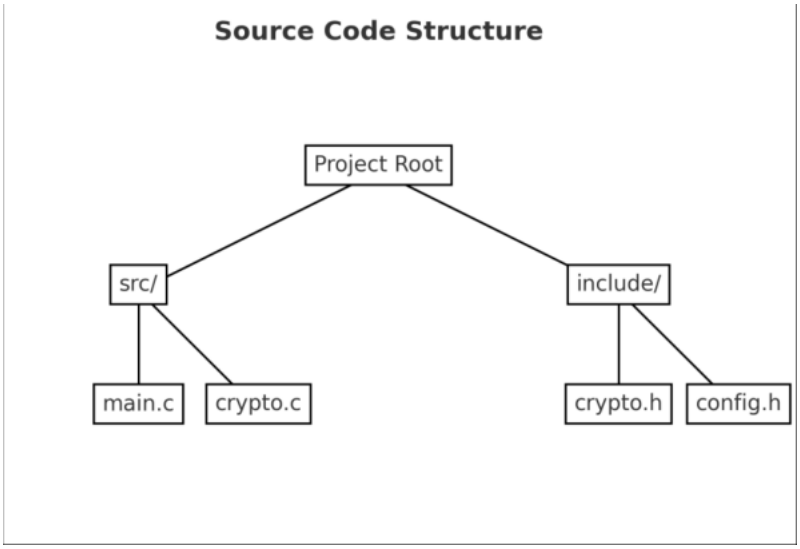


Figure 3-131 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-175 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

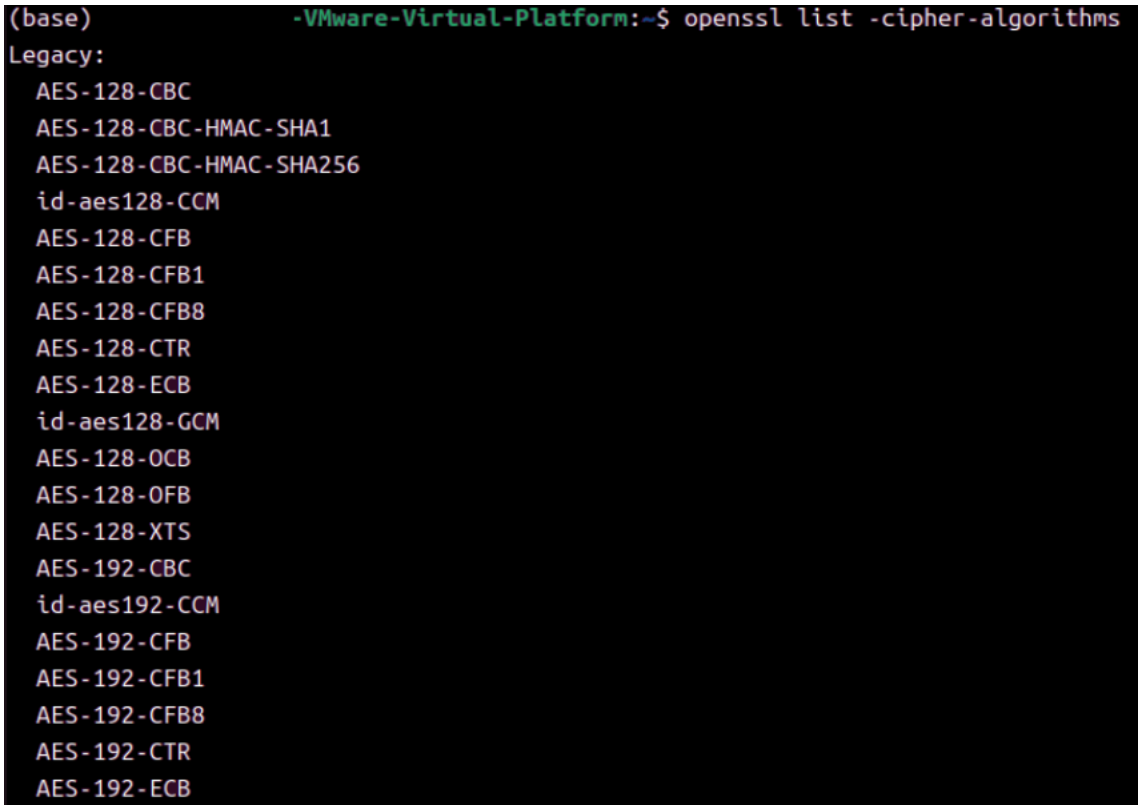


Figure 3-132 그림 제목

2.17.3 판정근거

Table 3-176 TE03.10.01 시험결과 판정근거

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

2.17.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.18 TE03.10.02

2.18.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.10.02	오류 상태에서 모든 제어 출력 금지 및 오류 유형의 상태 정보만 출력	암호모듈 검사

2.18.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-177 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

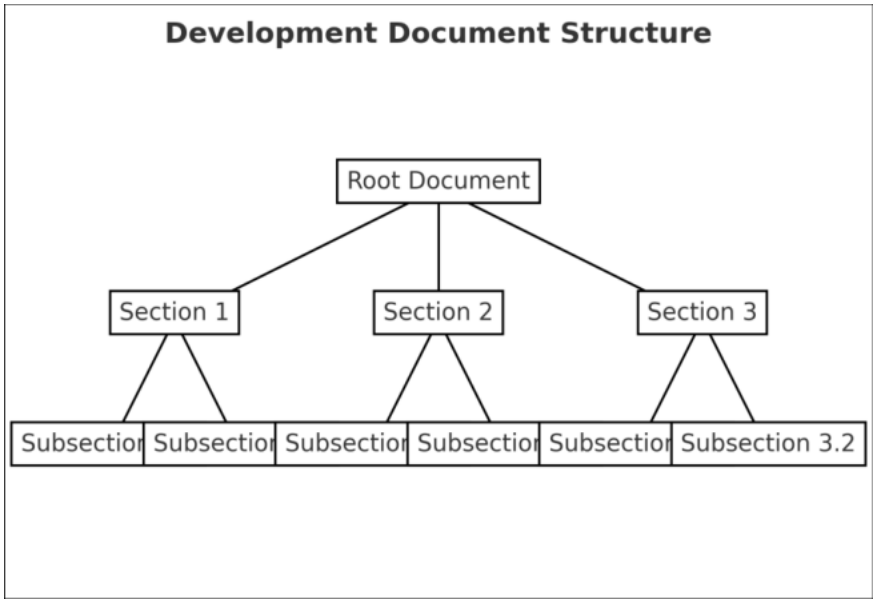


Figure 3-133 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-178 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

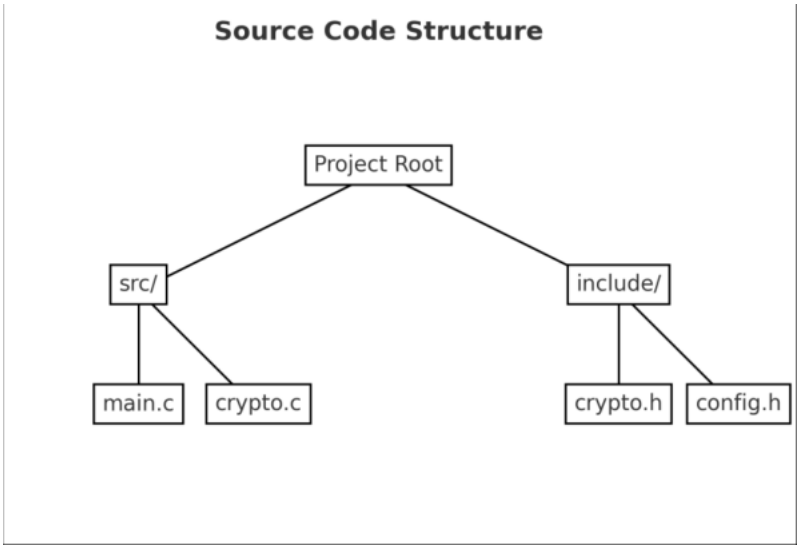


Figure 3-134 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-179 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

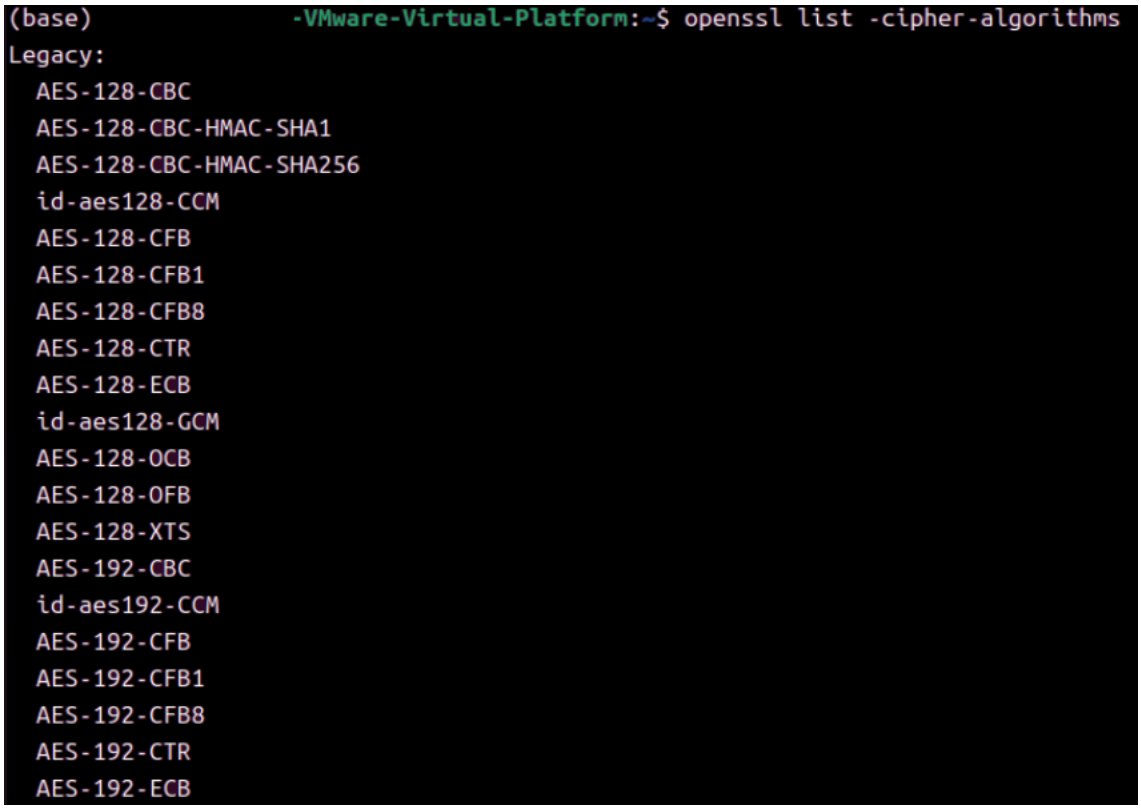


Figure 3-135 그림 제목

2.18.3 판정근거

Table 3-180 TE03.10.02 시험결과 판정근거

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

2.18.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.19 TE03.10.03

2.19.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.10.03	자가시험 상태에서 제어 출력 인터페이스를 통한 모든 제어 출력 금지 및 상태 정보만 출력	개발문서 검토

2.19.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-181 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

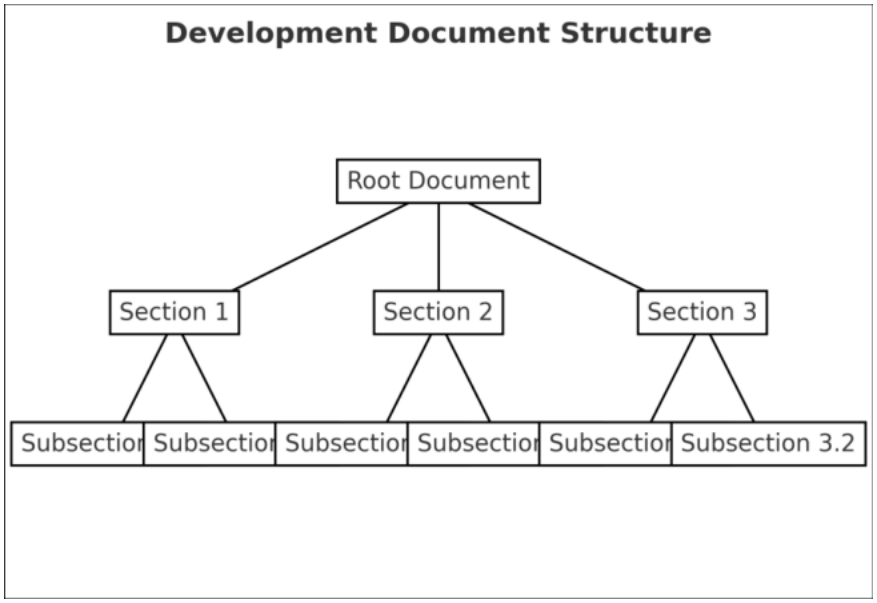


Figure 3-136 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-182 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

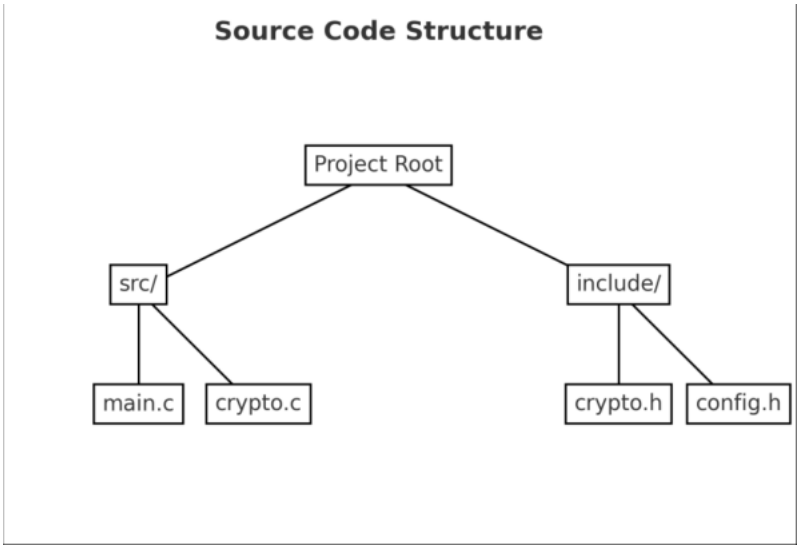


Figure 3-137 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-183 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

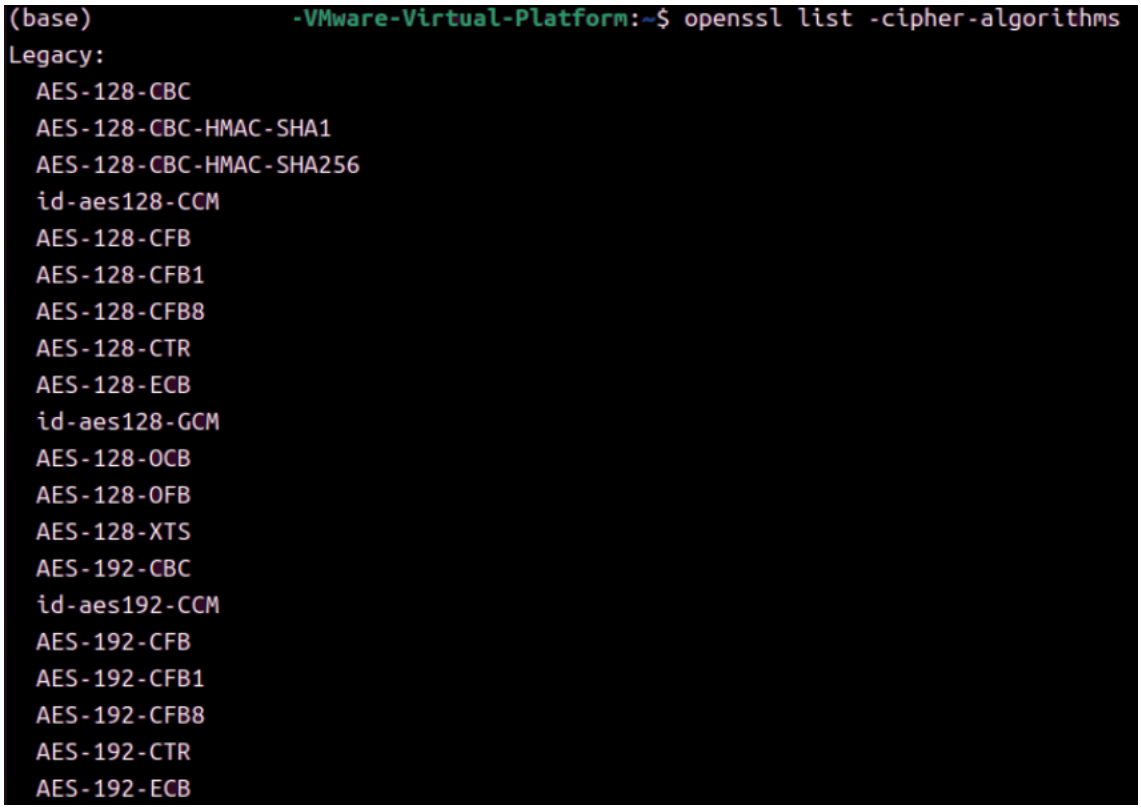


Figure 3-138 그림 제목

2.19.3 판정근거

Table 3-184 TE03.10.03 시험결과 판정근거

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

2.19.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.20 TE03.10.04

2.20.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.10.04	자가시험 수행하여 모든 제어 출력 금지 및 자가시험 결과 표시를 위한 상태 정보만 출력	암호모듈 검사

2.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-185 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

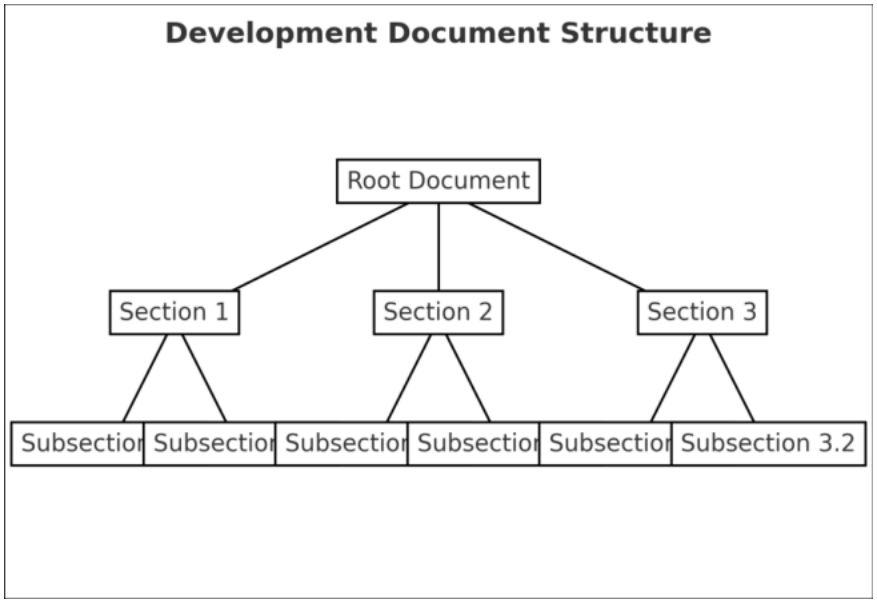


Figure 3-139 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-186 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

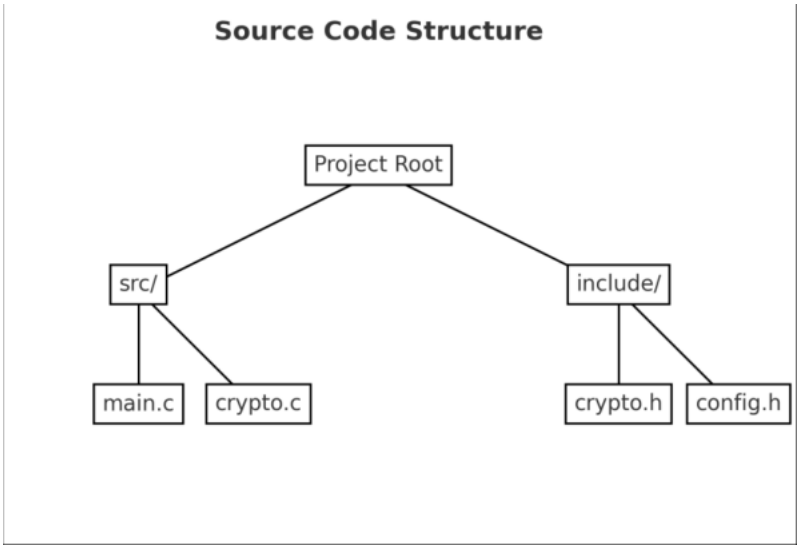


Figure 3-140 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-187 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

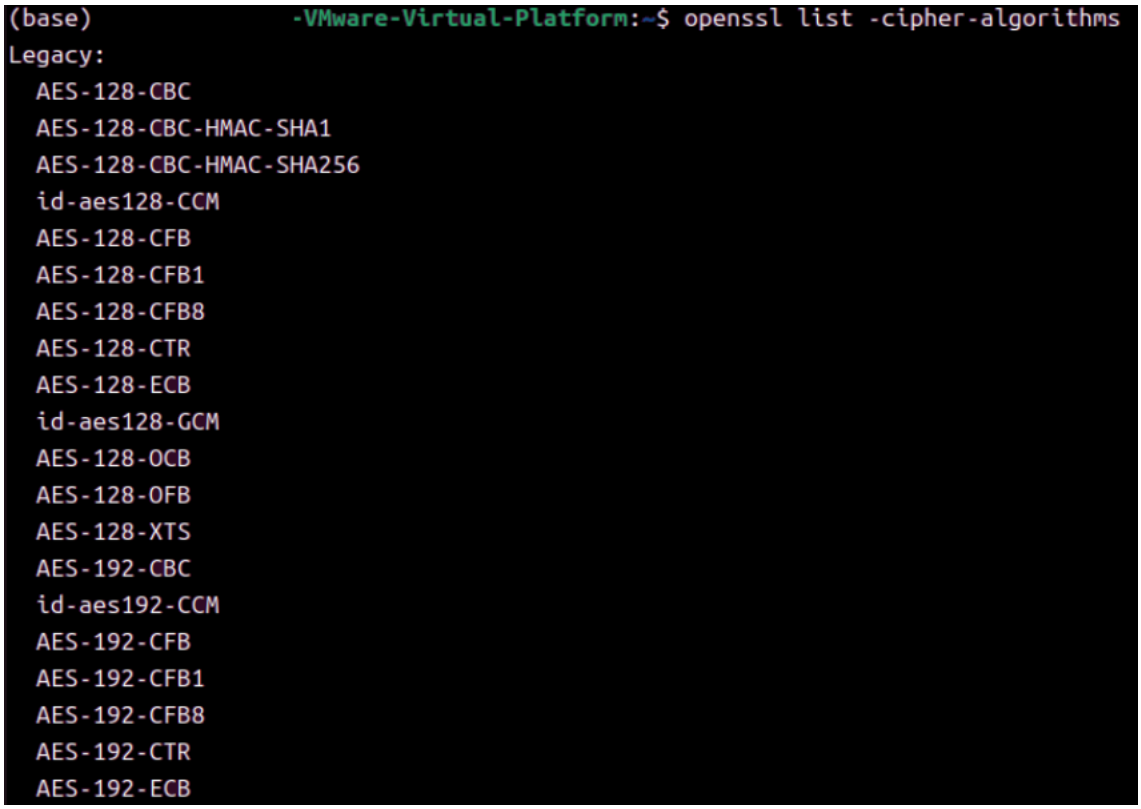


Figure 3-141 그림 제목

2.20.3 판정근거

Table 3-188 TE03.10.04 시험결과 판정근거

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

2.20.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.21 TE03.10.05

2.21.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.10.05	오류 상태나 자가시험 상태에서 모든 제어 출력 금지	개발문서 검토

2.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-189 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

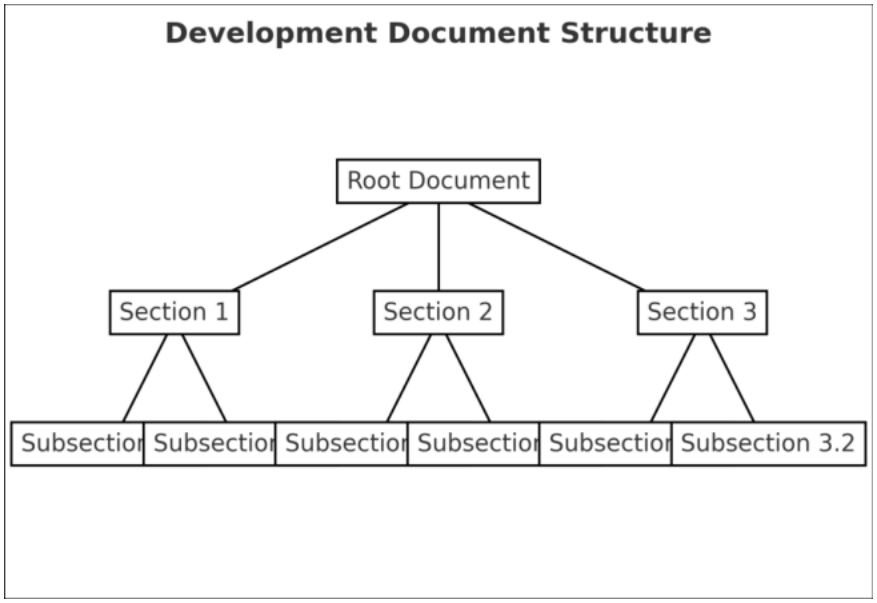


Figure 3-142 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-190 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

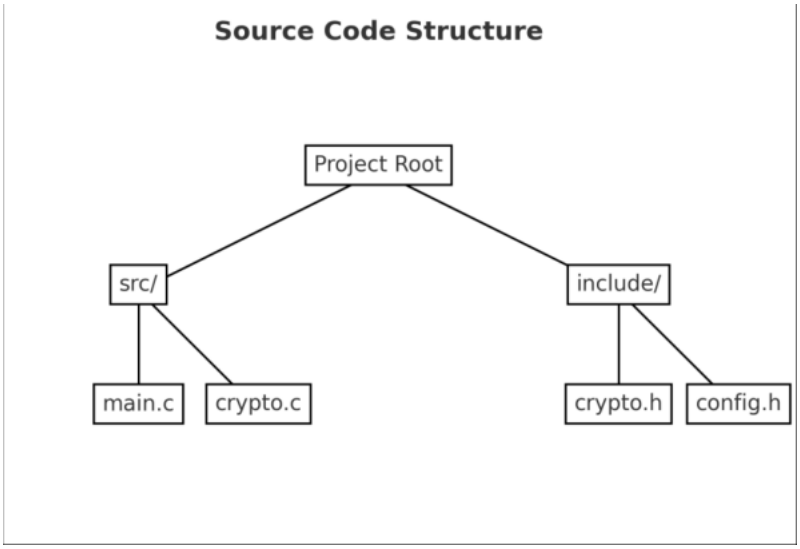


Figure 3-143 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-191 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

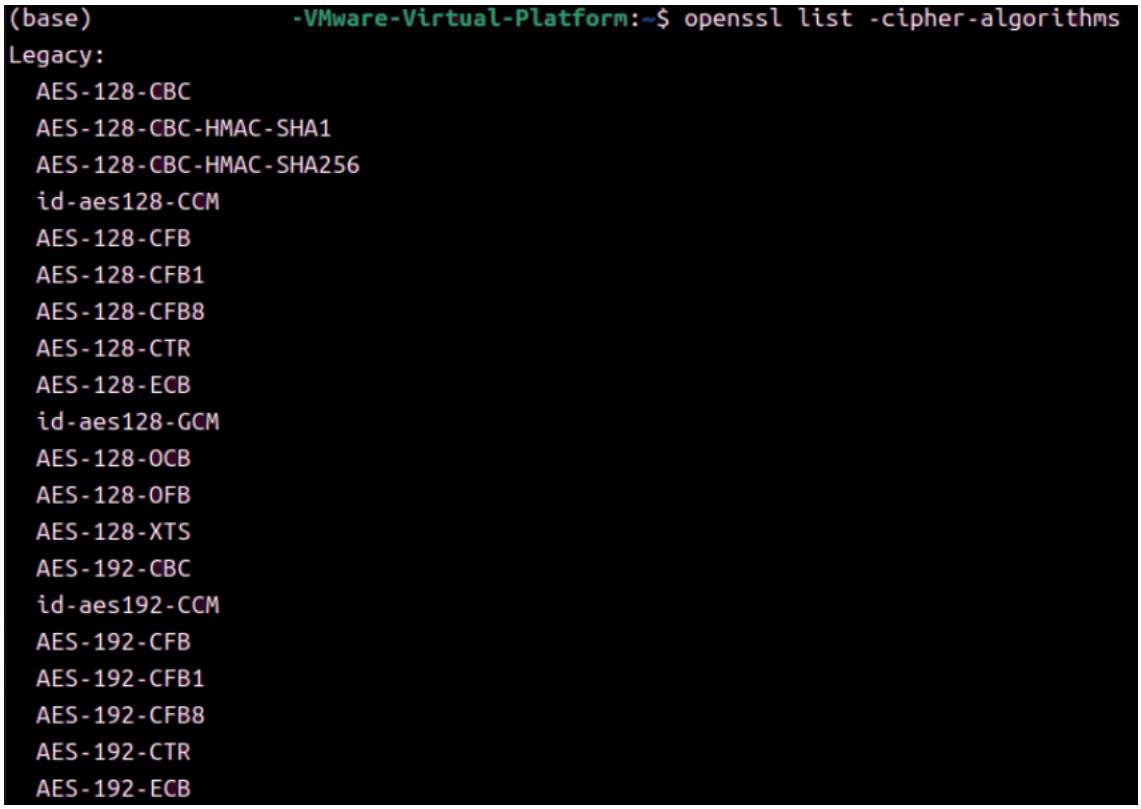


Figure 3-144 그림 제목

2.21.3 판정근거

Table 3-192 TE03.10.05 시험결과 판정근거

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

2.21.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.22 TE03.11.01

2.22.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.11.01	상태 출력 인터페이스 동작	암호모듈 검사

2.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-193 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

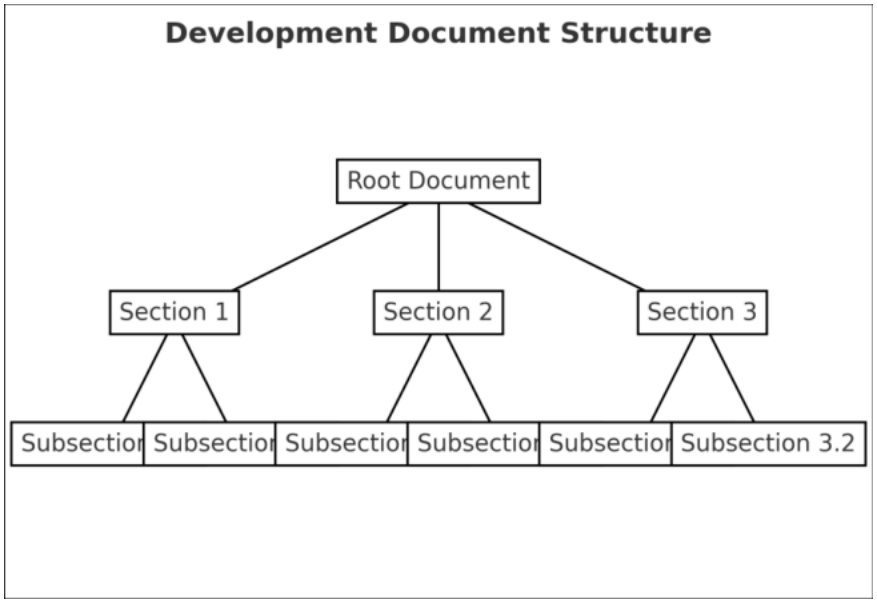


Figure 3-145 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-194 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

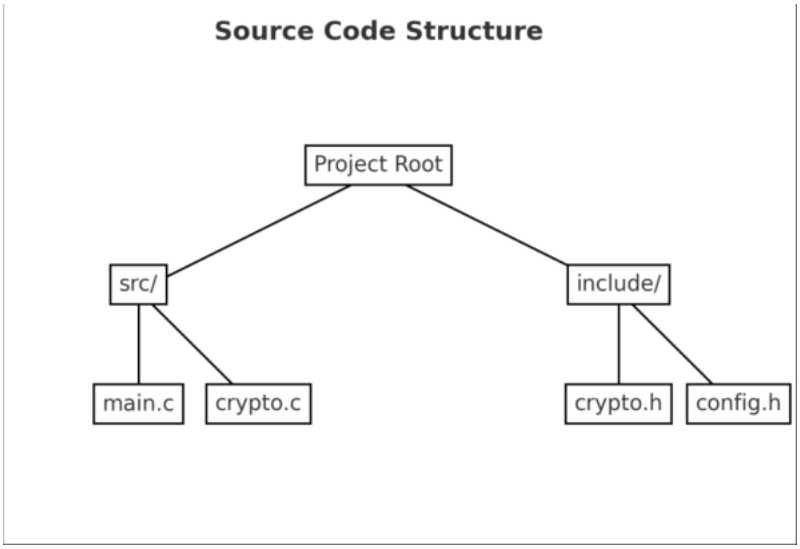


Figure 3-146 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-195 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

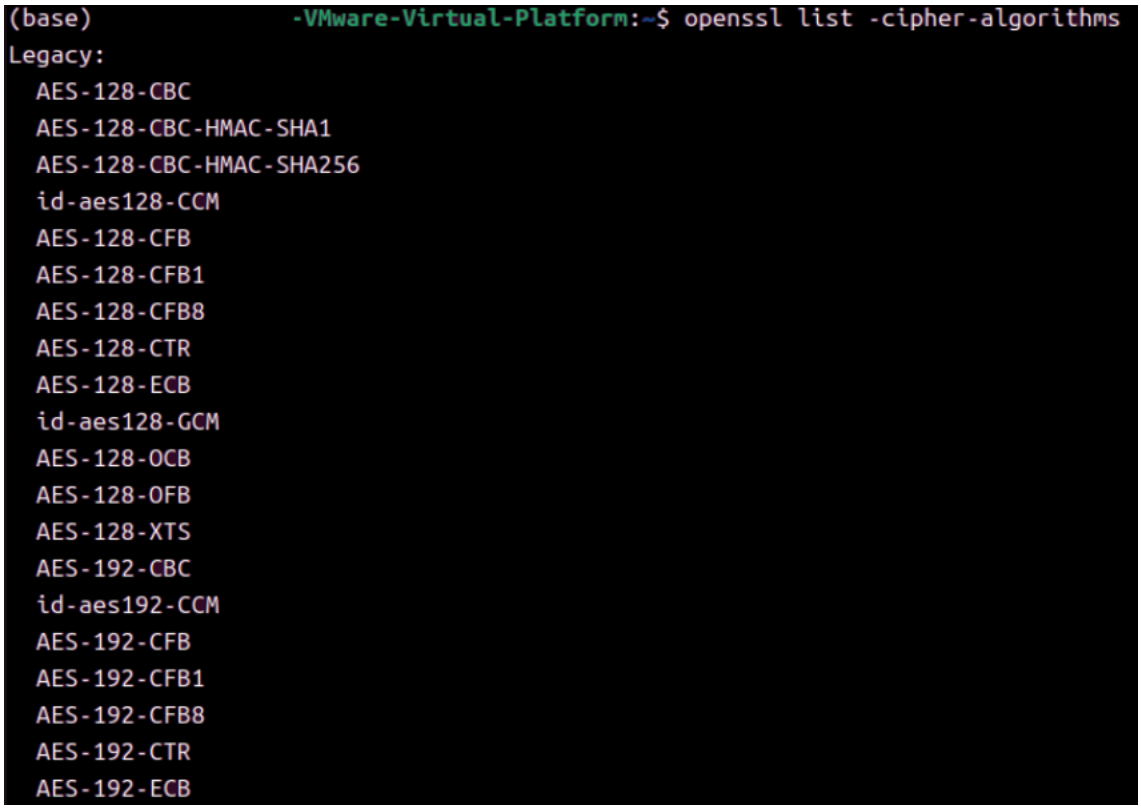


Figure 3-147 그림 제목

2.22.3 판정근거

Table 3-196 TE03.11.01 시험결과 판정근거

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

2.22.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.23 TE03.11.02

2.23.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.11.02	상태 출력 인터페이스의 외부 출력 장치 사용 명세	개발문서 검토

2.23.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-197 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

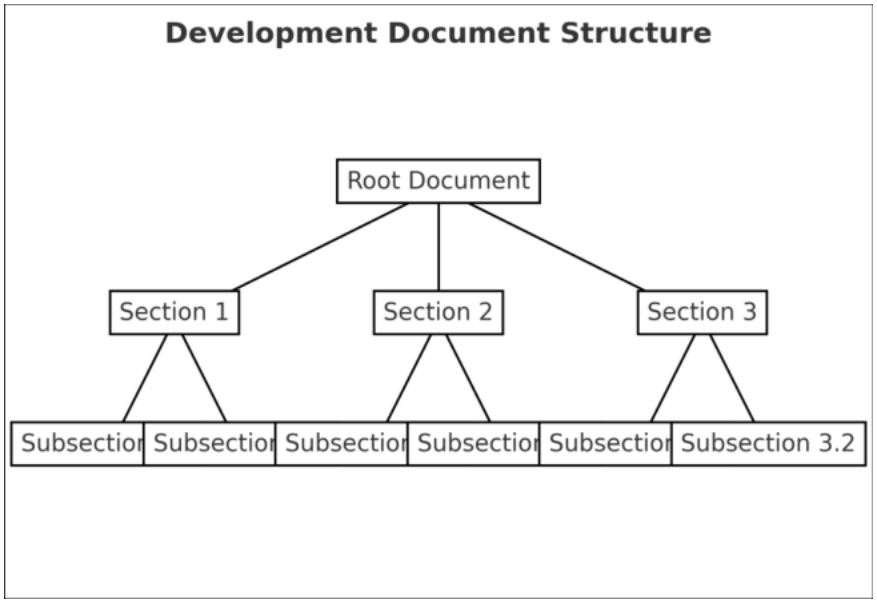


Figure 3-148 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-198 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

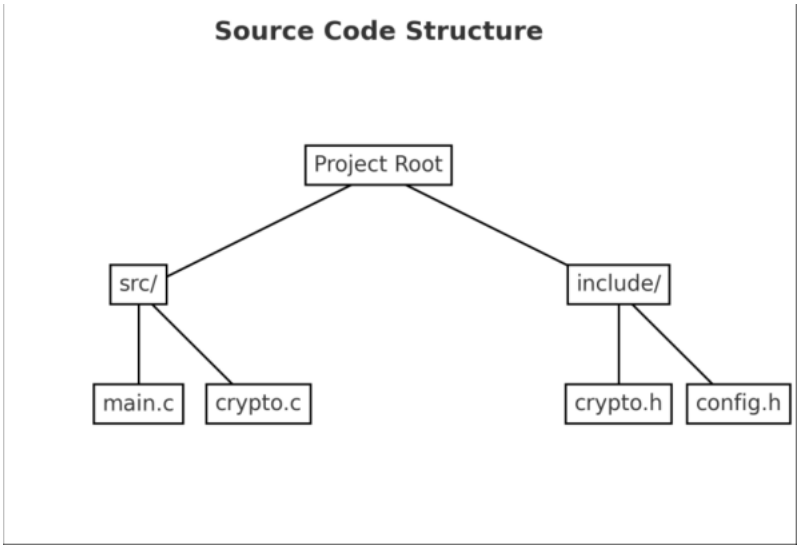


Figure 3-149 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-199 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

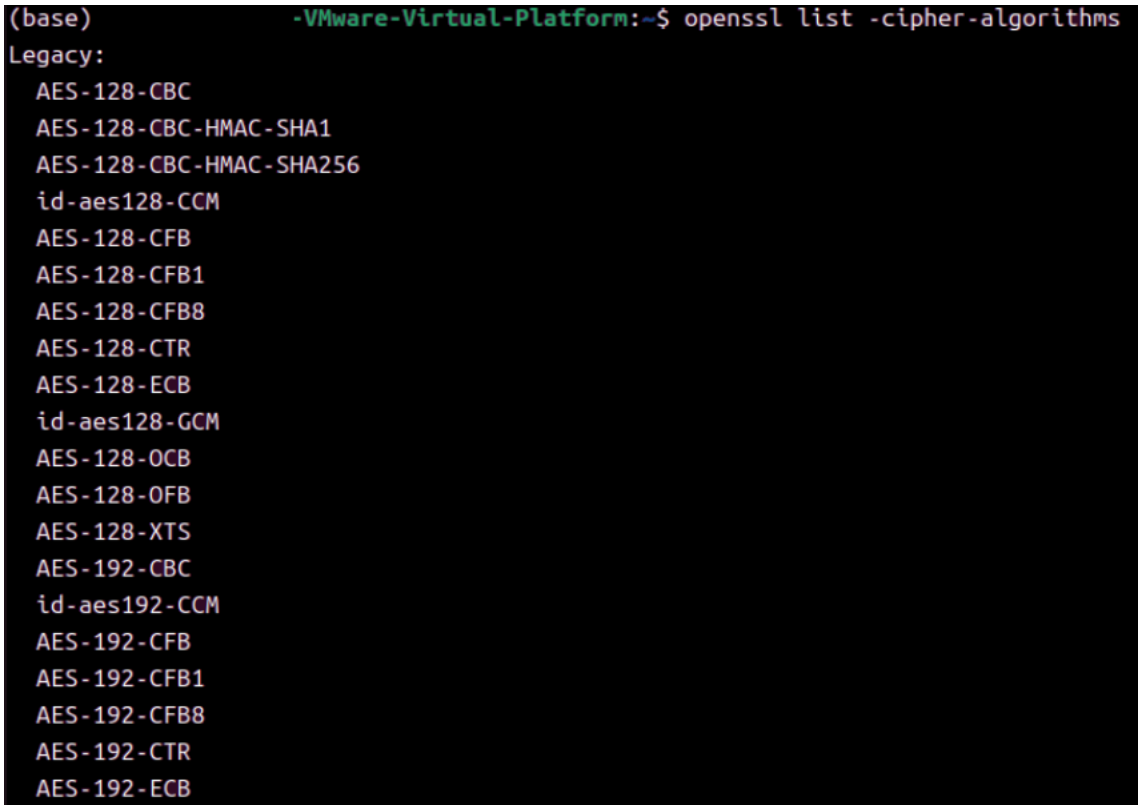


Figure 3-150 그림 제목

2.23.3 판정근거

Table 3-200 TE03.11.02 시험결과 판정근거

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

2.23.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.24 TE03.15.01

2.24.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.01	데이터 입력 인터페이스를 통해 입력되는 데이터에 사용되는 물리적·논리적 경로 명세 여부	개발문서 검토

2.24.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-201 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

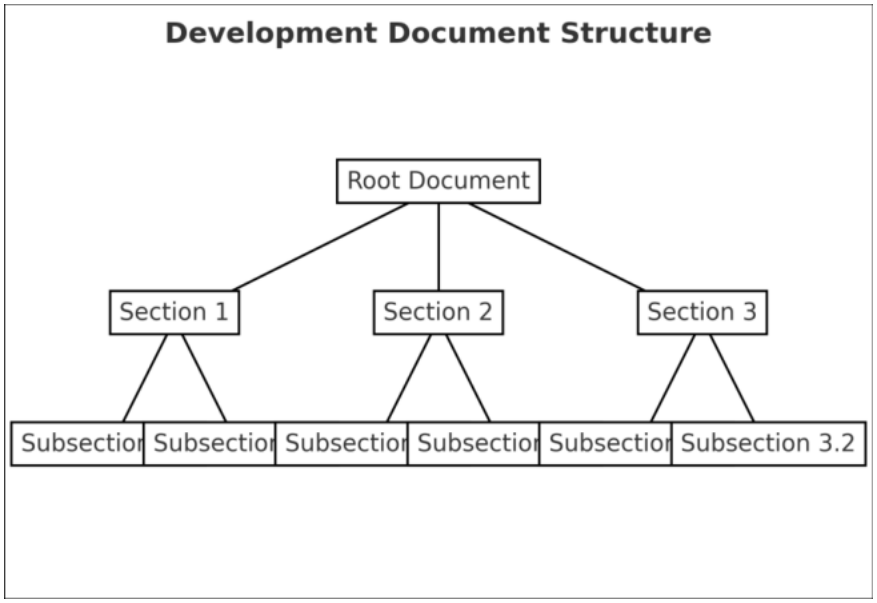


Figure 3-151 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-202 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

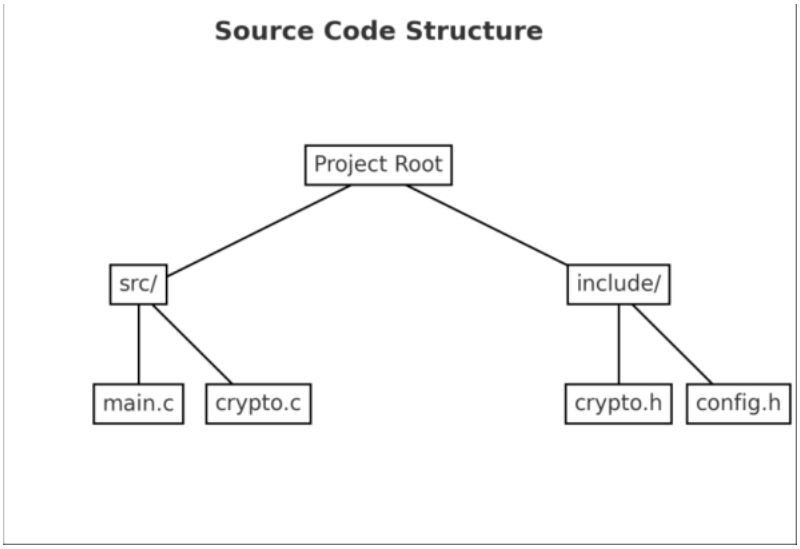


Figure 3-152 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-203 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

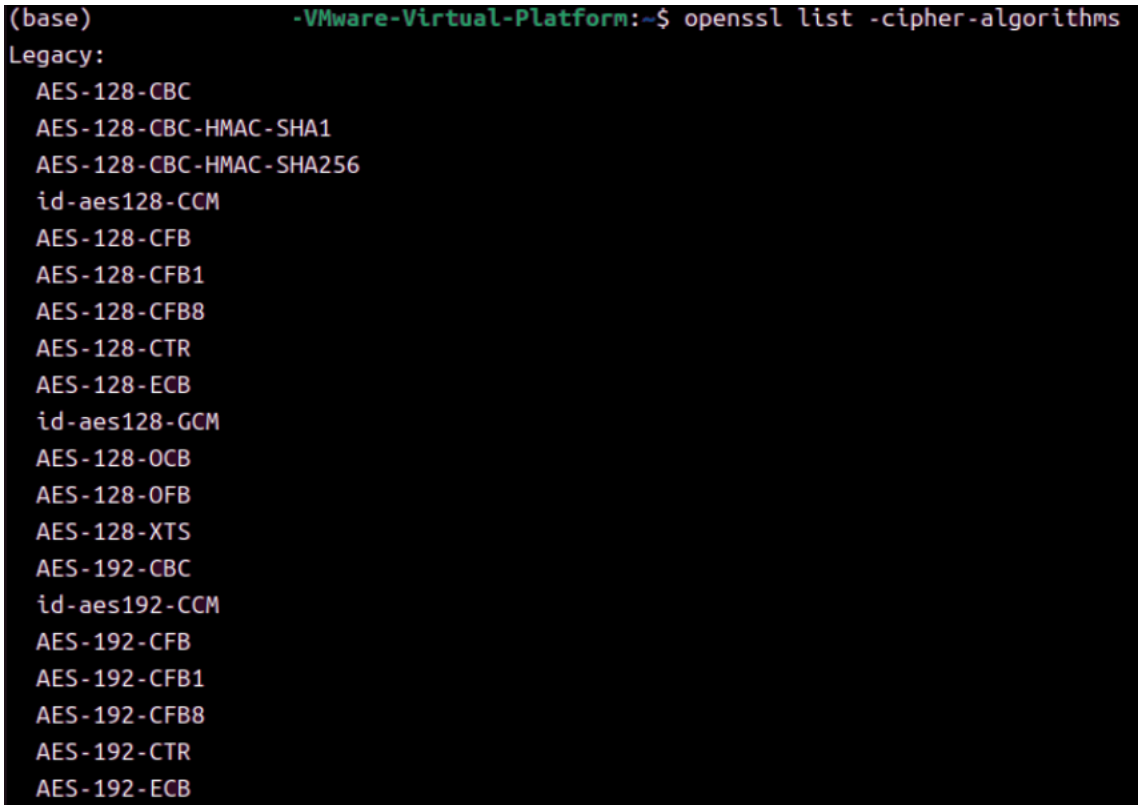


Figure 3-153 그림 제목

2.24.3 판정근거

Table 3-204 TE03.15.01 시험결과 판정근거

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

2.24.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.25 TE03.15.02

2.25.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.02	데이터 입력 경로 동작	암호모듈 검사

2.25.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-205 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

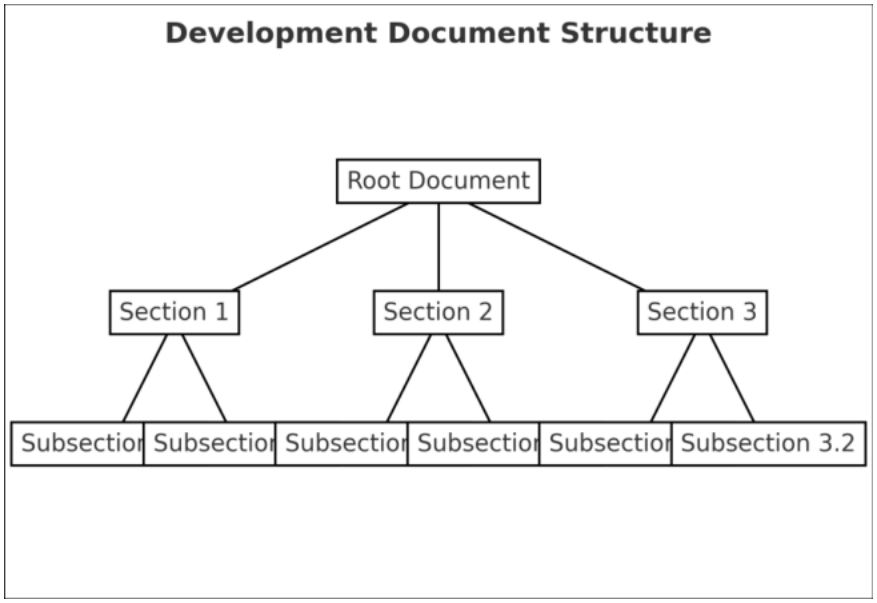


Figure 3-154 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-206 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

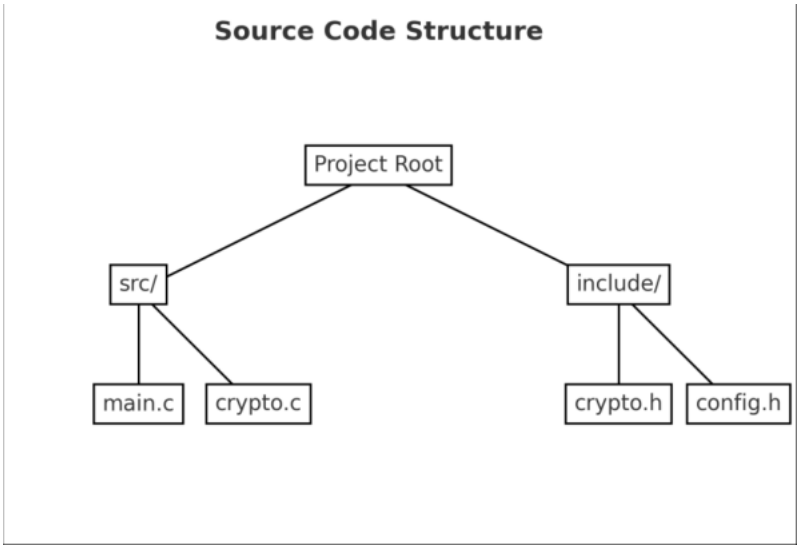


Figure 3-155 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-207 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

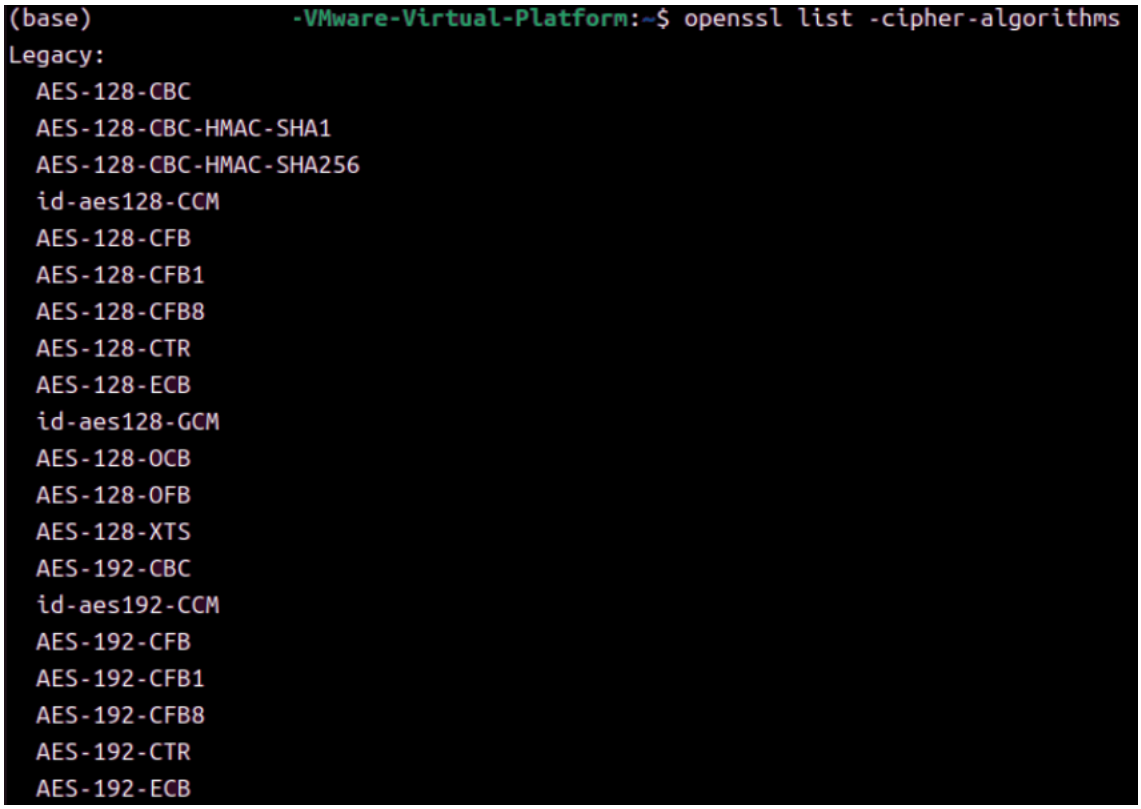


Figure 3-156 그림 제목

2.25.3 판정근거

Table 3-208 TE03.15.02 시험결과 판정근거

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

2.25.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.26 TE03.15.03

2.26.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.03	길이 제한을 포함한 입력 및 제어 정보 형식 확인	개발문서 검토

2.26.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-209 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

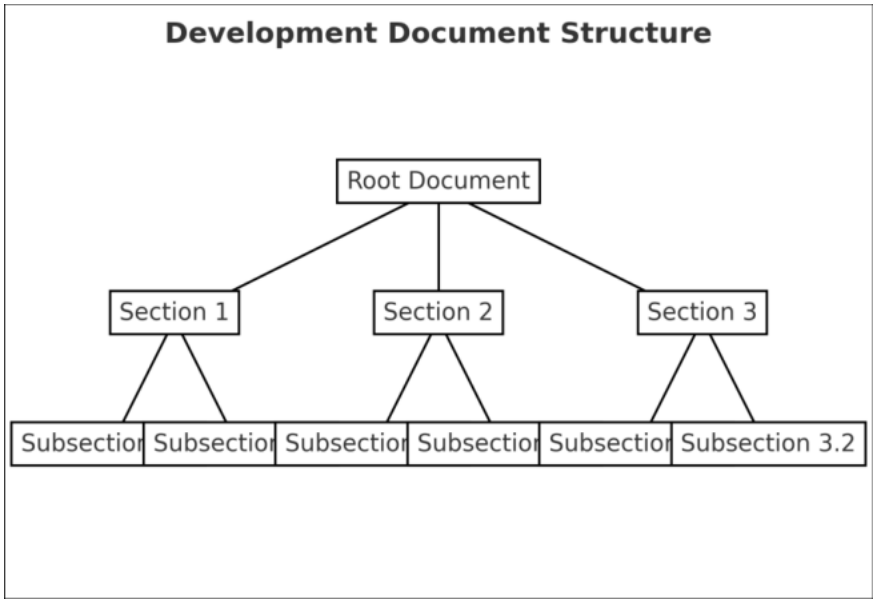


Figure 3-157 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-210 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

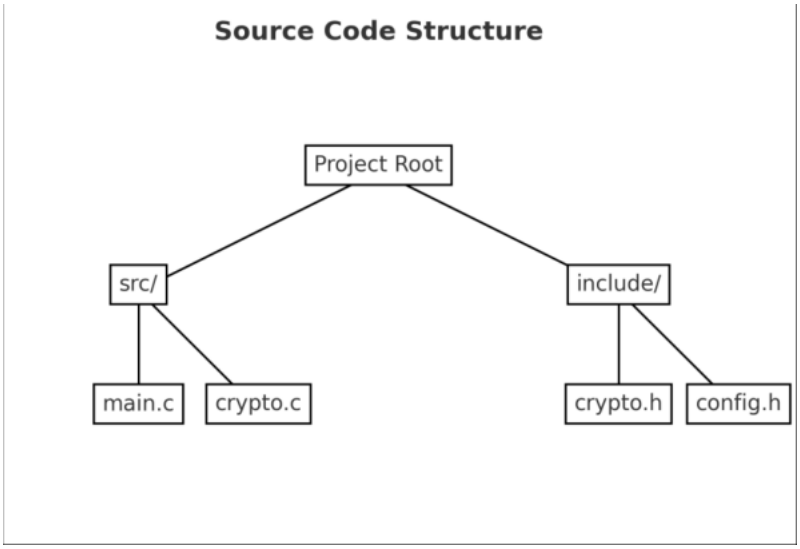


Figure 3-158 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-211 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

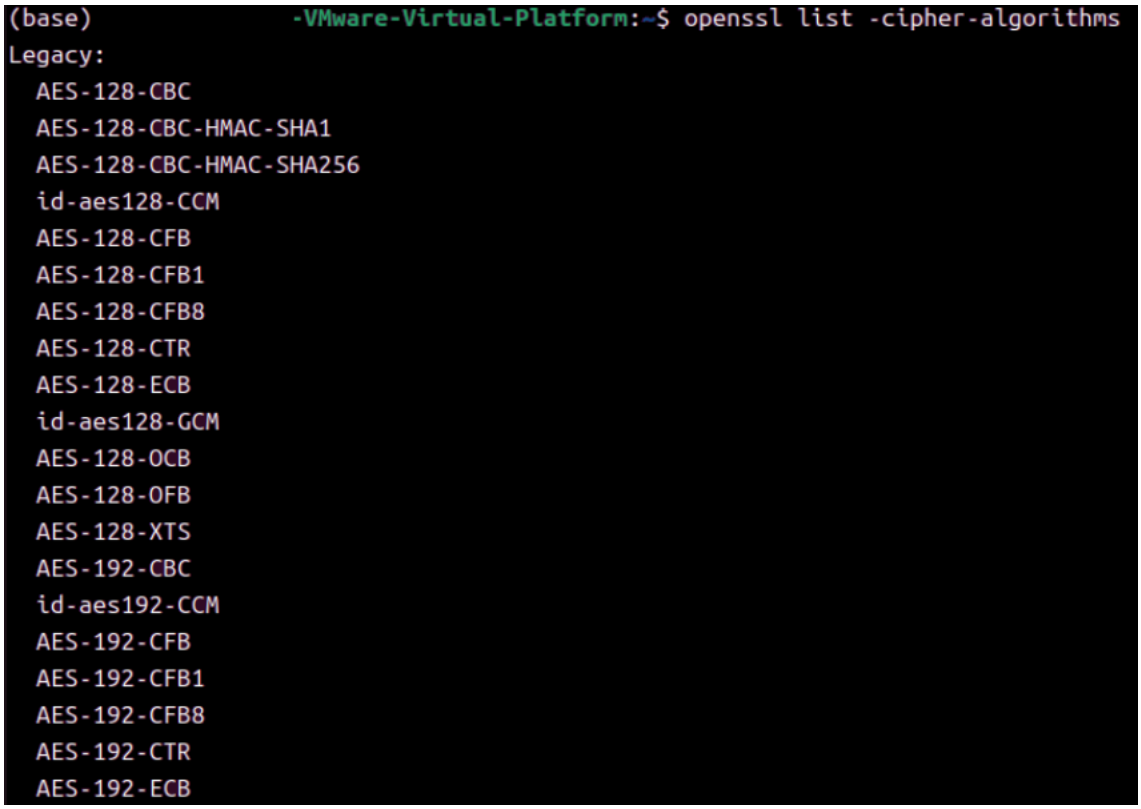


Figure 3-159 그림 제목

2.26.3 판정근거

Table 3-212 TE03.15.03 시험결과 판정근거

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

2.26.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.27 TE03.15.04

2.27.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.04	형식을 검증하는 구성요소의 위치	암호모듈 검사

2.27.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-213 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

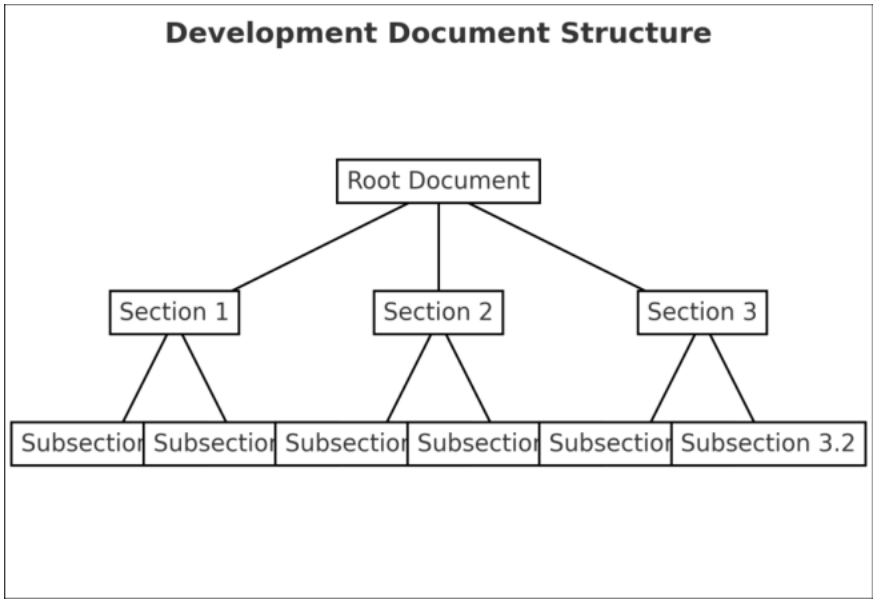


Figure 3-160 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-214 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

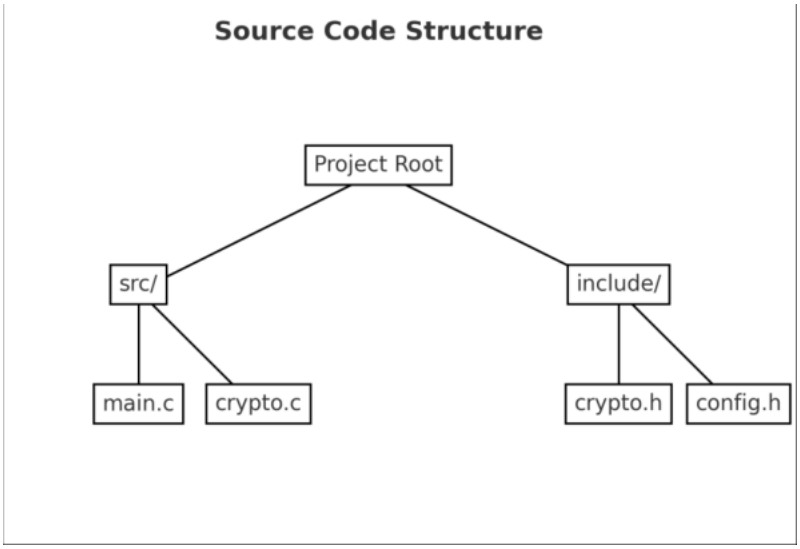


Figure 3-161 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-215 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

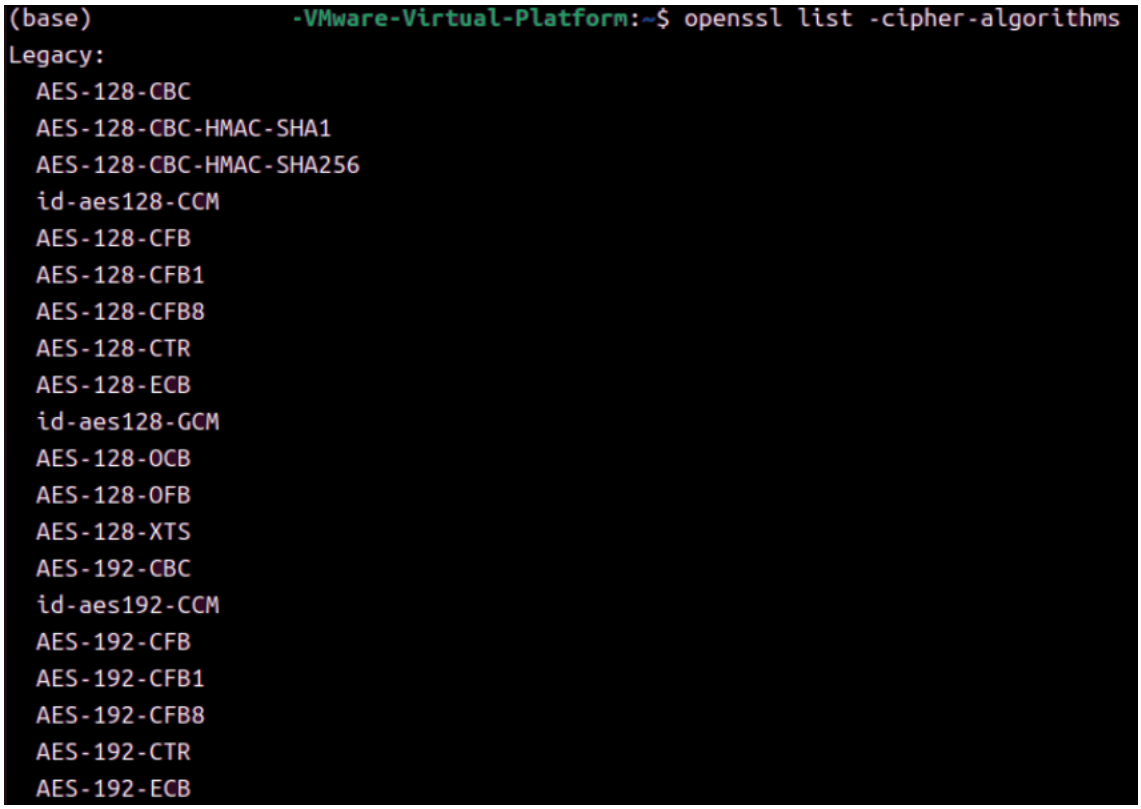


Figure 3-162 그림 제목

2.27.3 판정근거

Table 3-216 TE03.15.04 시험결과 판정근거

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

2.27.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.28 TE03.15.05

2.28.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.05	형식 검증 여부 소스코드 확인	소스코드 검토

2.28.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-217 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

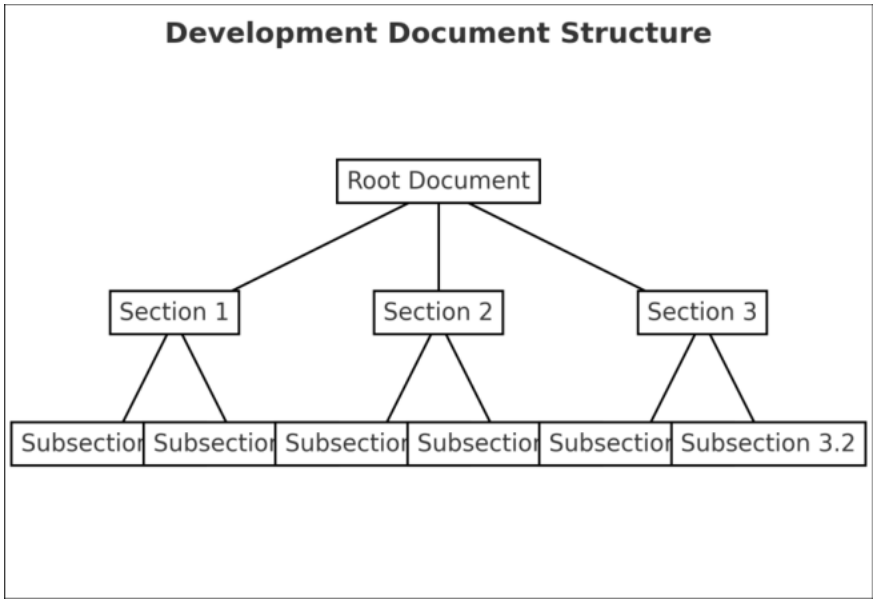


Figure 3-163 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-218 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

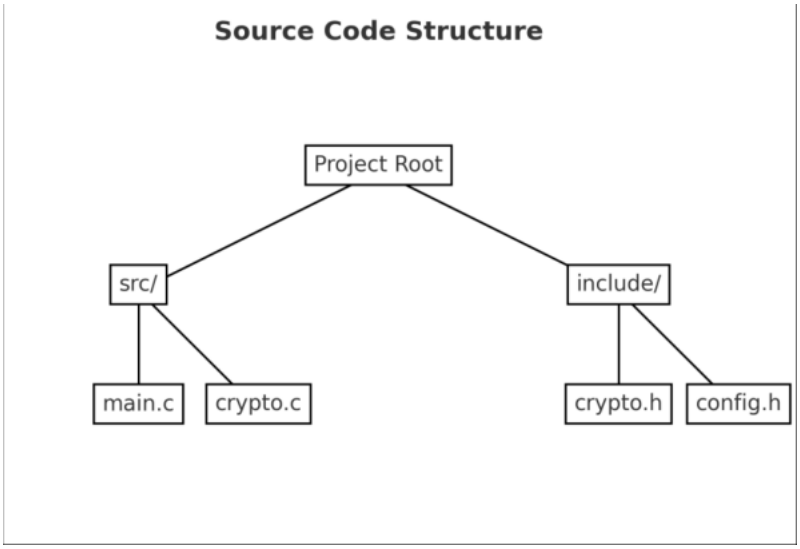


Figure 3-164 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-219 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

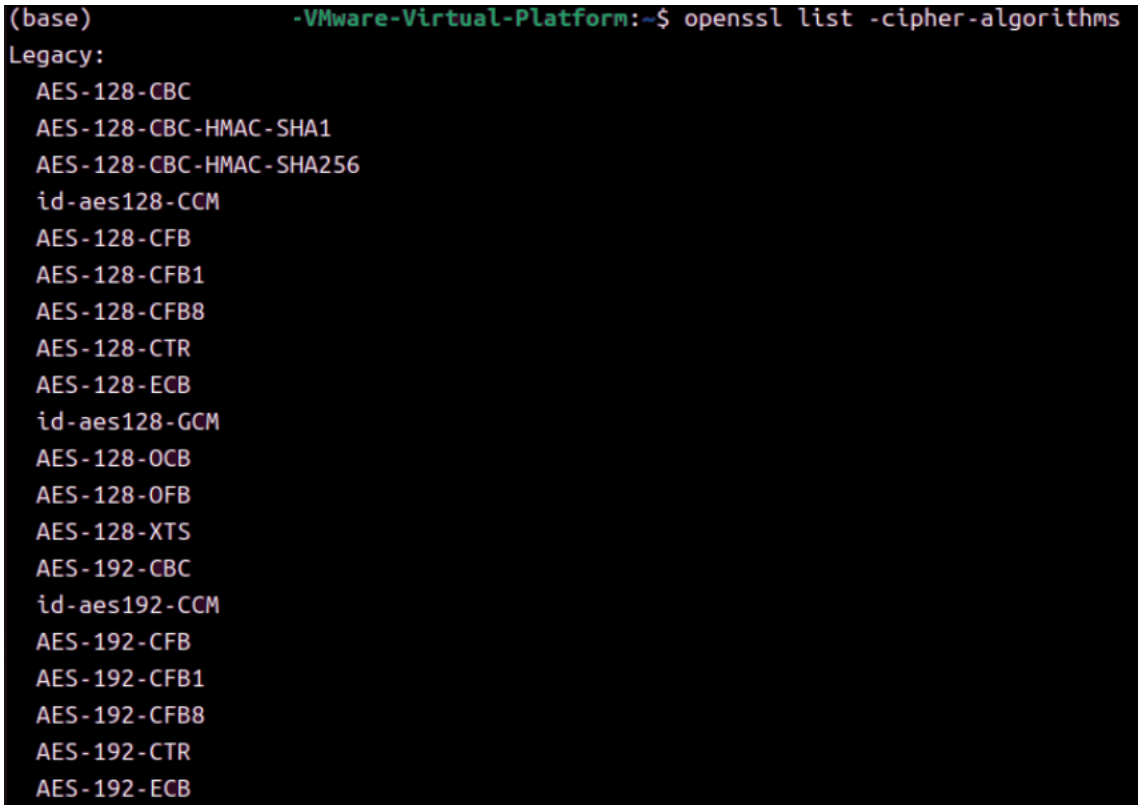


Figure 3-165 그림 제목

2.28.3 판정근거

Table 3-220 TE03.15.05 시험결과 판정근거

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

2.28.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

2.29 TE03.15.06

2.29.1 시험 요구사항

TE	주요 확인사항	확인방법
TE03.15.06	형식과 다른 데이터 및 제어 입력 거절	암호모듈 검사

2.29.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-221 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

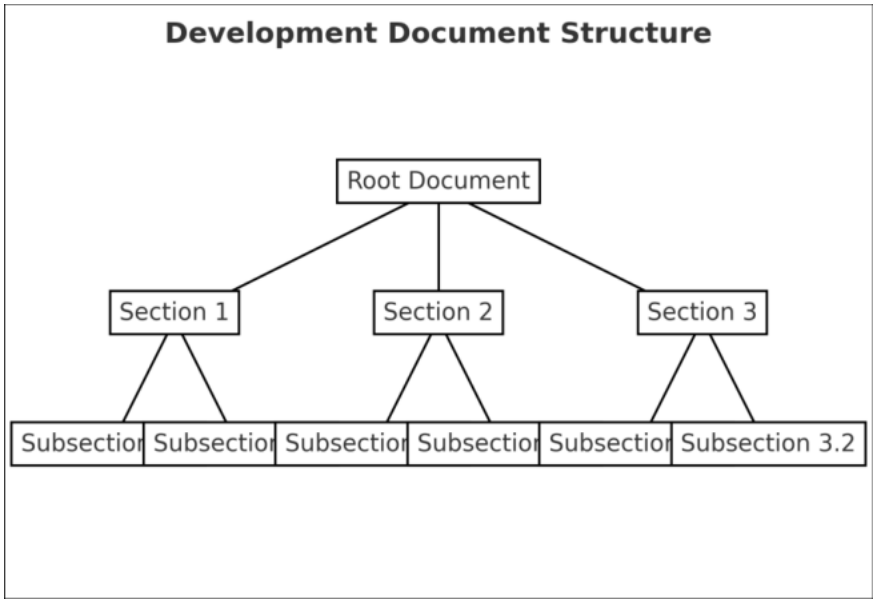


Figure 3-166 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 소스코드 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-222 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

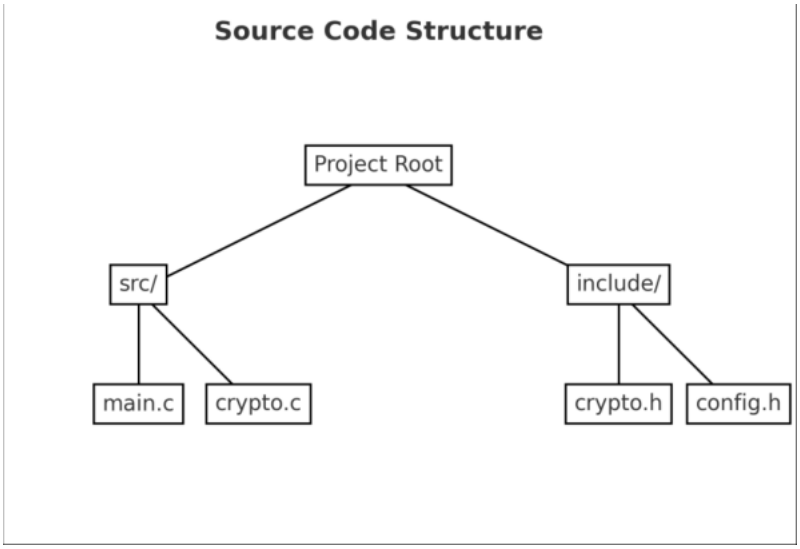


Figure 3-167 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-223 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

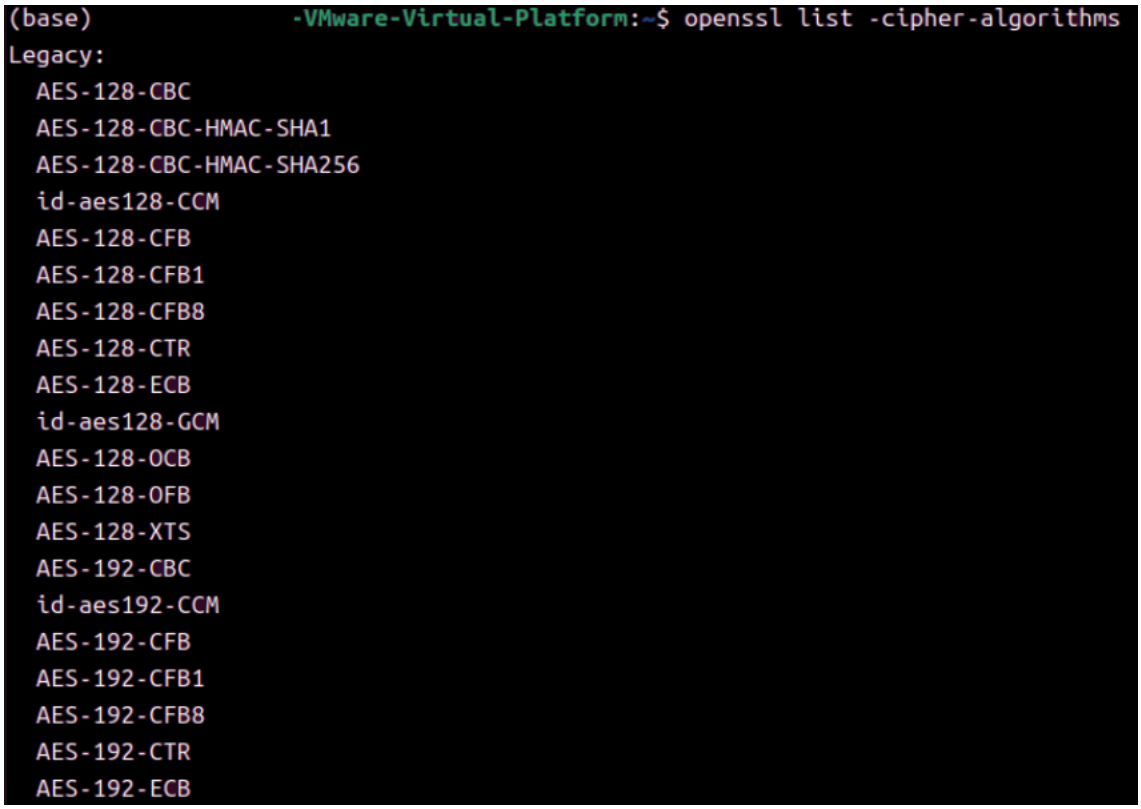


Figure 3-168 그림 제목

2.29.3 판정근거

Table 3-224 TE03.15.06 시험결과 판정근거

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

2.29.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3. 역할 , 서비스 및 인증 (AS04)

□ 암호모듈은 운영자에게 인가된 역할을 지원하고 각 역할에 상응하는 서비스를 제공해야 한다 .

□ 암호모듈은 암호모듈의 역할과 각 역할에 대응하는 서비스 및 보안수준에 따른 인증을 통한 접근 통제가 수행되어야 한다 .

3.1 AS04 시험항목

AS	TE	확인사항
AS04.02	1, 2, 3	복수 운영자 역할 할당
AS04.05	1	암호관리자 역할
AS04.06	1	사용자 역할
AS04.11	1, 2	서비스 입력 및 출력
AS04.13	1, 2, 3	버전 정보 표시
AS04.14	1, 2	상태 표시
AS04.15	1	동작 전 자가시험 수행
AS04.43	1, 2	전원 꺼짐 후 인증 효력
AS04.44	1, 2	인가되지 않은 노출 , 변경 , 대체에 대한 인증 데이터 보호 방법
AS04.56	1, 2	인증 메커니즘 부재 시 운영자의 암묵적 또는 명시적 역할

3.2 TE04.02.01

3.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.02.01	복수 운영자에 의해 실행되는 역할과 서비스 분리	개발문서 검토

3.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-225 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

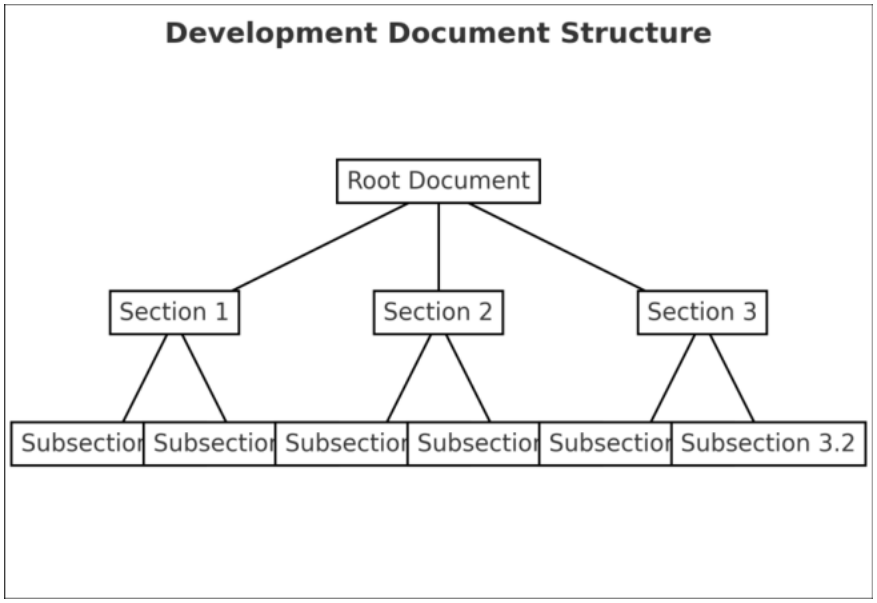


Figure 3-169 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-226 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

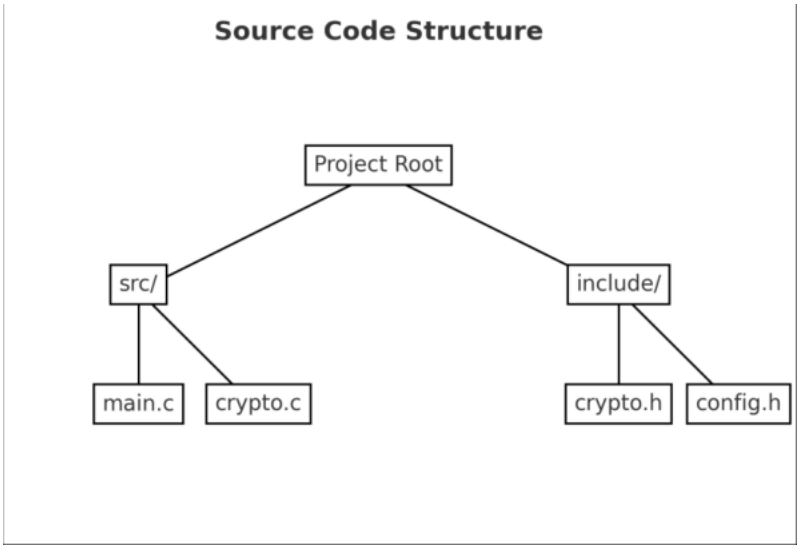


Figure 3-170 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-227 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

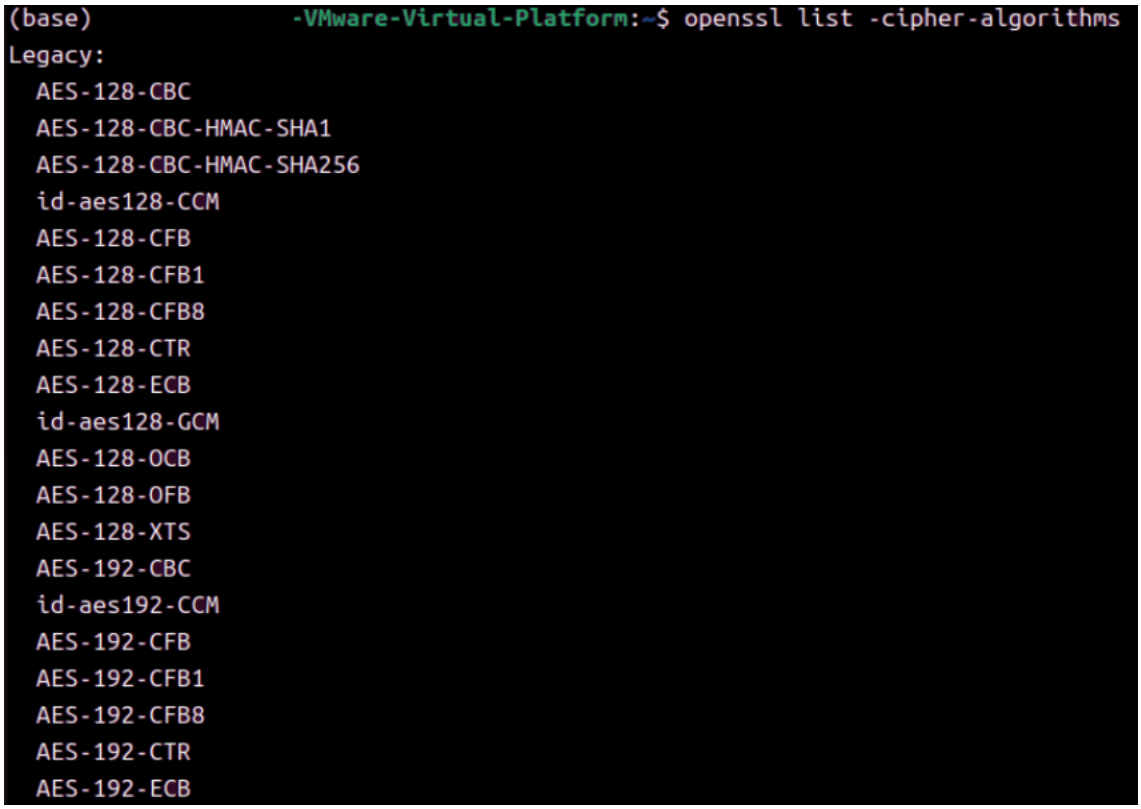


Figure 3-171 그림 제목

3.2.3 판정근거

Table 3-228 TE04.02.01 시험결과 판정근거

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

3.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.3 TE04.02.02

3.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.02.02	역할별 서비스 실행 및 운영자별 역할과 서비스 분리	암호모듈 검사

3.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-229 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

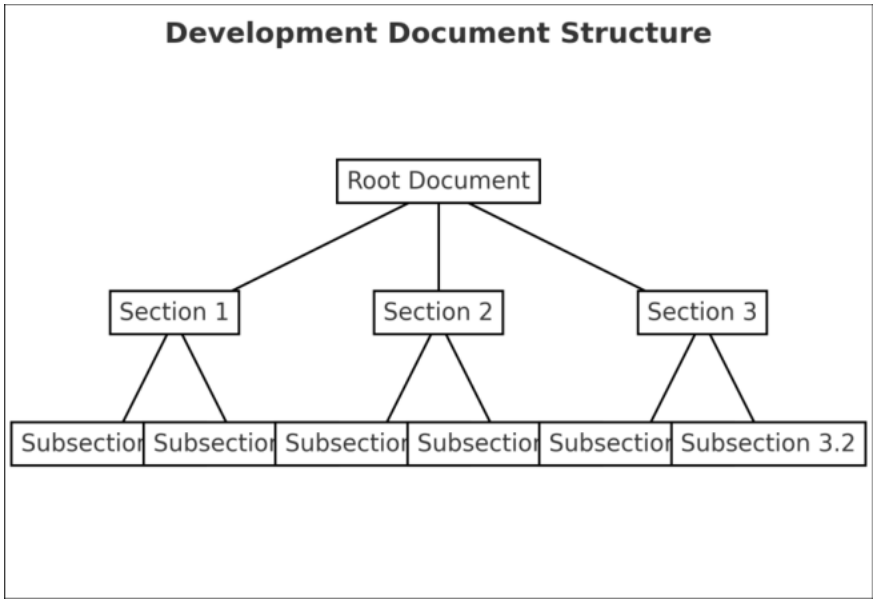


Figure 3-172 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-230 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

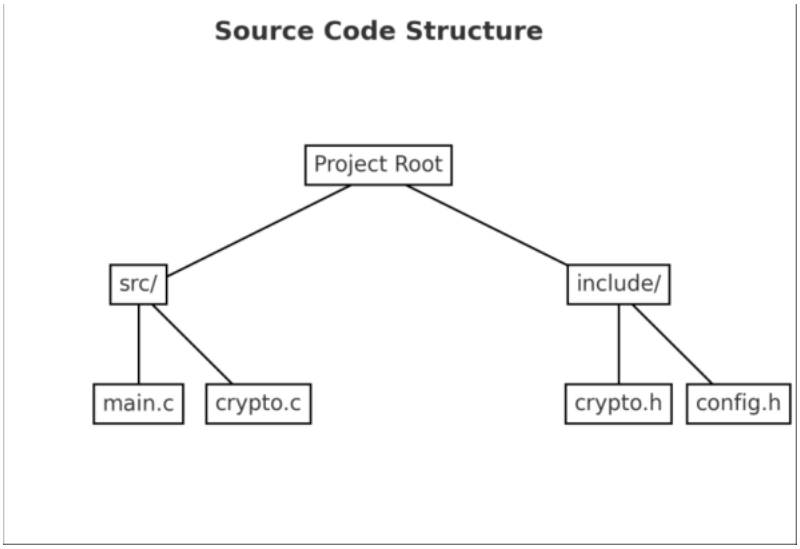


Figure 3-173 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-231 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

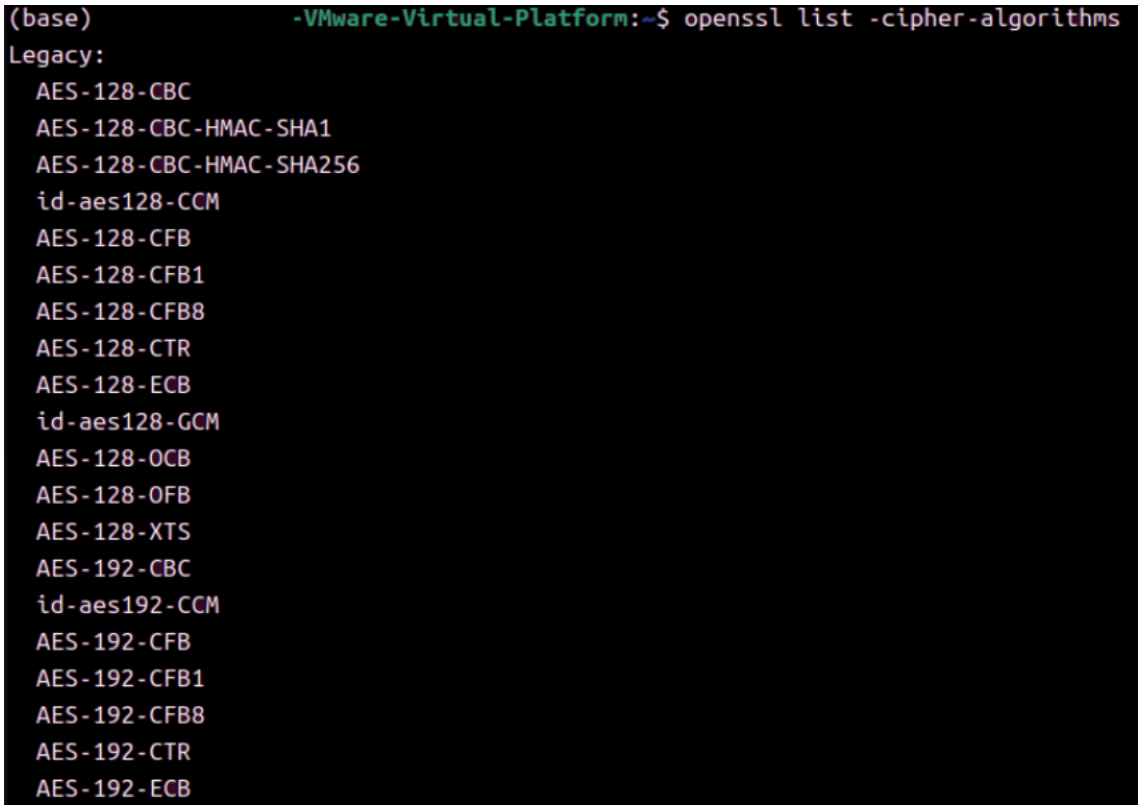


Figure 3-174 그림 제목

3.3.3 판정근거

Table 3-232 TE04.02.02 시험결과 판정근거

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

3.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.4 TE04.02.03

3.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.02.03	복수 운영자 역할 위반에 대한 제한 조치 수행	암호모듈 검사

3.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-233 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

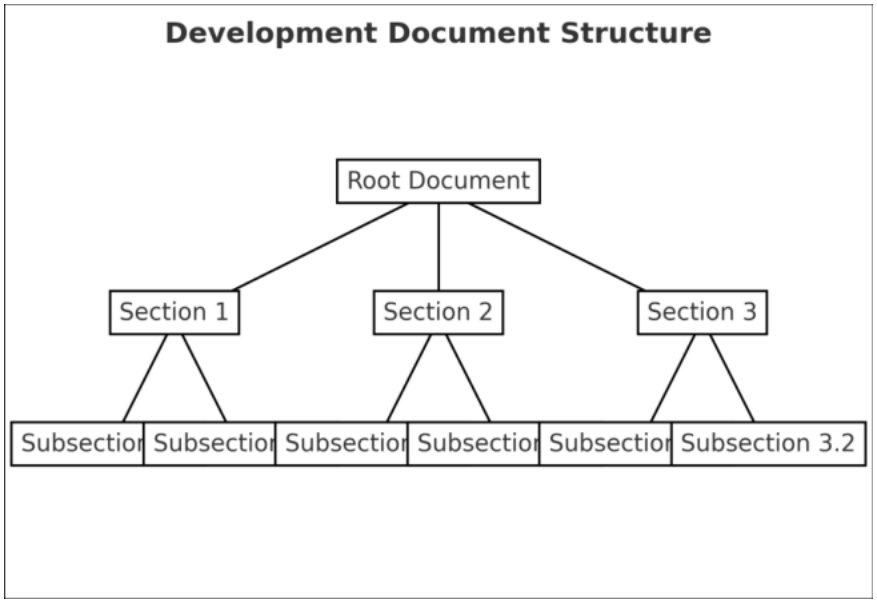


Figure 3-175 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-234 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

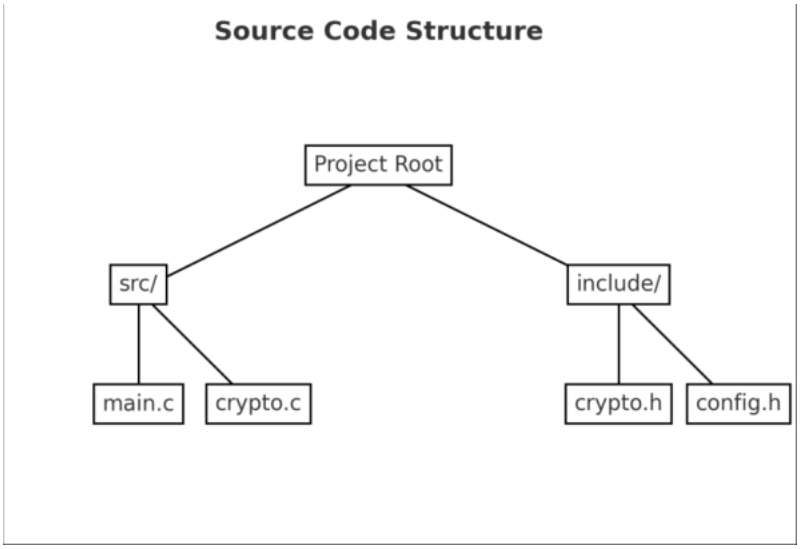


Figure 3-176 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-235 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

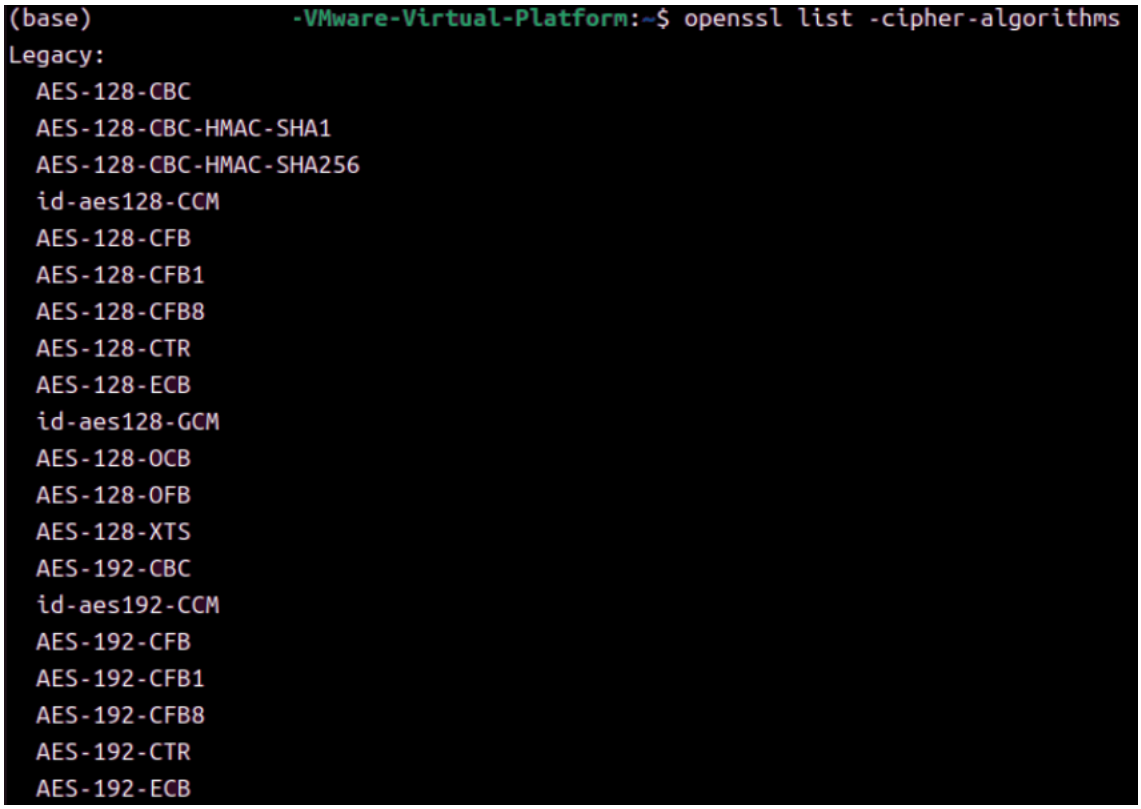


Figure 3-177 그림 제목

3.4.3 판정근거

Table 3-236 TE04.02.03 시험결과 판정근거

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

3.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.5 TE04.05.01

3.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.05.01	암호 관리자 역할 정의 및 서비스	개발문서 검토

3.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-237 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

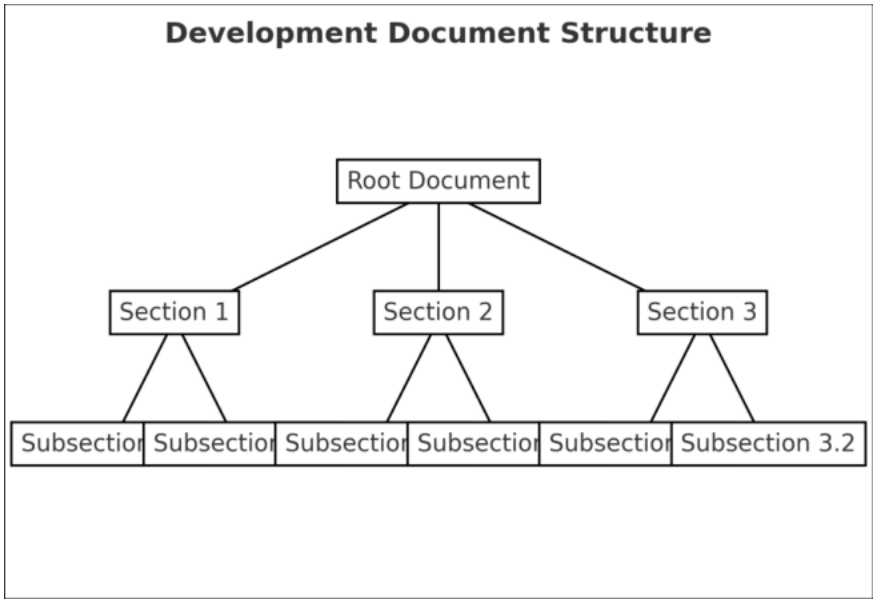


Figure 3-178 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-238 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

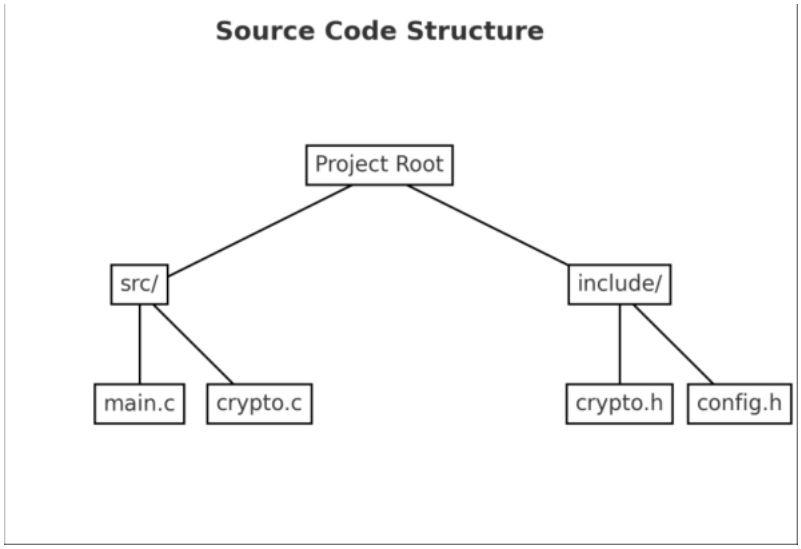


Figure 3-179 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-239 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

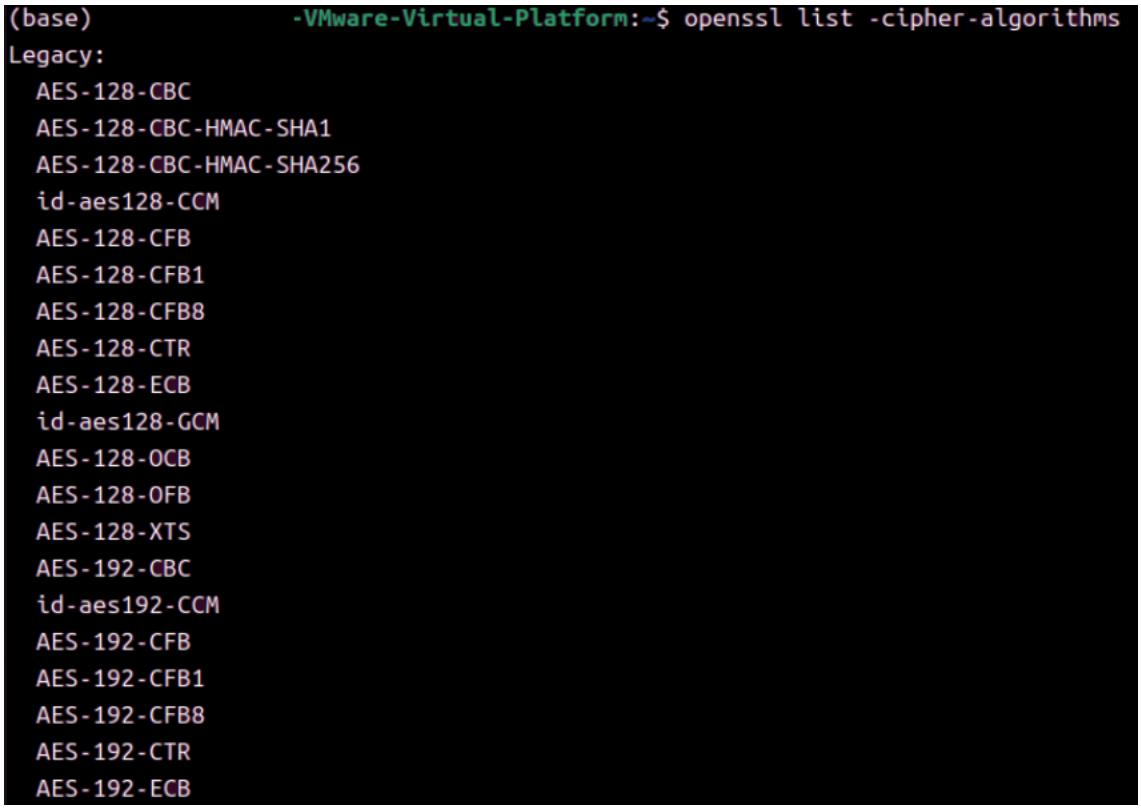


Figure 3-180 그림 제목

3.5.3 판정근거

Table 3-240 TE04.05.01 시험결과 판정근거

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

3.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.6 TE04.06.01

3.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.06.01	사용자 역할 정의 및 서비스	개발문서 검토

3.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-241 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

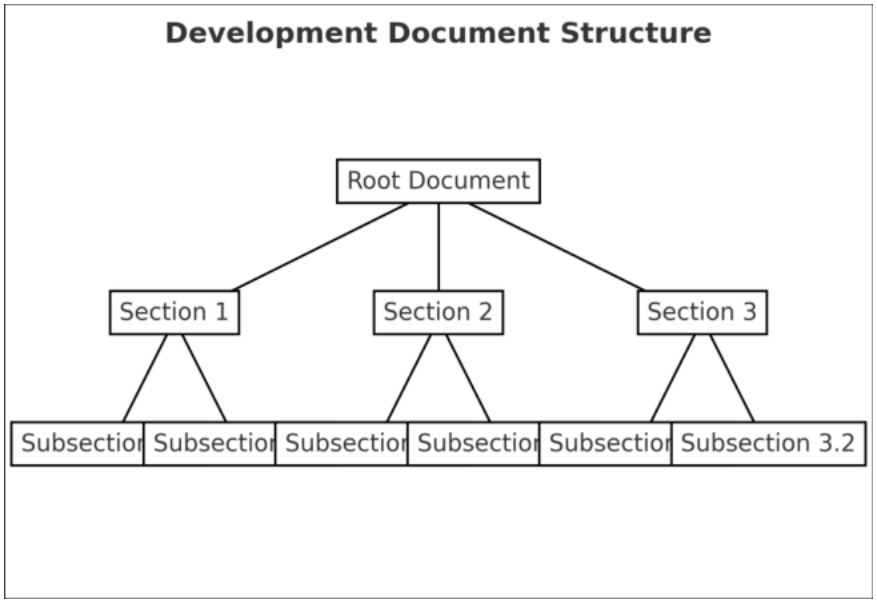


Figure 3-181 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-242 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

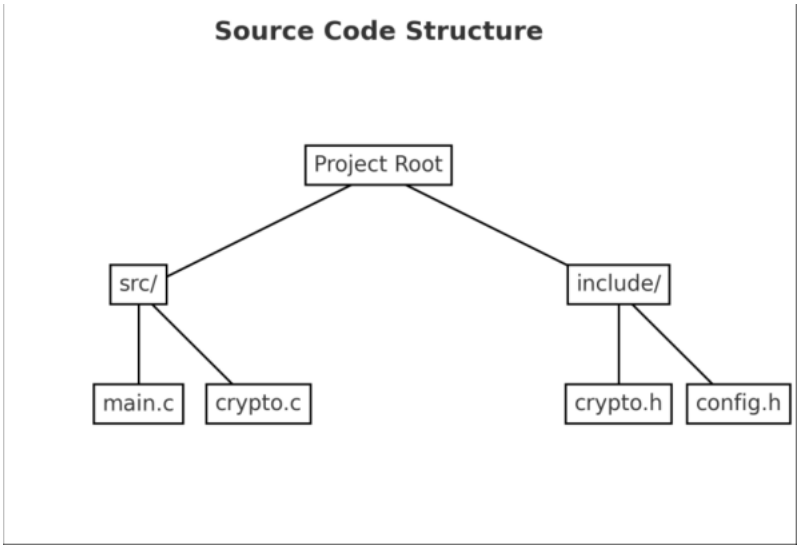


Figure 3-182 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-243 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

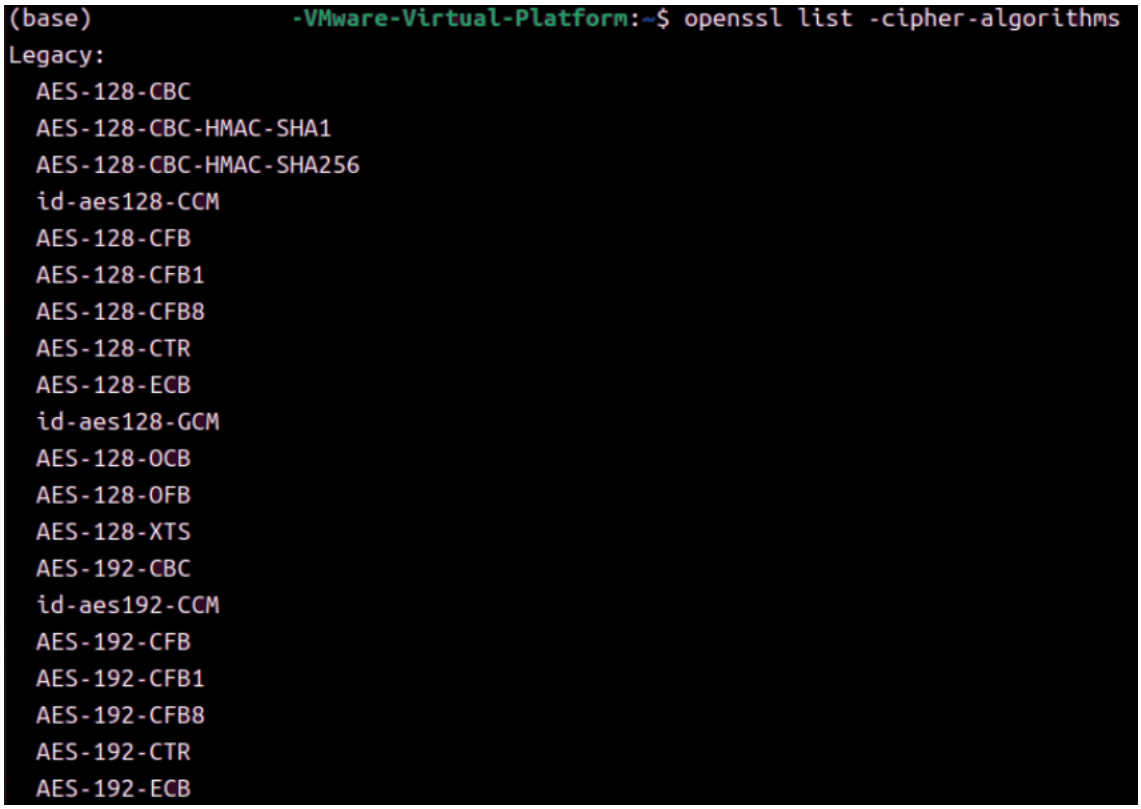


Figure 3-183 그림 제목

3.6.3 판정근거

Table 3-244 TE04.06.01 시험결과 판정근거

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

3.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.7 TE04.11.01

3.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.11.01	서비스 입력 , 출력 및 인가된 역할	개발문서 검토

3.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-245 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

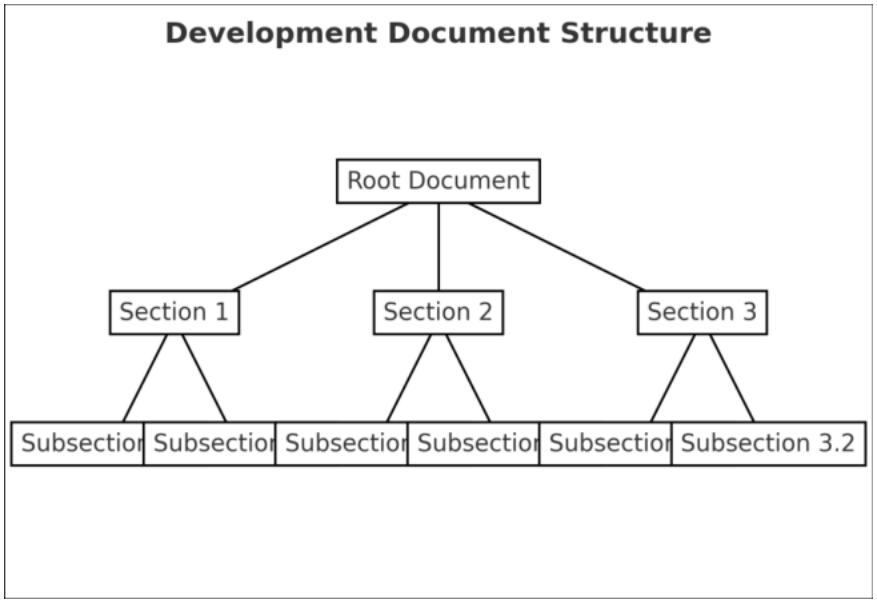


Figure 3-184 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-246 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

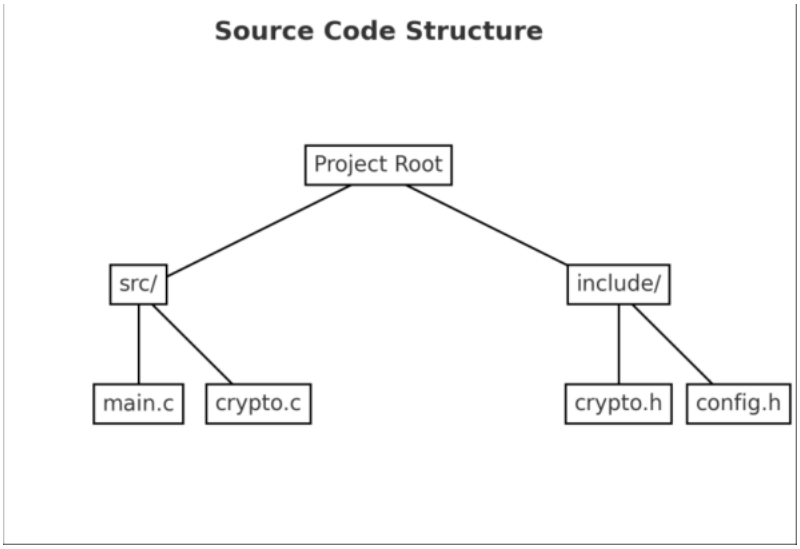


Figure 3-185 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-247 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

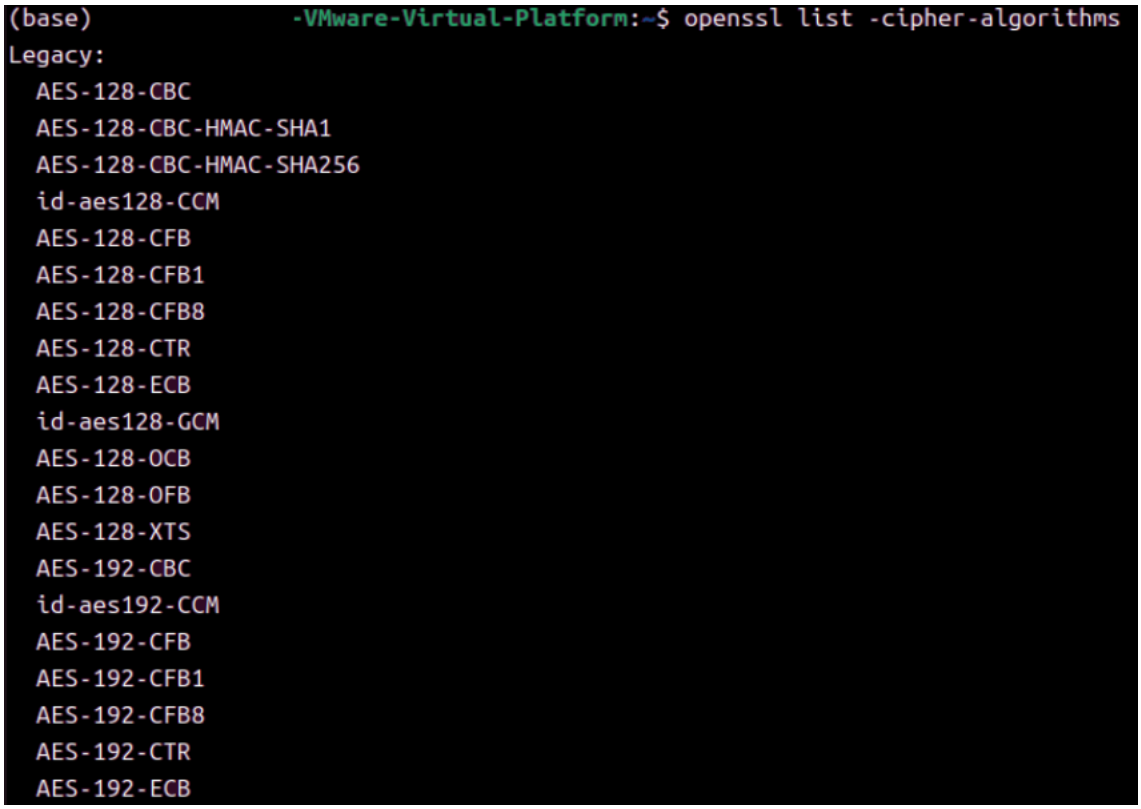


Figure 3-186 그림 제목

3.7.3 판정근거

Table 3-248 TE04.11.01 시험결과 판정근거

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

3.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.8 TE04.11.02

3.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.11.02	서비스 입력 , 출력 및 인가된 역할에 대한 동작	암호모듈 검사

3.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-249 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

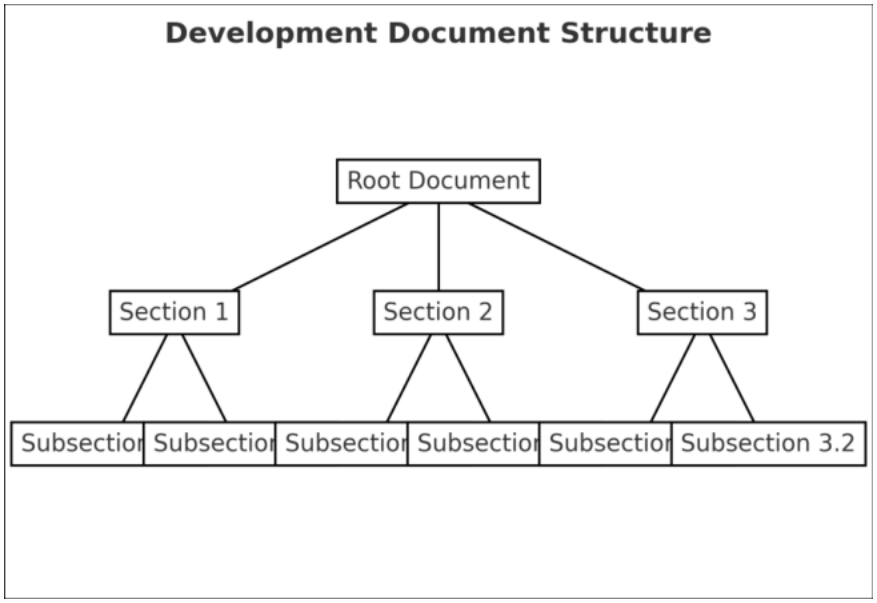


Figure 3-187 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-250 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

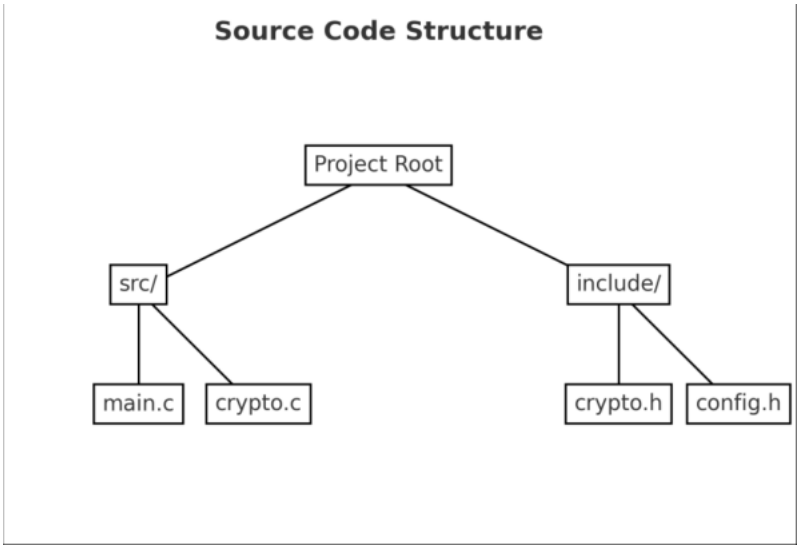


Figure 3-188 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-251 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

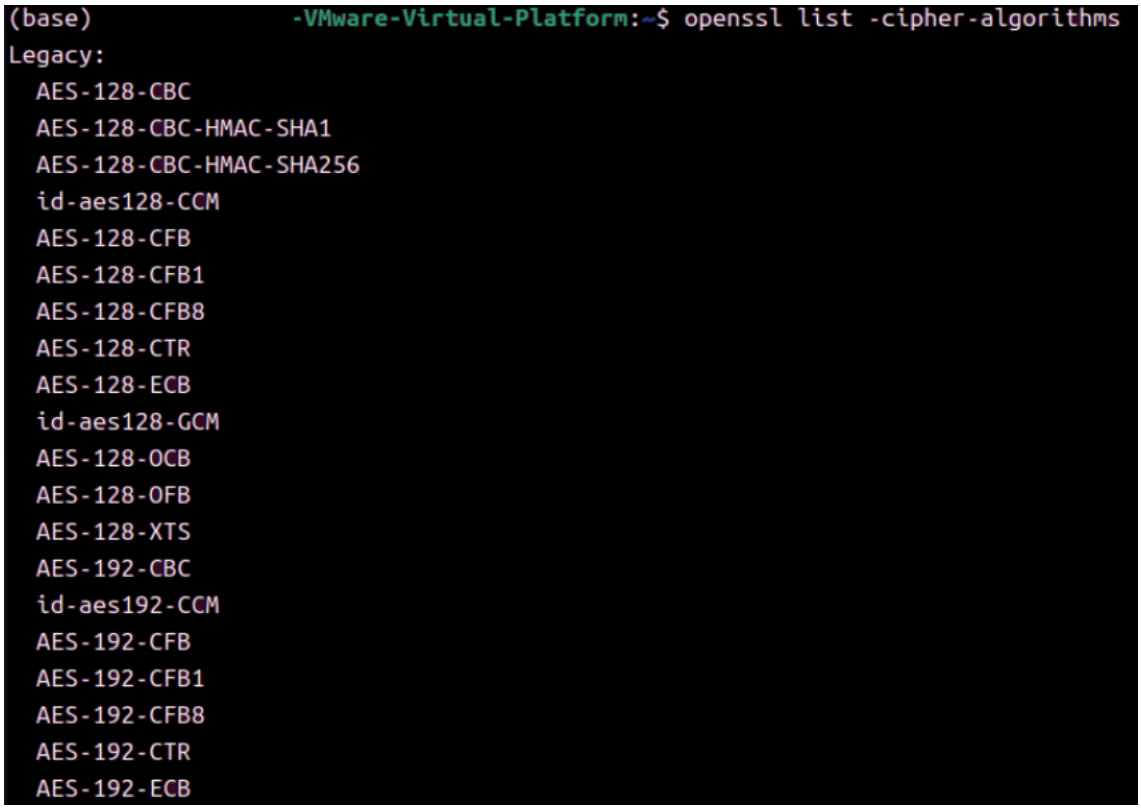


Figure 3-189 그림 제목

3.8.3 판정근거

Table 3-252 TE04.11.02 시험결과 판정근거

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

3.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.9 TE04.13.01

3.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.13.01	암호모듈 명칭 , 식별자 , 버전 정보 제공	암호모듈 검사

3.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-253 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

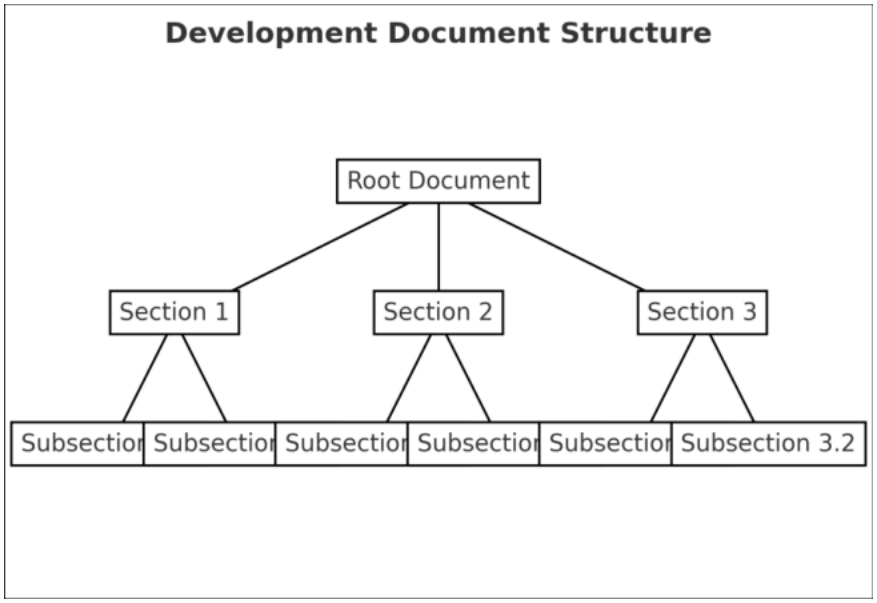


Figure 3-190 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-254 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

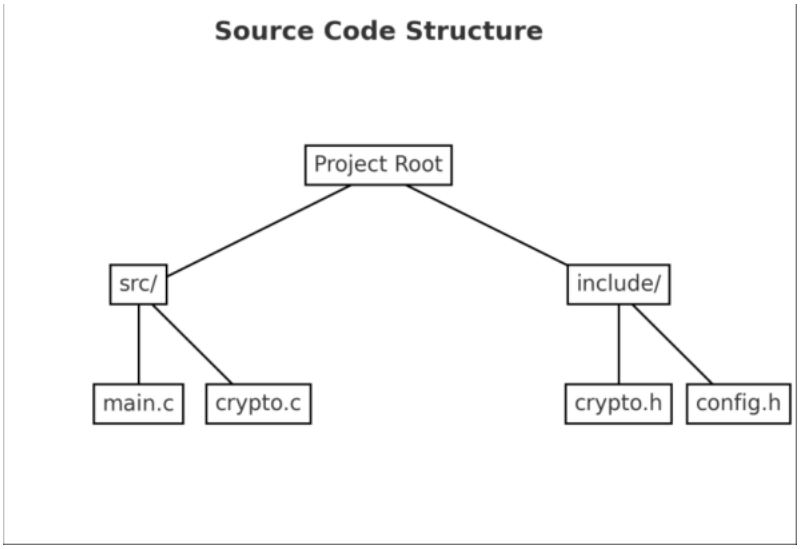


Figure 3-191 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-255 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

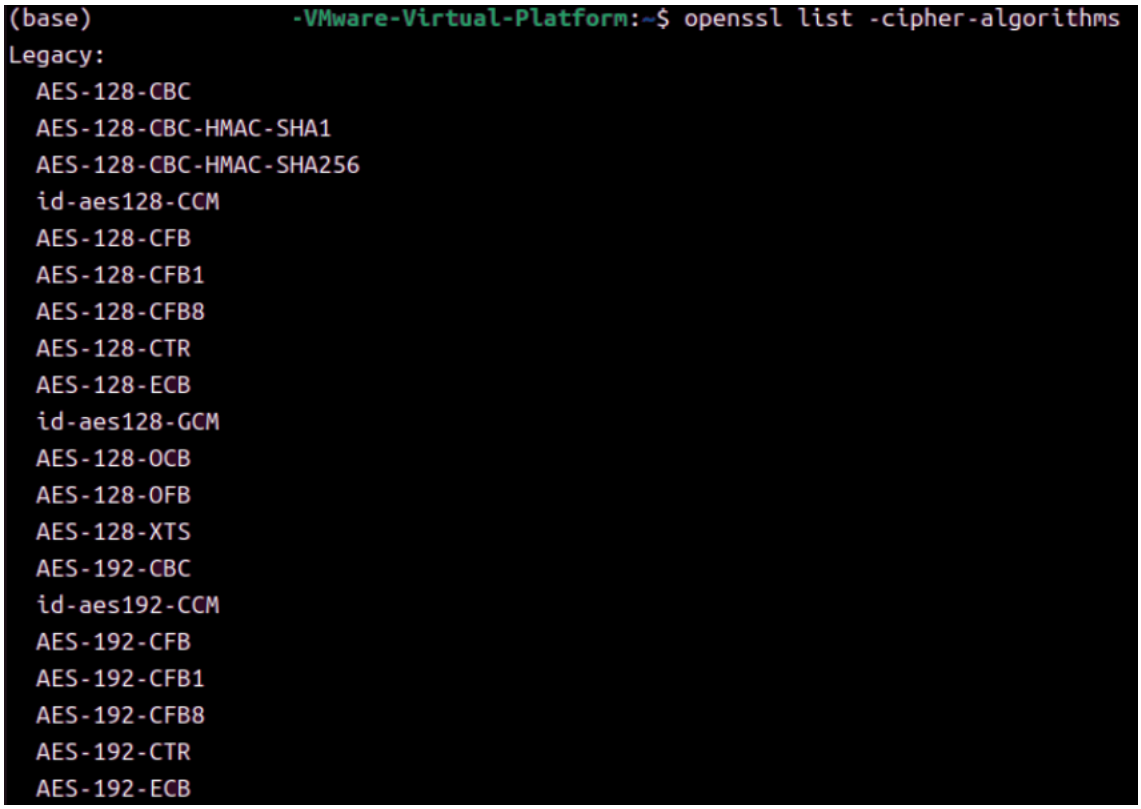


Figure 3-192 그림 제목

3.9.3 판정근거

Table 3-256 TE04.13.0 시험결과 판정근거

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

3.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.10 TE04.13.02

3.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.13.02	보안정책문서에 모듈 정보 제공	개발문서 검토

3.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-257 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

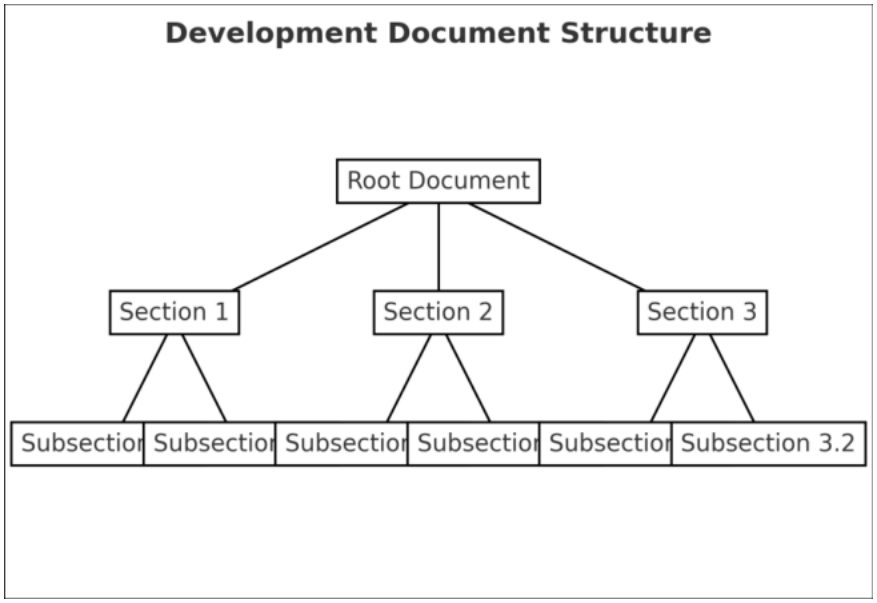


Figure 3-193 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-258 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

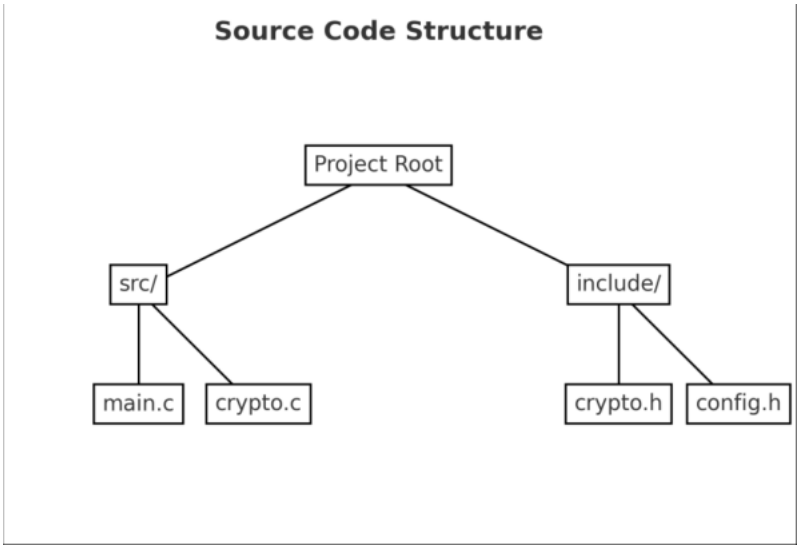


Figure 3-194 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-259 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

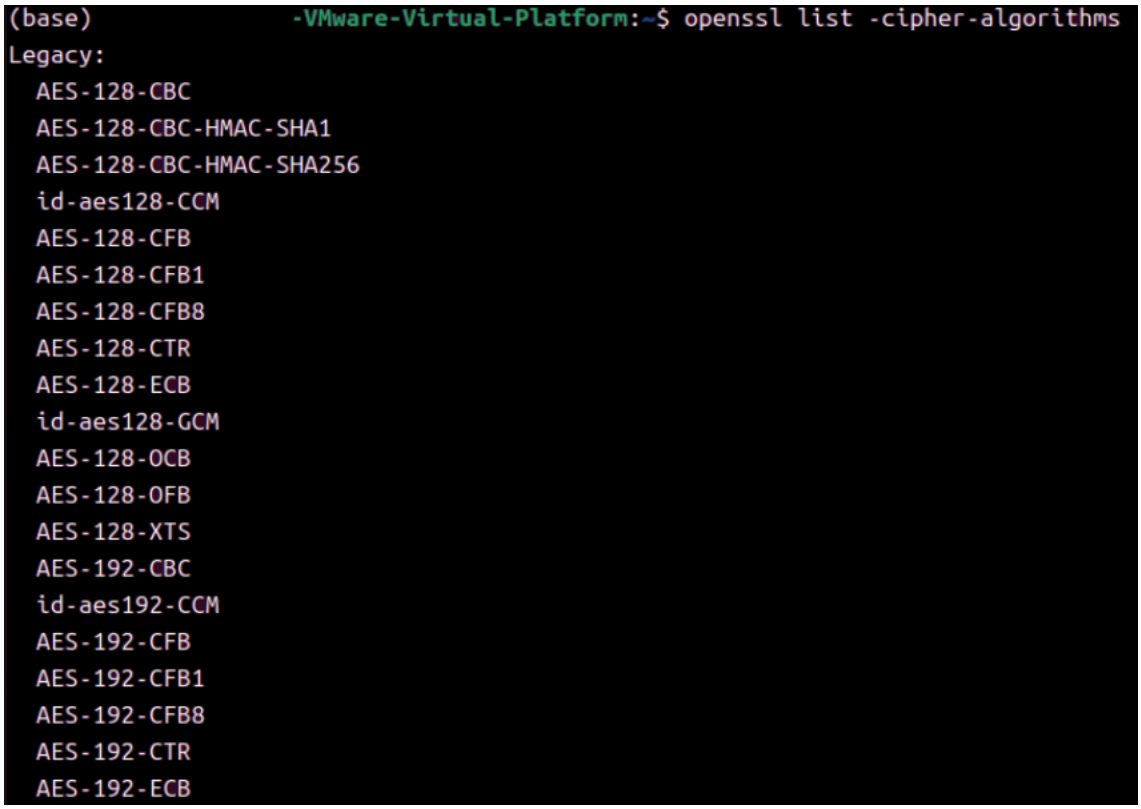


Figure 3-195 그림 제목

3.10.3 판정근거

Table 3-260 TE04.13.02 시험결과 판정근거

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

3.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.11 TE04.13.03

3.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.13.03	보안정책문서의 모듈 정보와 검증 목록 연관	개발문서 검토

3.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-261 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

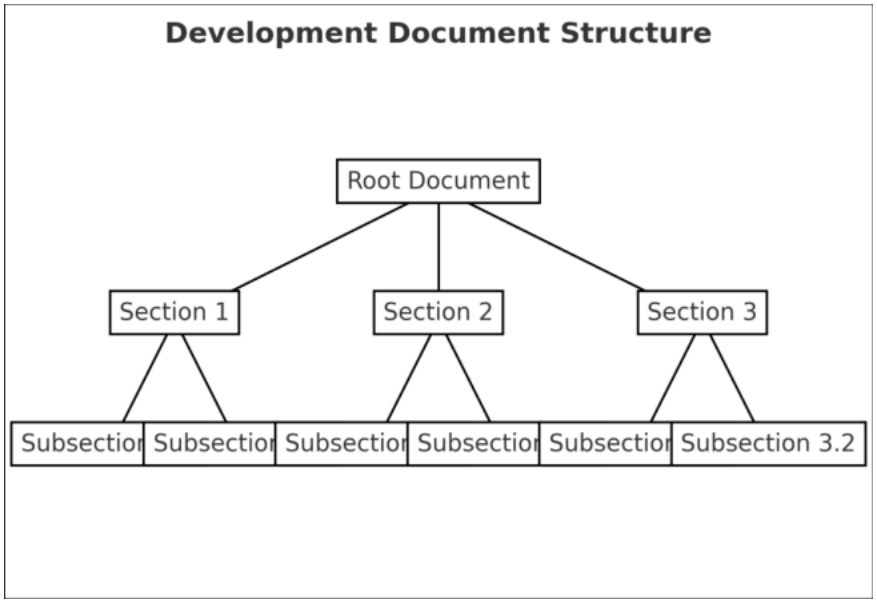


Figure 3-196 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-262 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

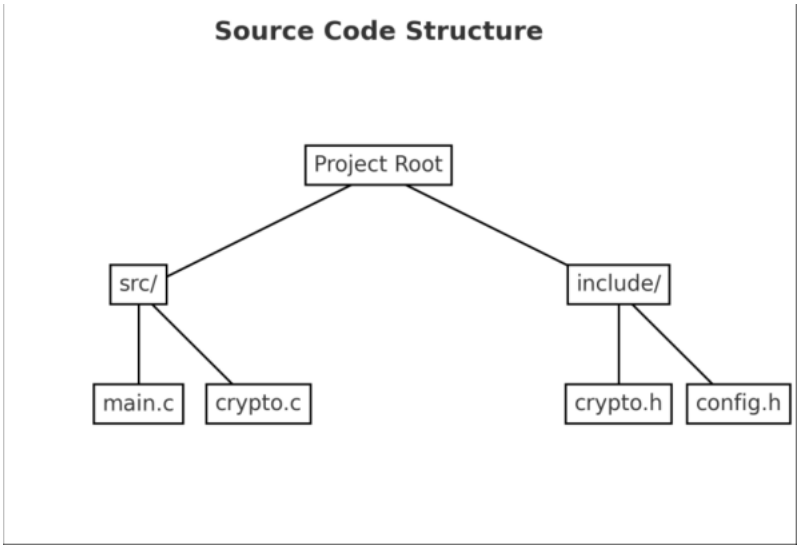


Figure 3-197 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-263 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

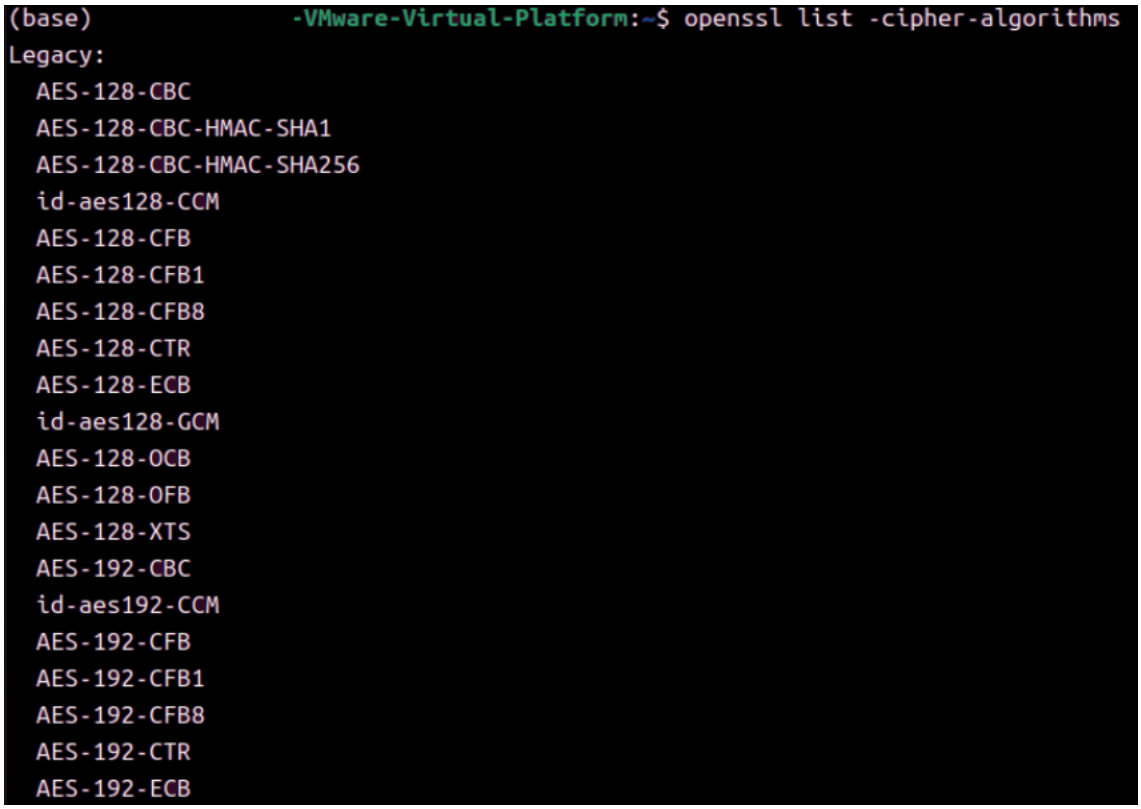


Figure 3-198 그림 제목

3.11.3 판정근거

Table 3-264 TE04.13.03 시험결과 판정근거

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

3.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.12 TE04.13.03

3.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.13.03	보안정책문서의 모듈 정보와 검증 목록 연관	개발문서 검토

3.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-265 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

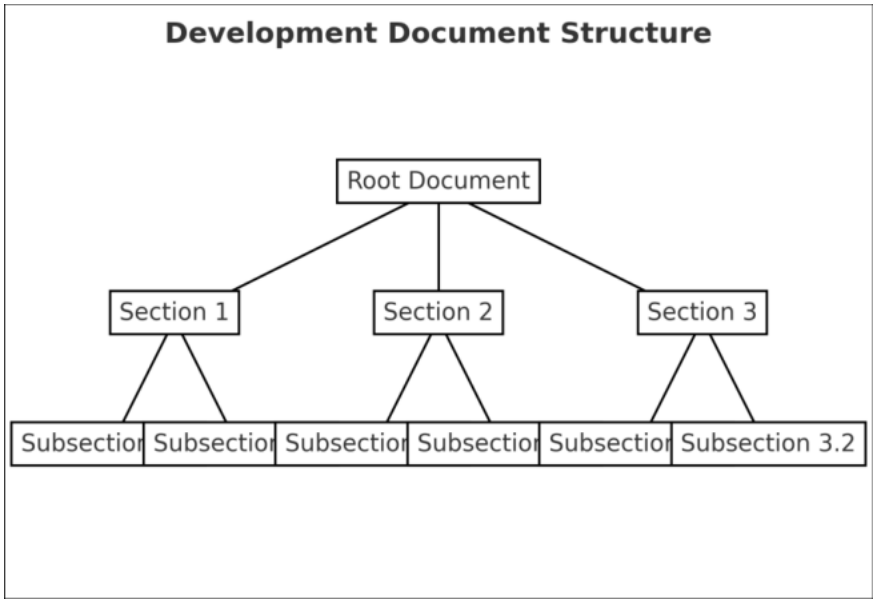


Figure 3-199 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-266 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

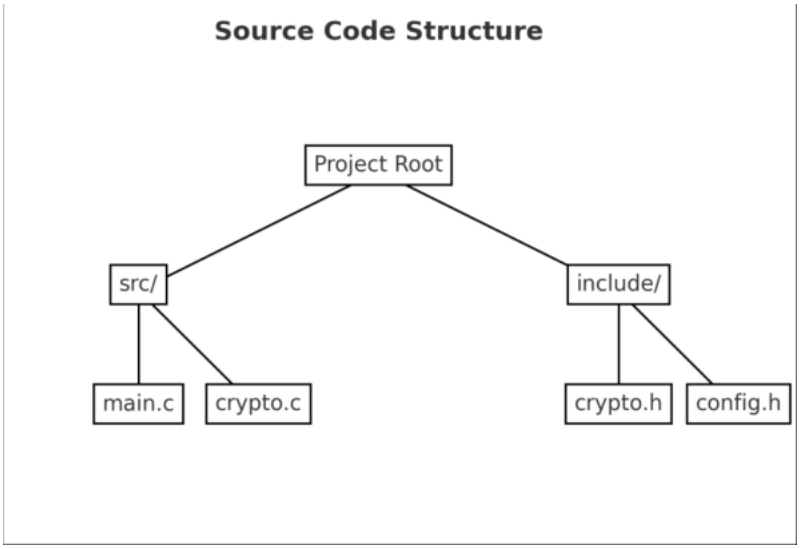


Figure 3-200 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-267 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

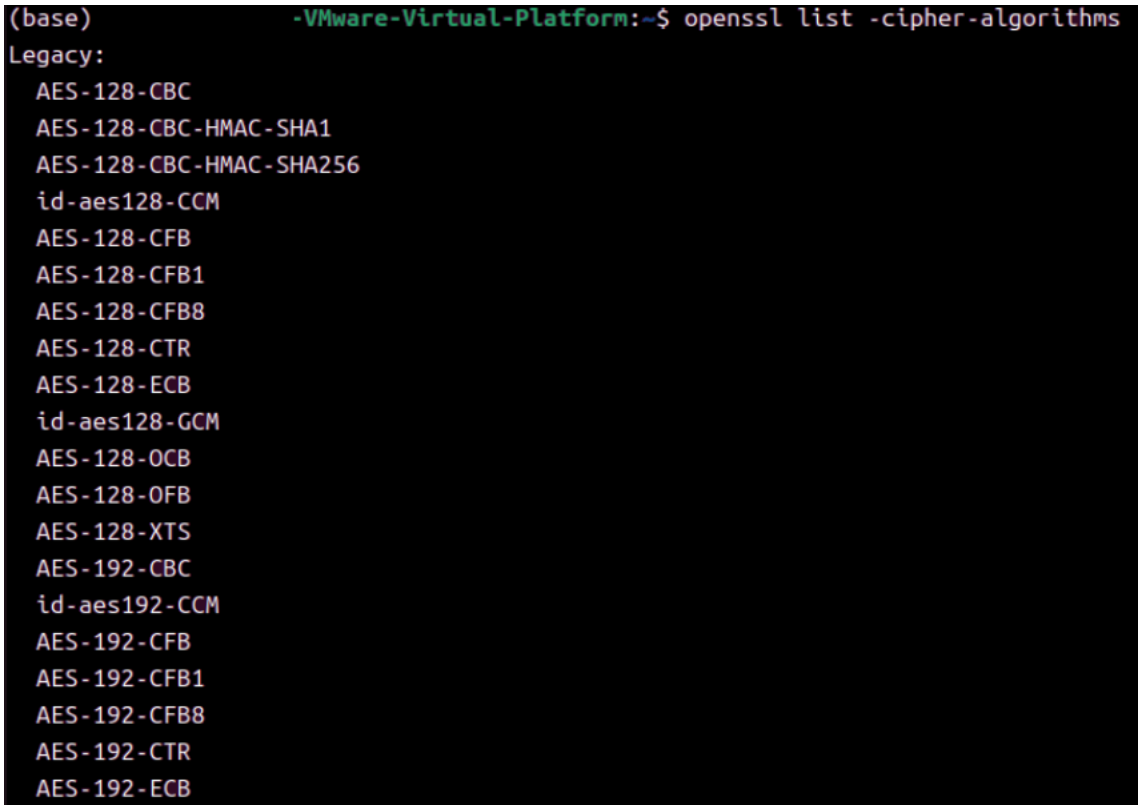


Figure 3-201 그림 제목

3.12.3 판정근거

Table 3-268 TE04.13.03 시험결과 판정근거

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

3.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.13 TE04.14.01

3.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.14.01	보안정책 상태 표시 서비스 및 인가된 역할	개발문서 검토

3.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-269 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

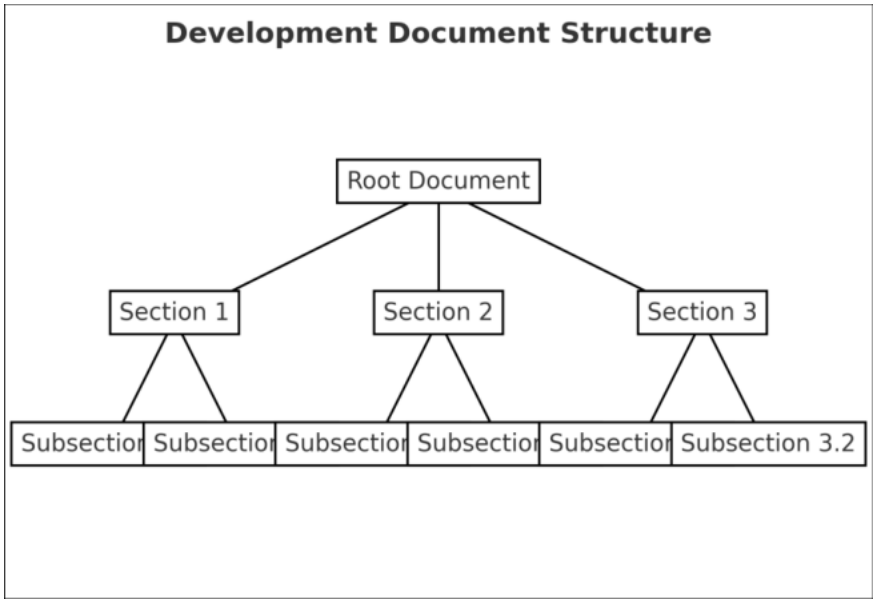


Figure 3-202 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-270 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

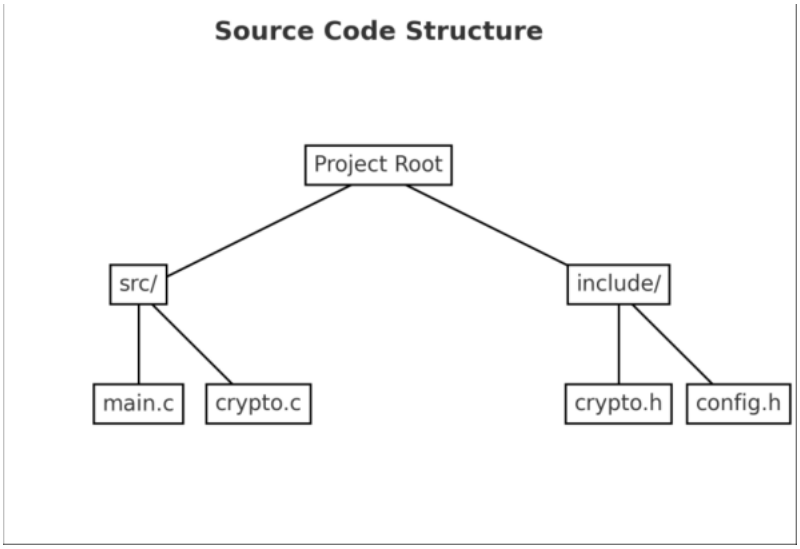


Figure 3-203 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-271 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

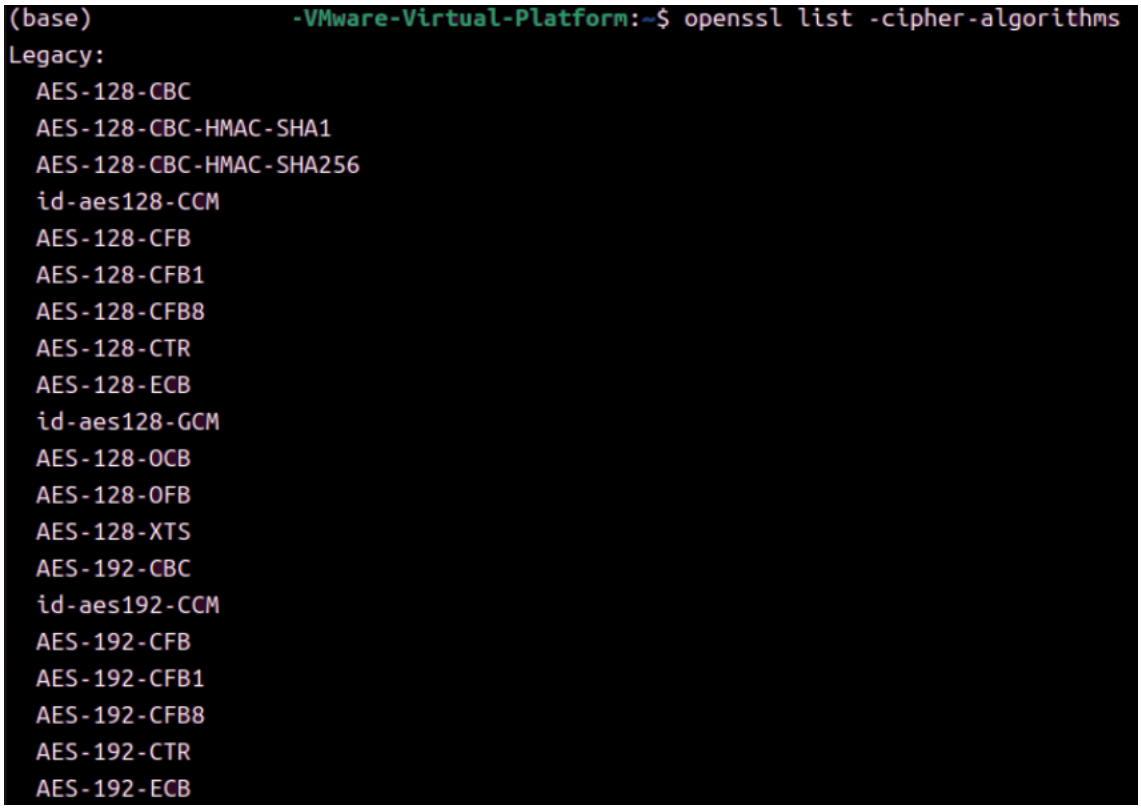


Figure 3-204 그림 제목

3.13.3 판정근거

Table 3-272 TE04.14.01 시험결과 판정근거

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

3.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.14 TE04.14.02

3.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.14.02	개발문서와 상태 표시 일치 여부	암호모듈 검사

3.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-273 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

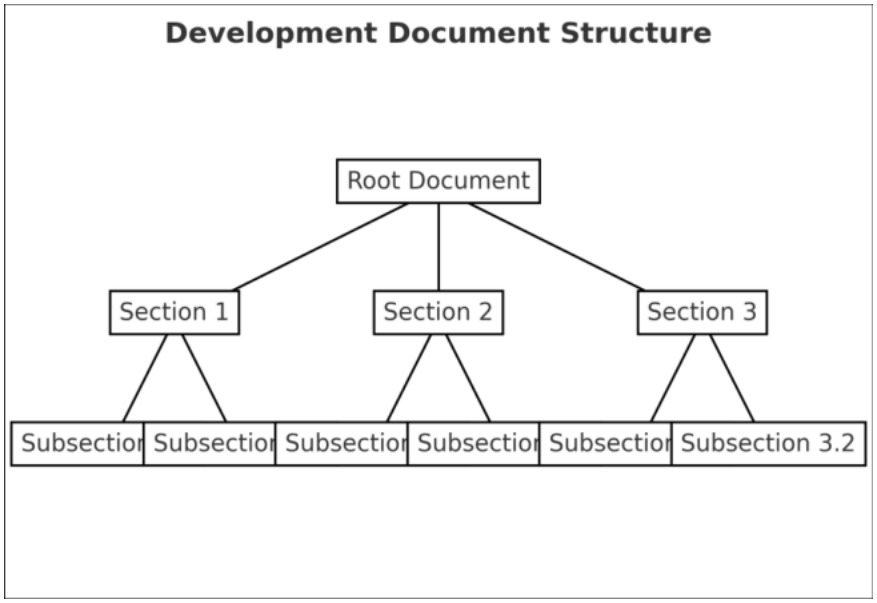


Figure 3-205 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-274 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

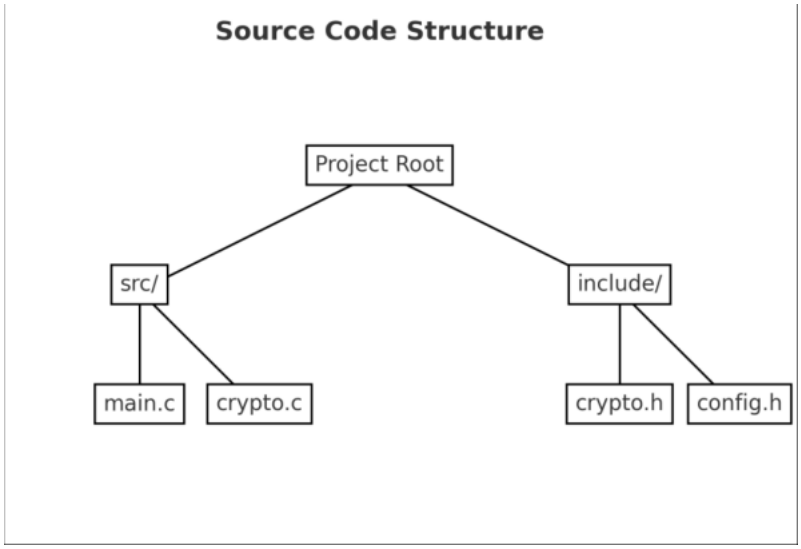


Figure 3-206 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-275 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

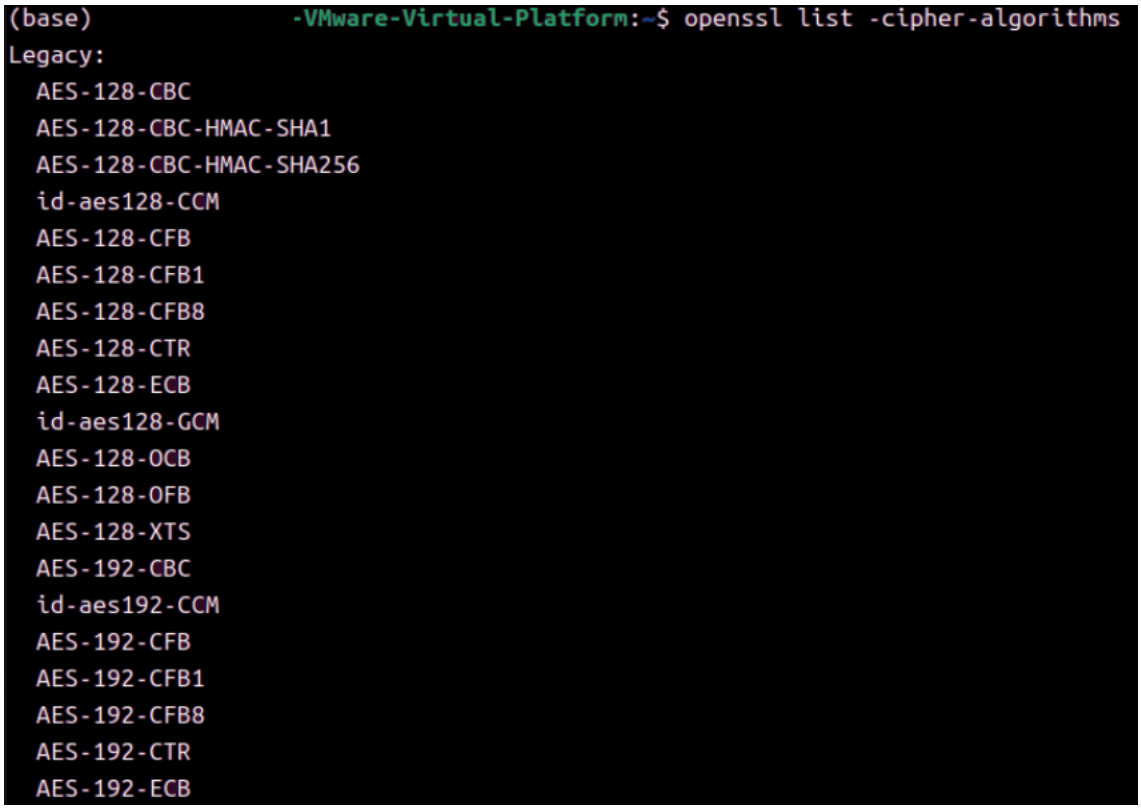


Figure 3-207 그림 제목

3.14.3 판정근거

Table 3-276 TE04.14.02 시험결과 판정근거

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

3.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

3.15 TE04.15.01

3.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE04.15.01	동작 전 자가시험 수행	암호모듈 검사

3.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-277 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

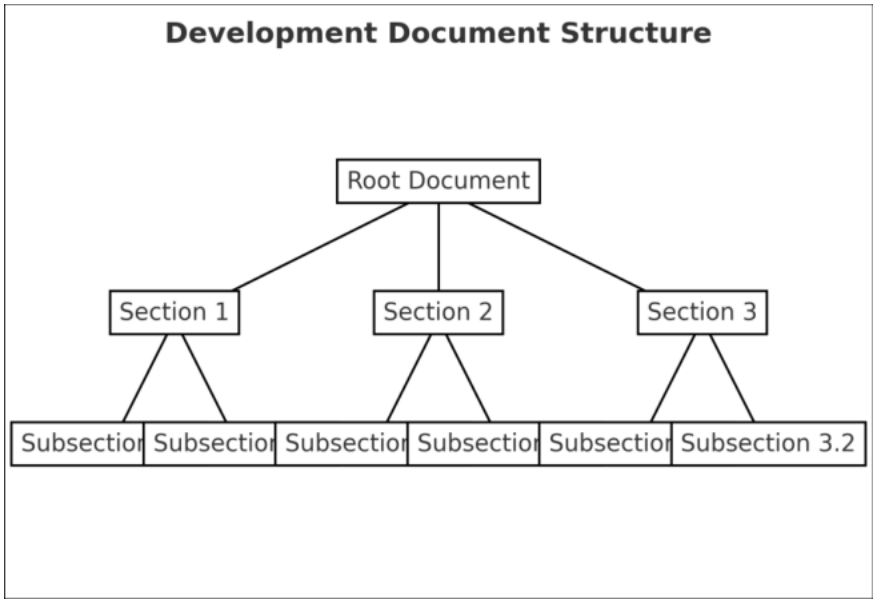


Figure 3-208 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-278 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

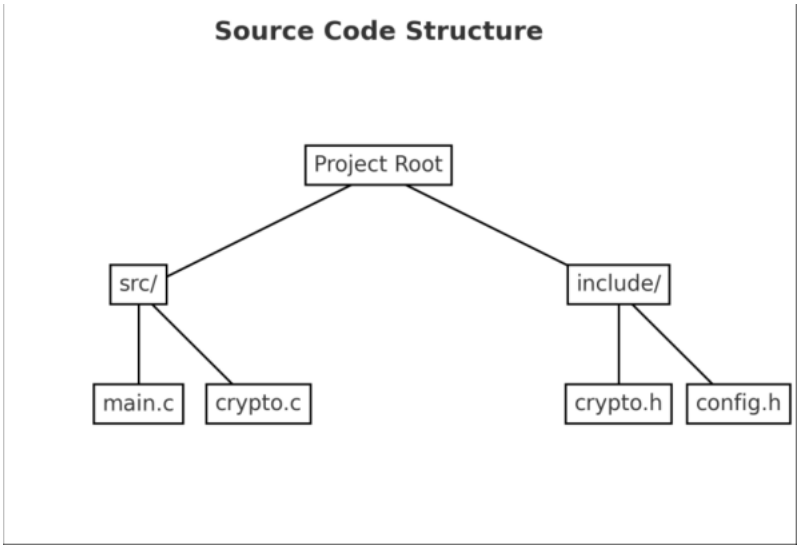


Figure 3-209 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-279 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

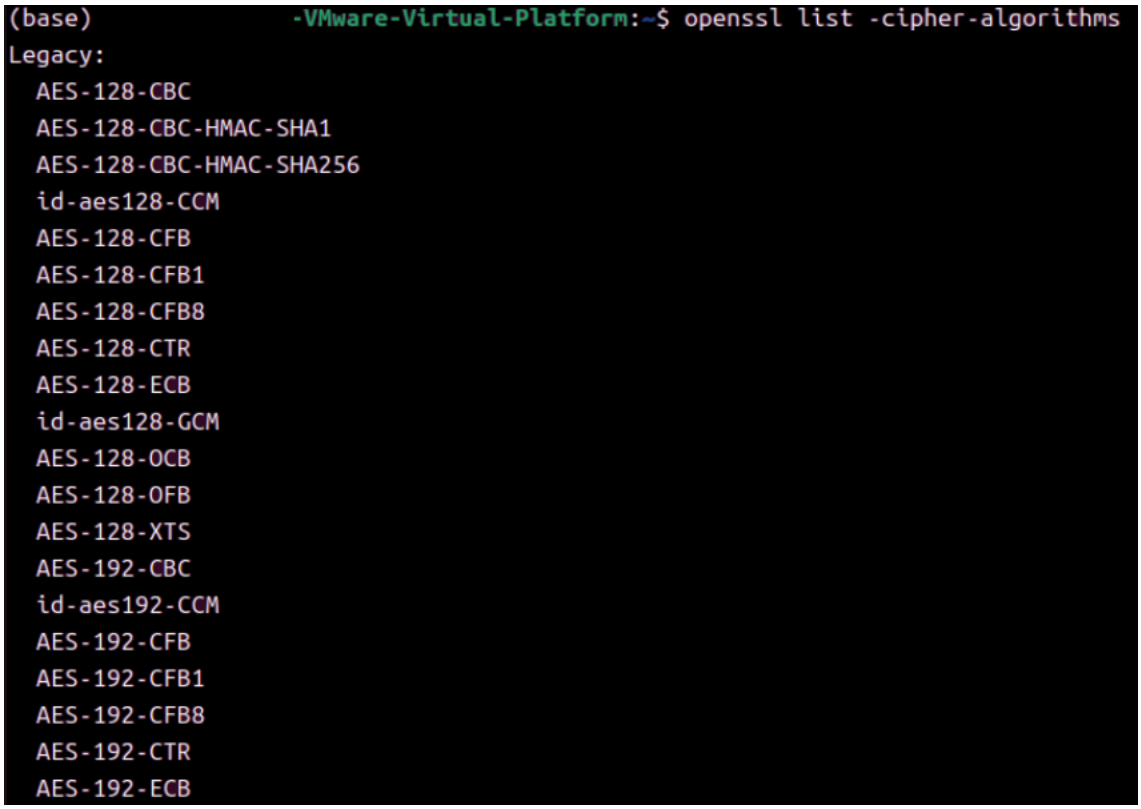


Figure 3-210 그림 제목

3.15.3 판정근거

Table 3-280 TE04.15.01 시험결과 판정근거

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

3.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4. 소프트웨어 / 펌웨어 보안 (AS05)

□ 암호모듈의 소프트웨어 , 펌웨어 구성요소에 대한 보안이 필요하다 .

4.1 AS05 시험항목

AS	TE	확인사항
AS05.02	1	개발문서의 최소 문서 요구사항 만족여부
AS05.04	1	개발문서와 암호모듈의 구성요소 일치여부
AS05.05	1	검증대상 무결성 기법의 암호 메커니즘
AS05.06	1, 2	무결성 시험 실패 시 오류상태 전환
AS05.09	1	인터페이스를 통한 무결성 시험

4.2 TE05.02.01

4.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.02.01	무결성 기법 및 수행방법에 대한 명세 여부	개발문서 검토

4.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-281 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

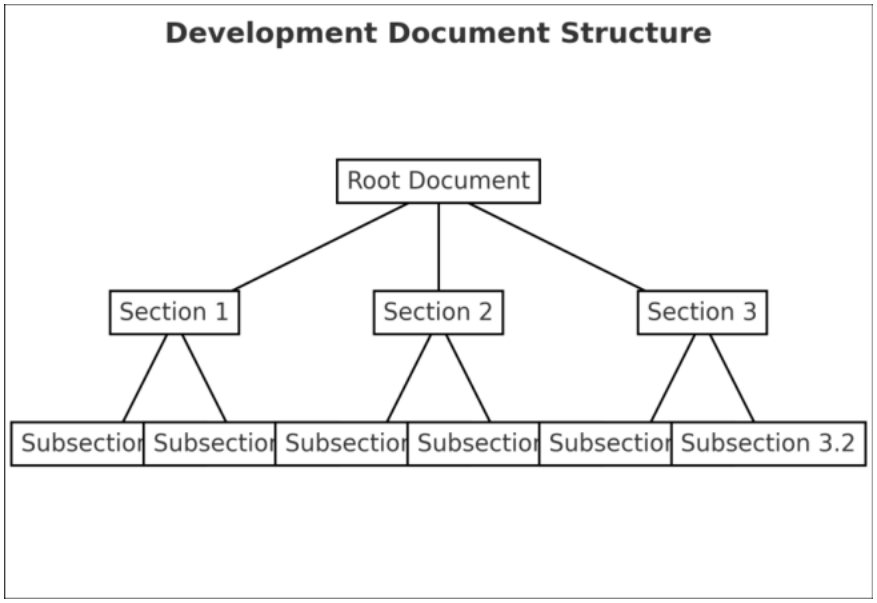


Figure 3-211 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-282 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

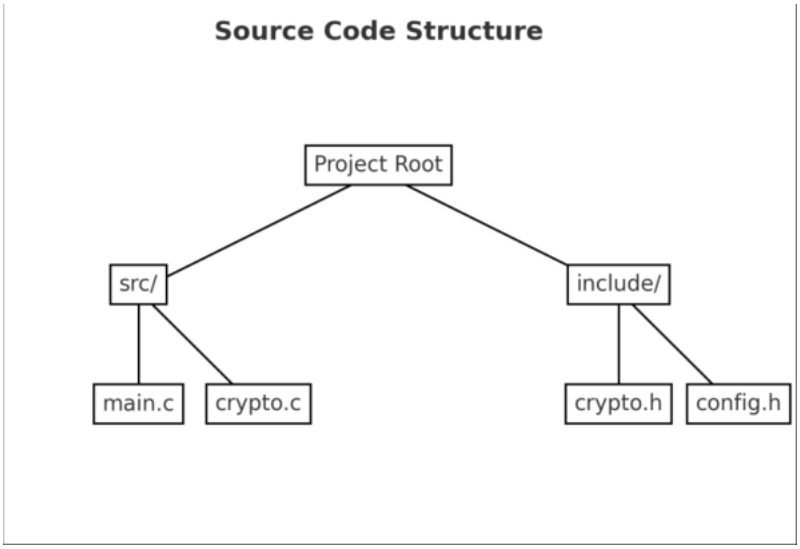


Figure 3-212 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-283 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

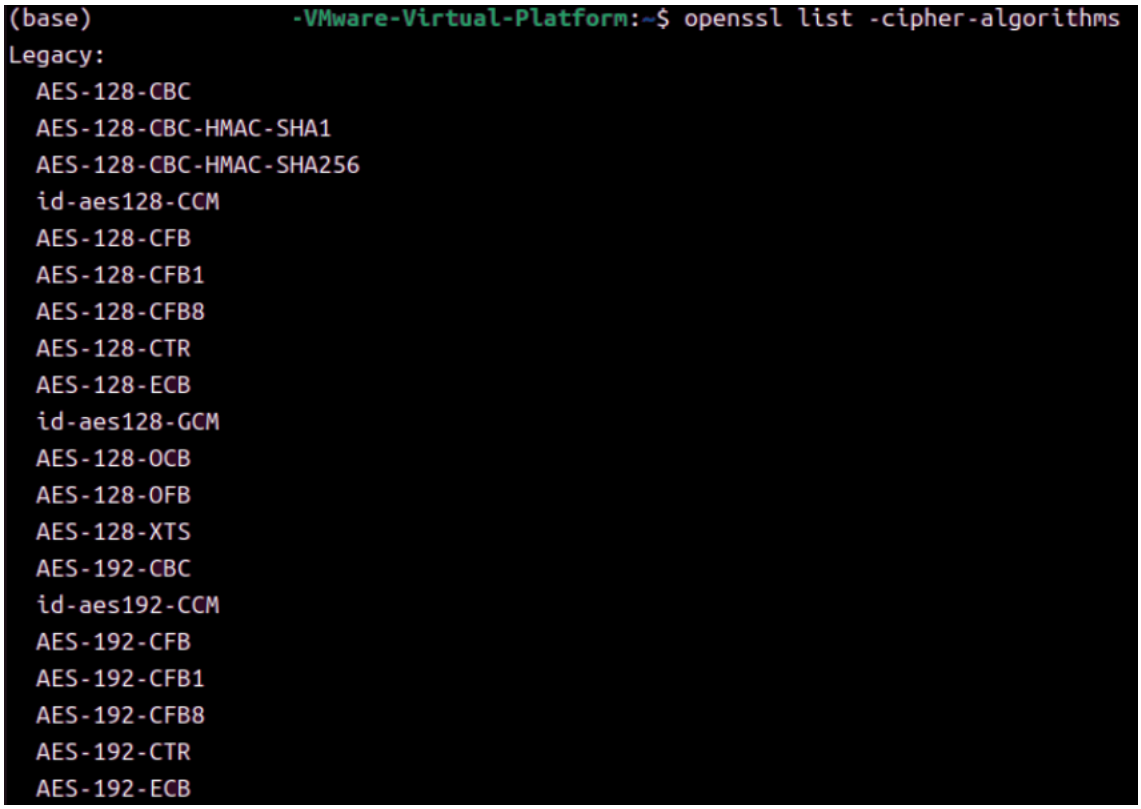


Figure 3-213 그림 제목

4.2.3 판정근거

Table 3-284 TE05.02.01 시험결과 판정근거

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

4.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4.3 TE05.04.01

4.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.04.01	암호모듈 구성요소 일치 여부 확인	개발문서 검토

4.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-285 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

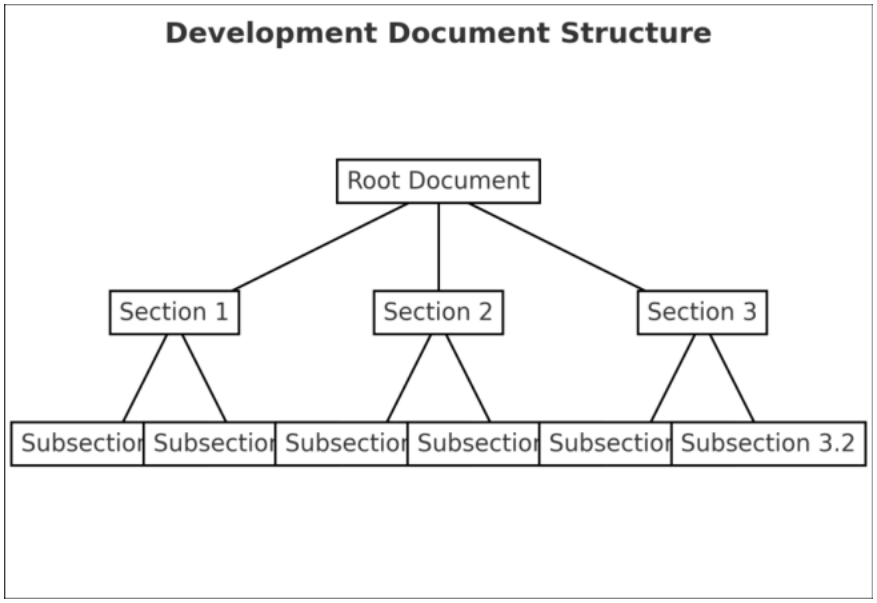


Figure 3-214 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-286 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

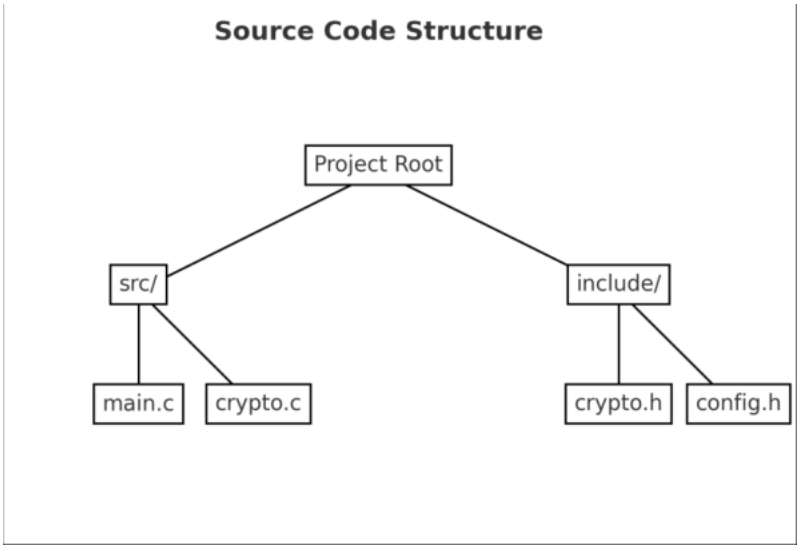


Figure 3-215 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-287 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

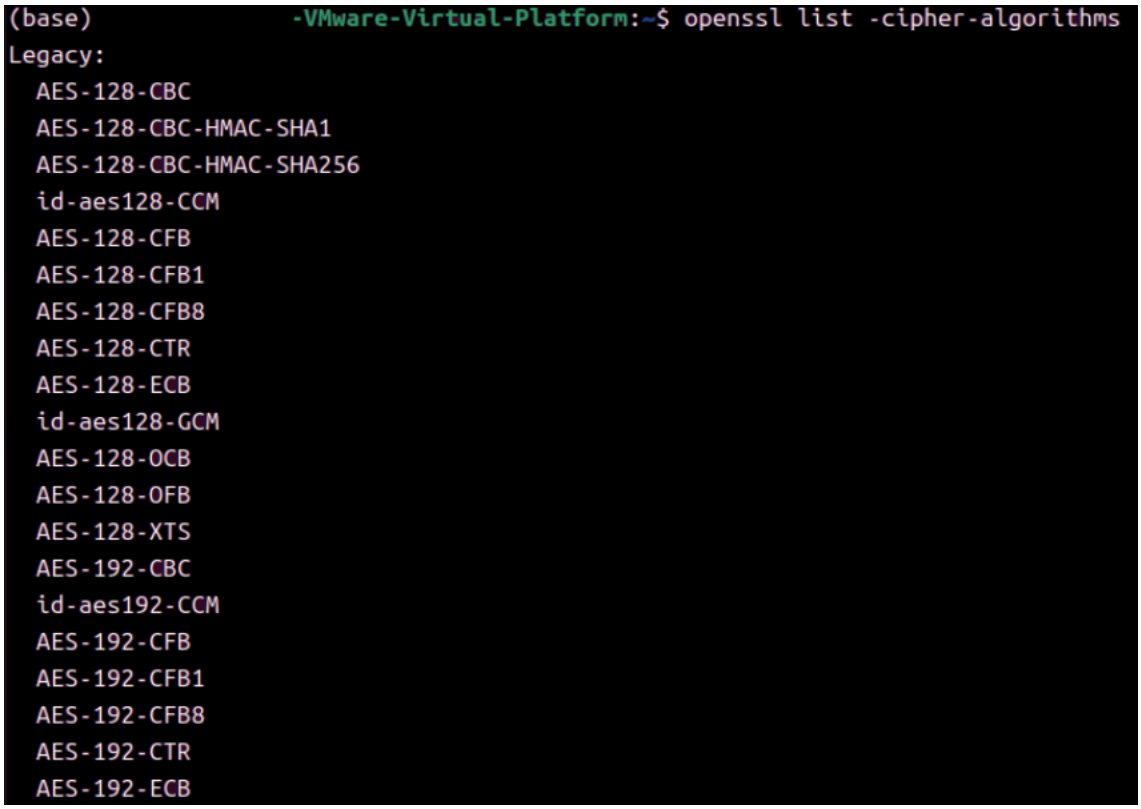


Figure 3-216 그림 제목

4.3.3 판정근거

Table 3-288 TE05.04.01 시험결과 판정근거

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

4.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4.4 TE05.05.01

4.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.05.01	모든 SW, FW 구성요소에 대해 무결성 기술 적용	암호모듈 검사

4.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-289 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

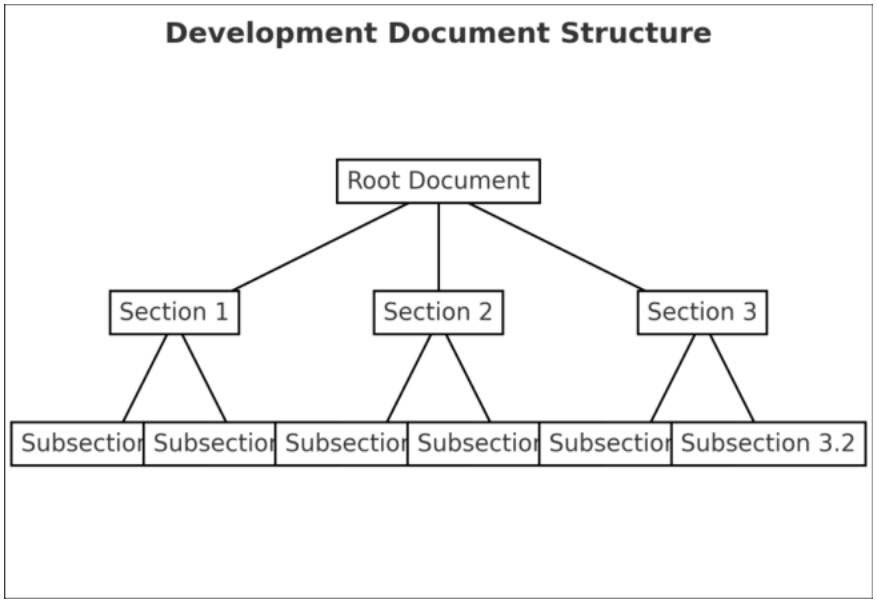


Figure 3-217 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-290 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

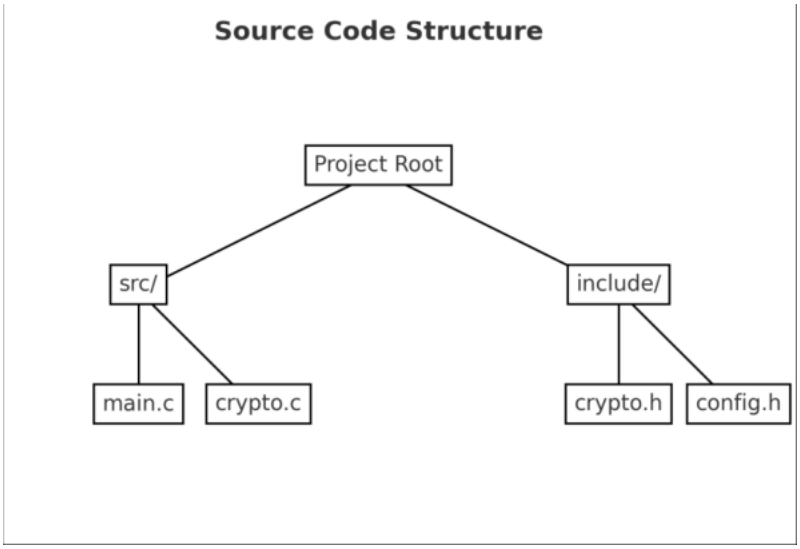


Figure 3-218 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-291 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

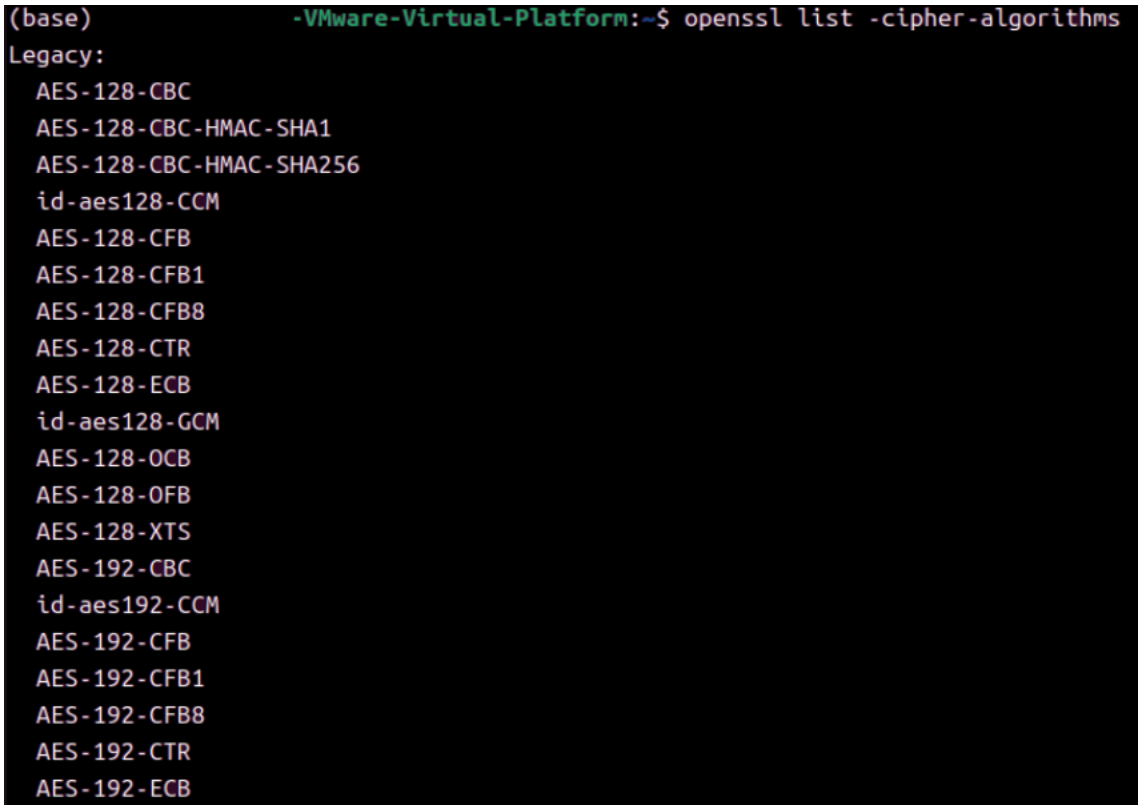


Figure 3-219 그림 제목

4.4.3 판정근거

Table 3-292 TE05.05.01 시험결과 판정근거

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

4.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4.5 TE05.06.01

4.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.06.01	무결성 시험 실패 시 오류 상태로 전환	암호모듈 검사

4.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-293 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

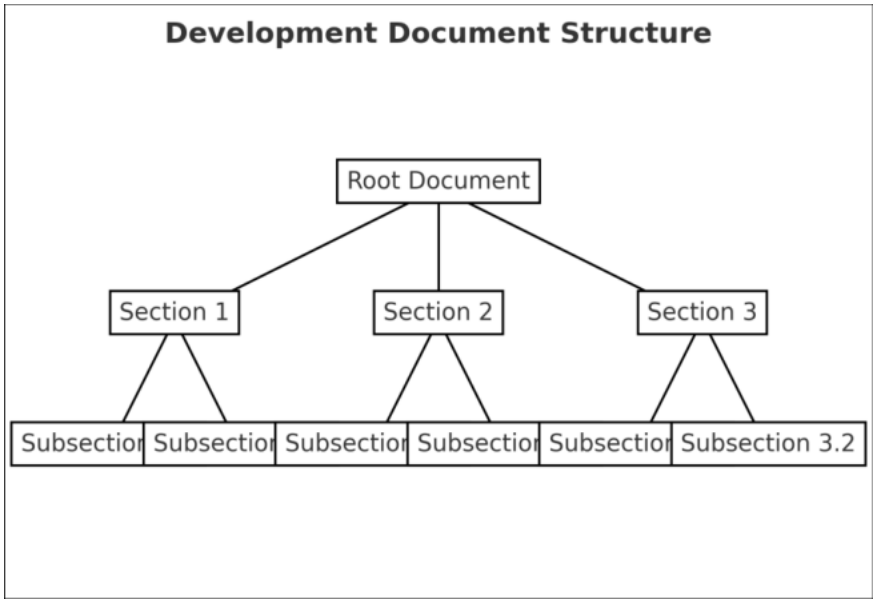


Figure 3-220 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-294 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

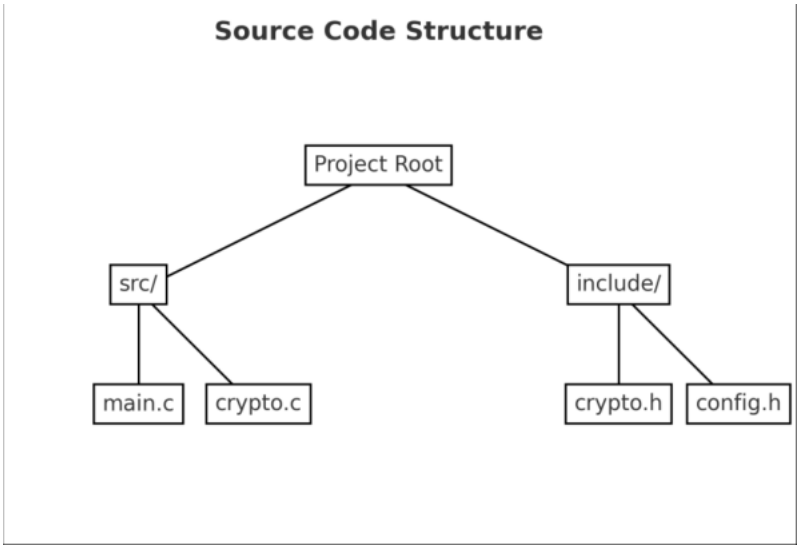


Figure 3-221 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-295 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

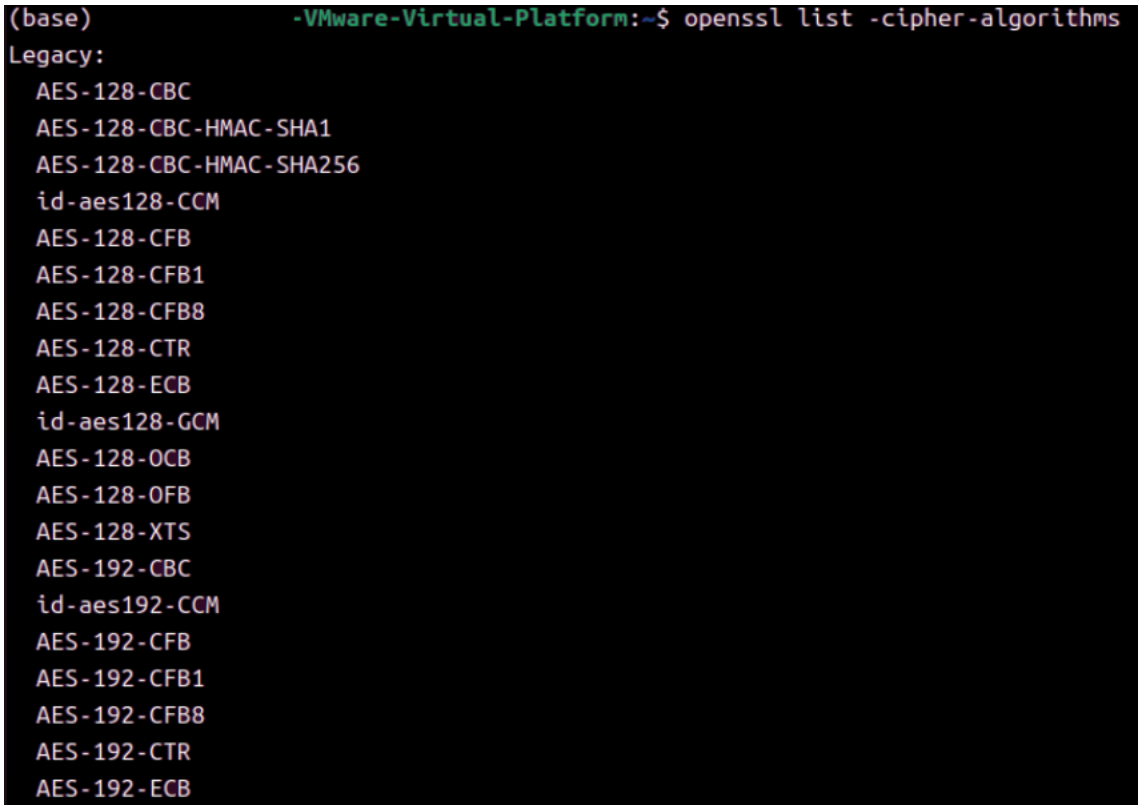


Figure 3-222 그림 제목

4.5.3 판정근거

Table 3-296 TE05.06.01 시험결과 판정근거

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

4.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4.6 TE05.06.02

4.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.06.02	무결성 시험 과정 중 생성된 중간값들 제로화	암호모듈 검사

4.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-297 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

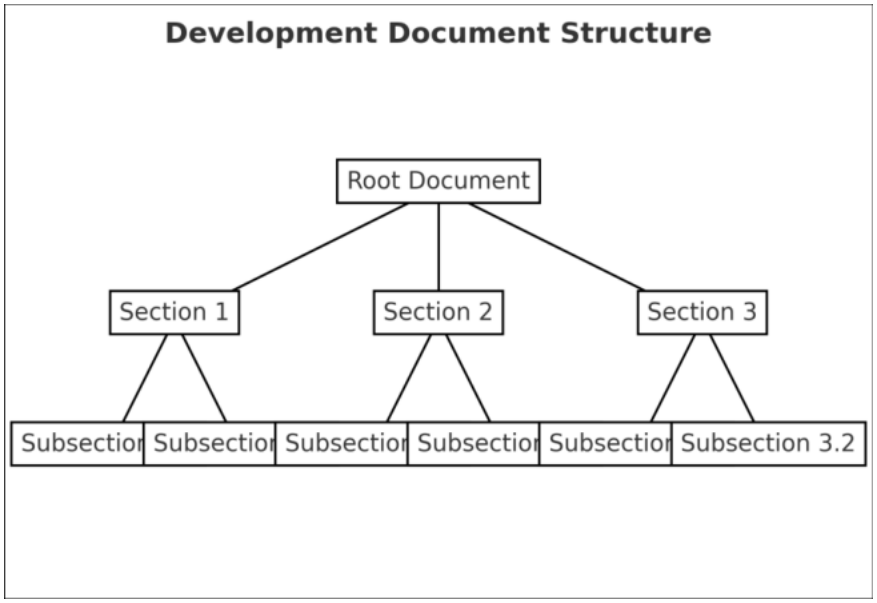


Figure 3-223 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-298 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

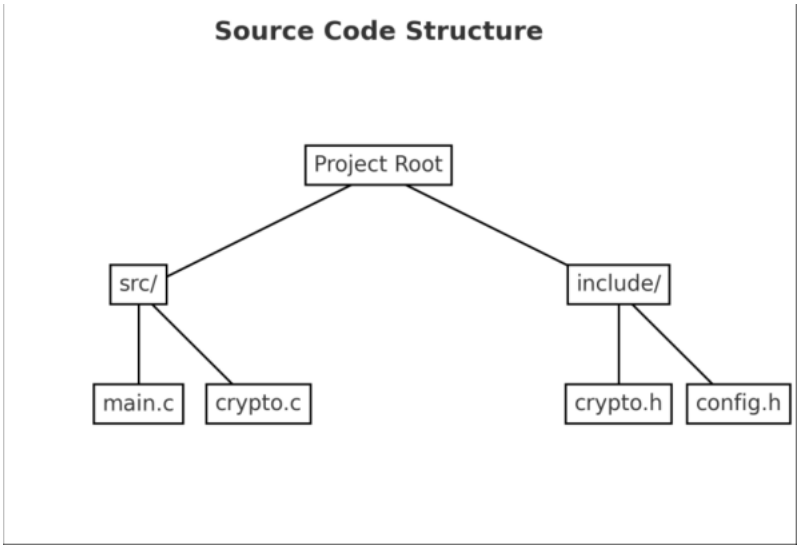


Figure 3-224 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-299 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

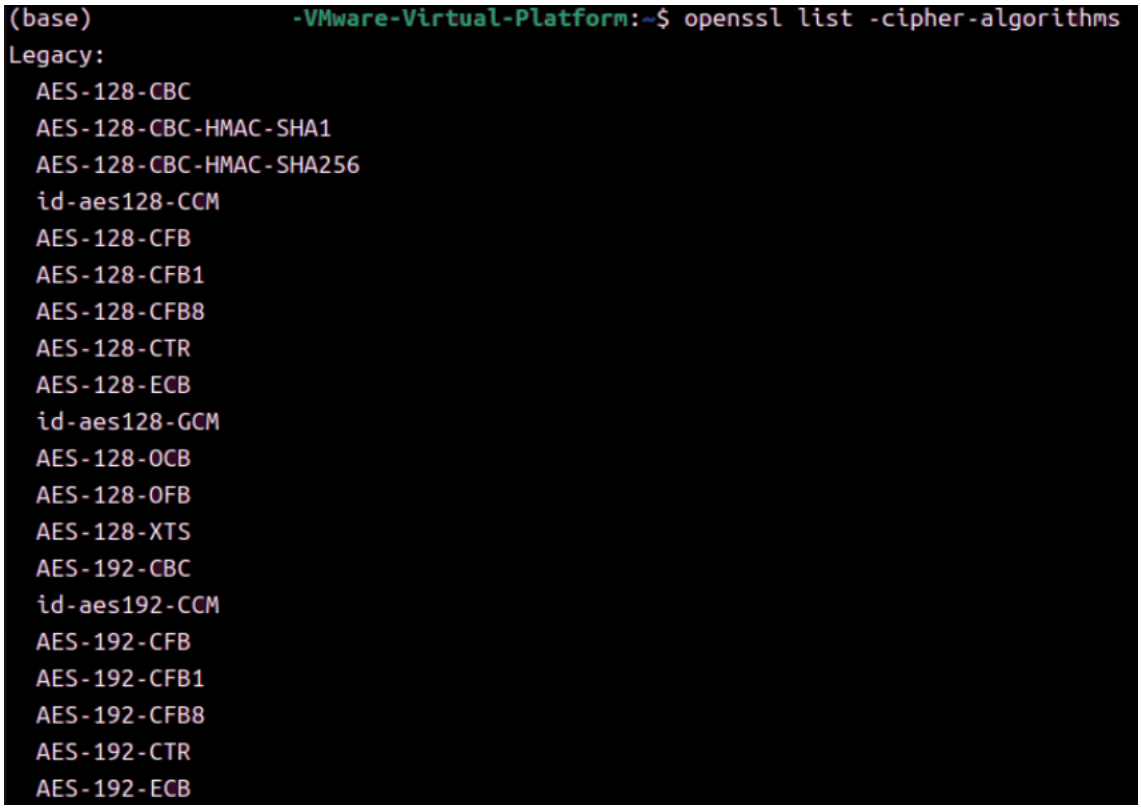


Figure 3-225 그림 제목

4.6.3 판정근거

Table 3-300 TE05.06.02 시험결과 판정근거

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

4.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

4.7 TE05.09.01

4.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE05.09.01	소프트웨어 모듈 인터페이스를 통한 무결성 시험 수행	소스코드 검토

4.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-301 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

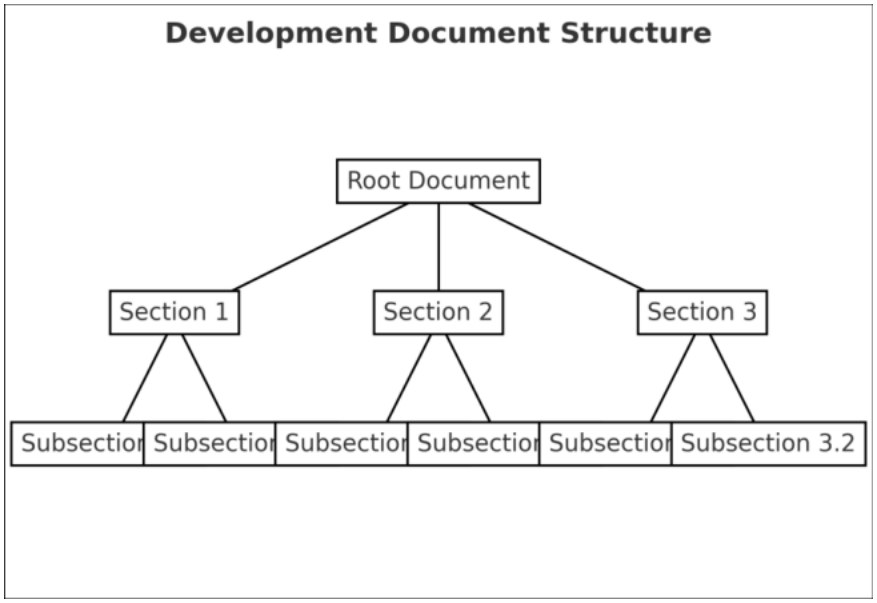


Figure 3-226 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-302 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

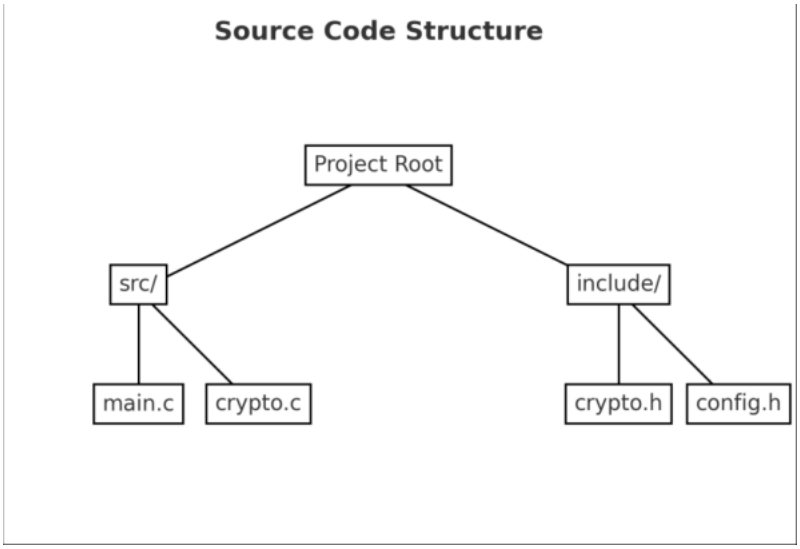


Figure 3-227 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-303 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

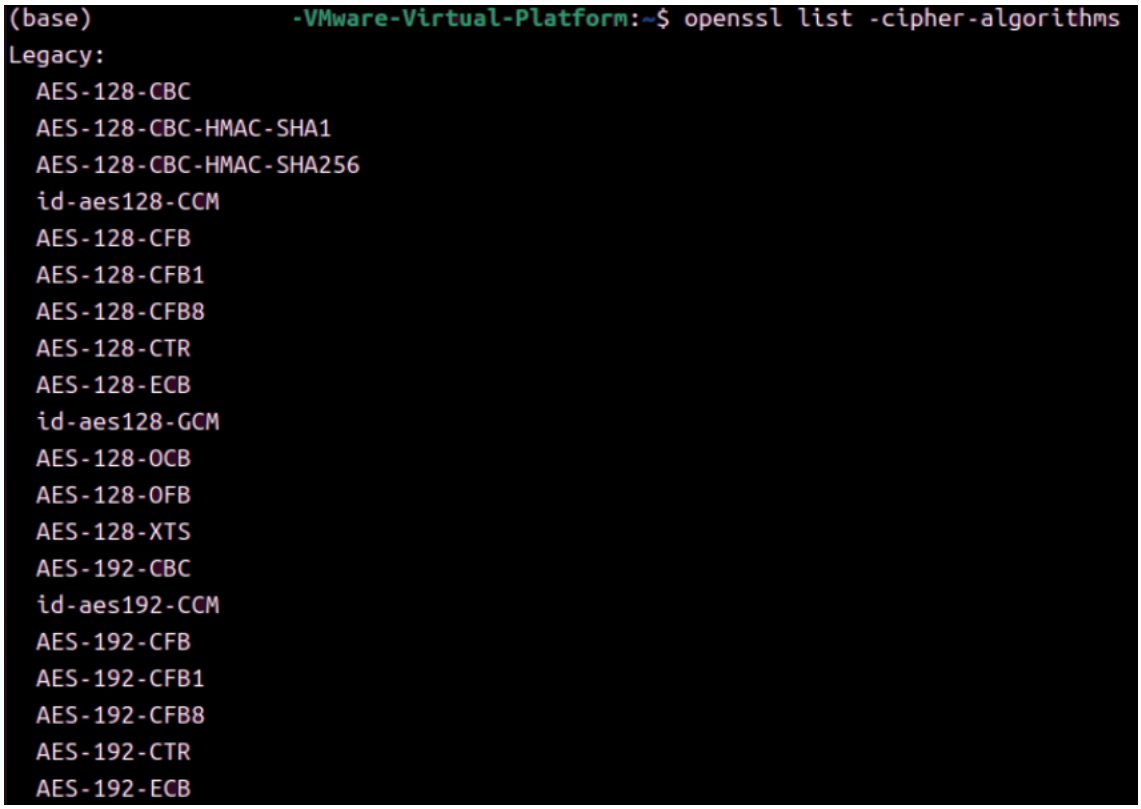


Figure 3-228 그림 제목

4.7.3 판정근거

Table 3-304 TE05.09.01 시험결과 판정근거

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

4.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5. 운영환경 (AS06)

□ 운영환경은 암호모듈을 동작 시키기 위해 필요한 소프트웨어 , 펌웨어 및 하드웨어 구성요소의 관리를 말한다 .

5.1 AS06 시험항목

AS	TE	확인사항
AS06.03	1	개발문서의 최소 문서 요구사항 만족 여부
AS06.05	1, 2, 3	운영체제를 통해 암호모듈 스스로 SSP 제어
AS06.06	1, 2	인가되지 않은 CSP 접근 및 제어되지 않는 보안매개변수 변경을 운영환경이 방지
AS06.07	1, 2	운영환경 설정 제한사항
AS06.08	1, 2, 3	암호모듈에 의해 생성된 프로세스는 해당 암호모듈만 소유

5.2 TE06.03.01

5.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.03.01	개발문서의 운영환경 문서 요구사항 만족	개발문서 검토

5.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-305 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

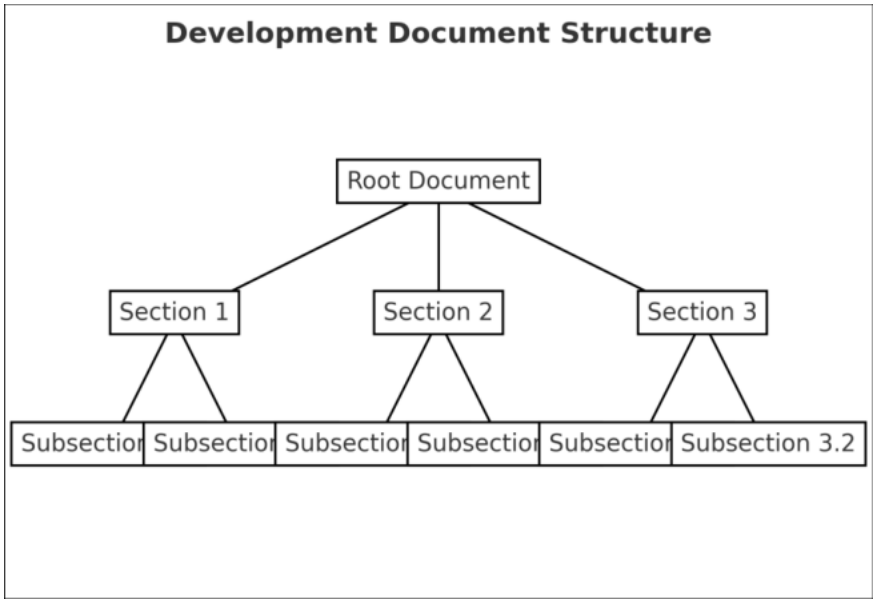


Figure 3-229 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-306 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

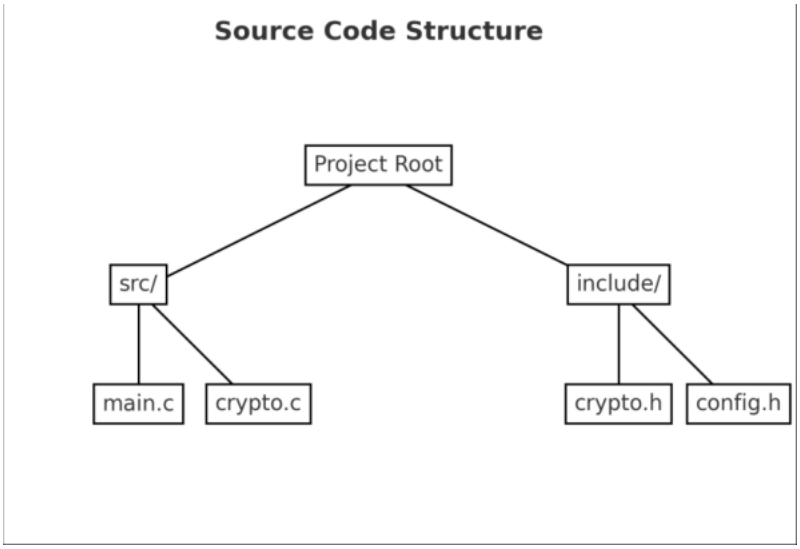


Figure 3-230 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-307 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

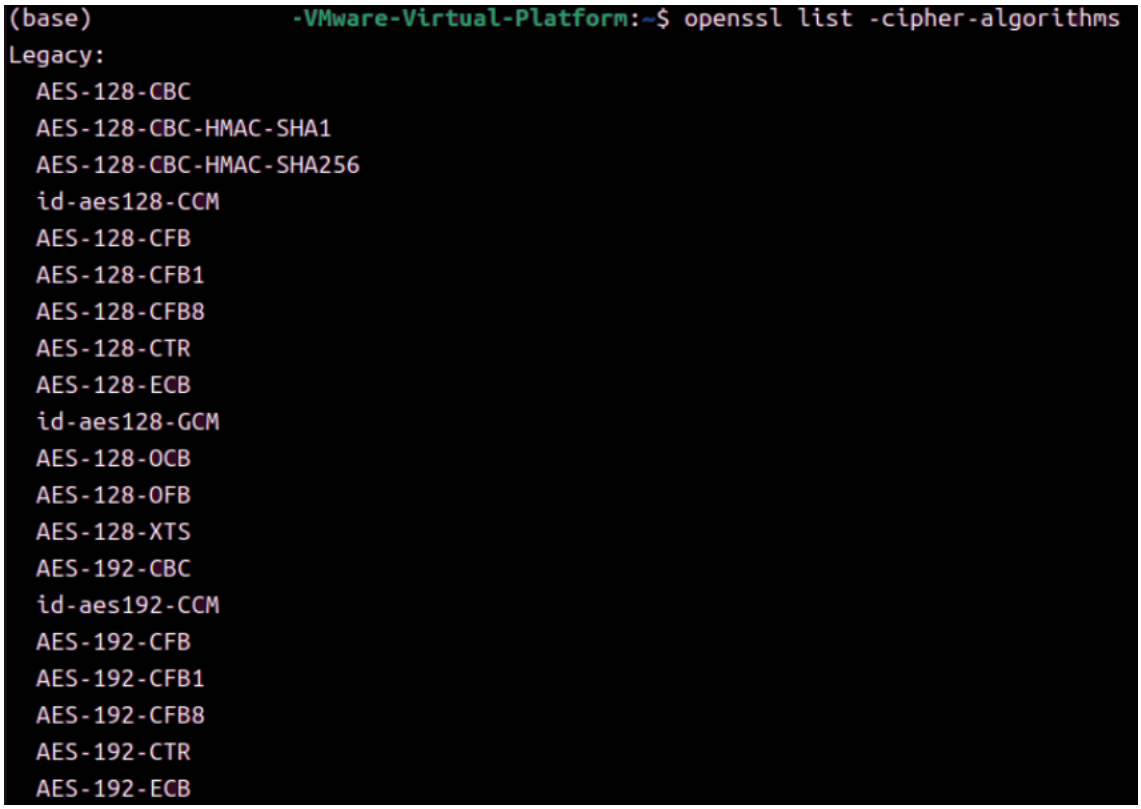


Figure 3-231 그림 제목

5.2.3 판정근거

Table 3-308 TE06.03.01 시험결과 판정근거

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

5.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.3 TE06.05.01

5.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.05.01	암호모듈의 각 인스턴스가 암호모듈 자신의 SSP 를 제어	개발문서 검토

5.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-309 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

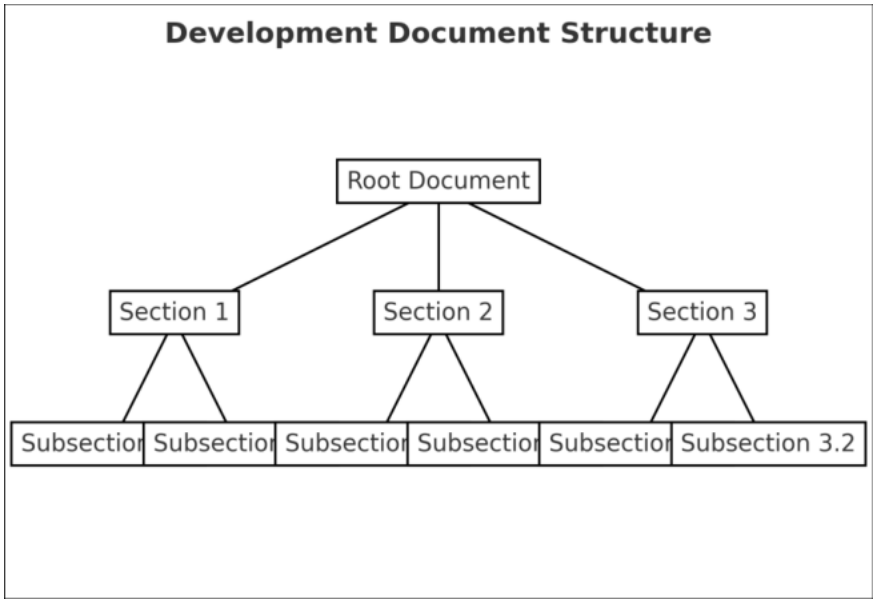


Figure 3-232 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-310 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

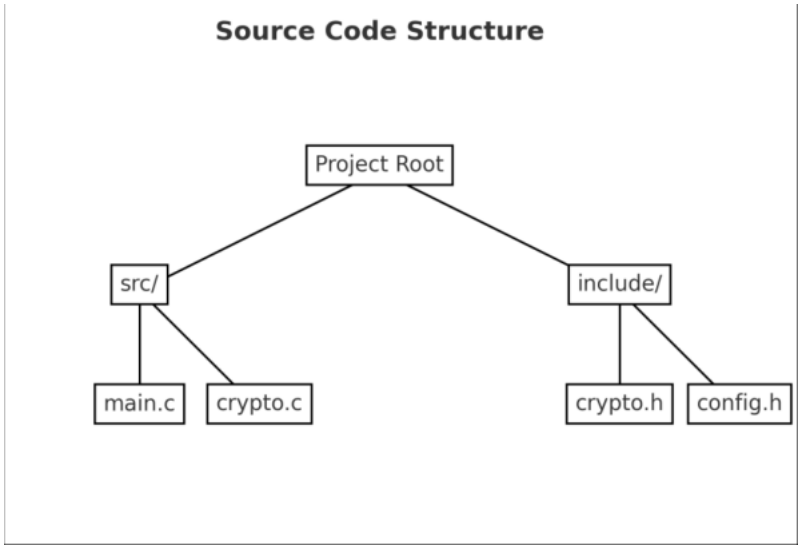


Figure 3-233 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-311 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

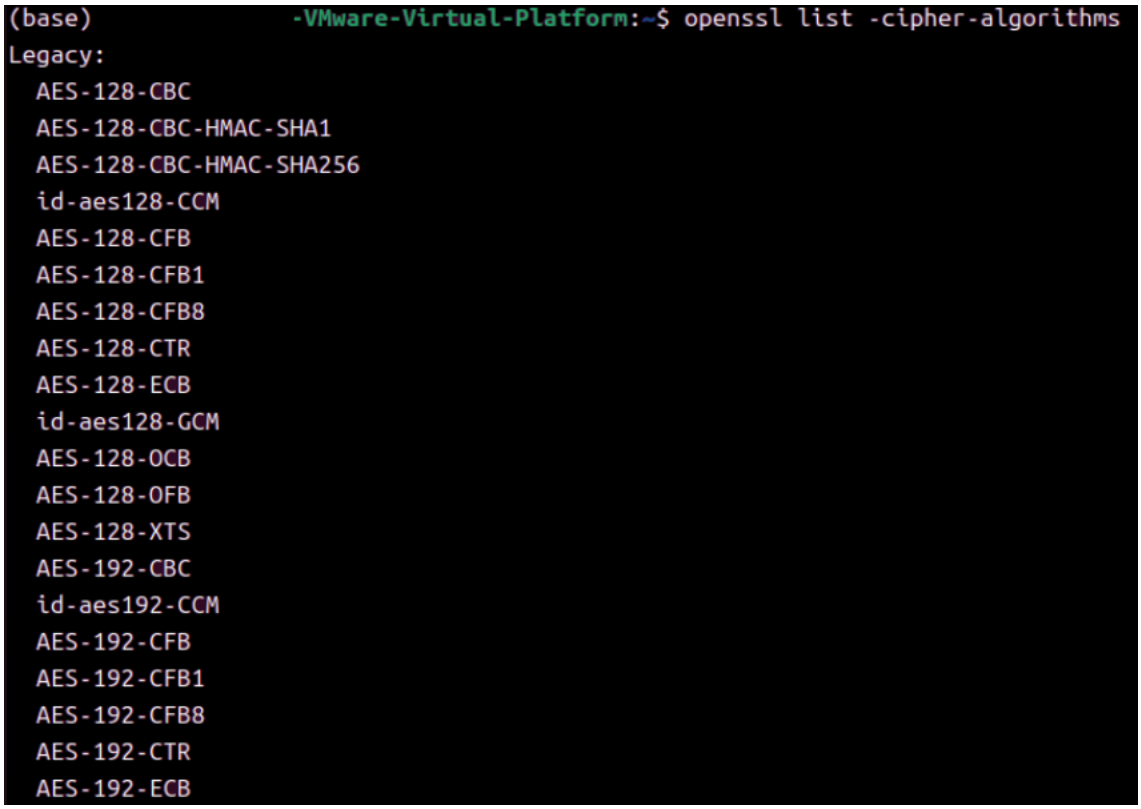


Figure 3-234 그림 제목

5.3.3 판정근거

Table 3-312 TE06.05.01 시험결과 판정근거

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

5.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.4 TE06.05.02

5.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.05.02	요구사항이 설명서나 관리적 절차가 아닌 암호모듈 스스로에 의해 수행	개발문서 검토

5.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-313 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

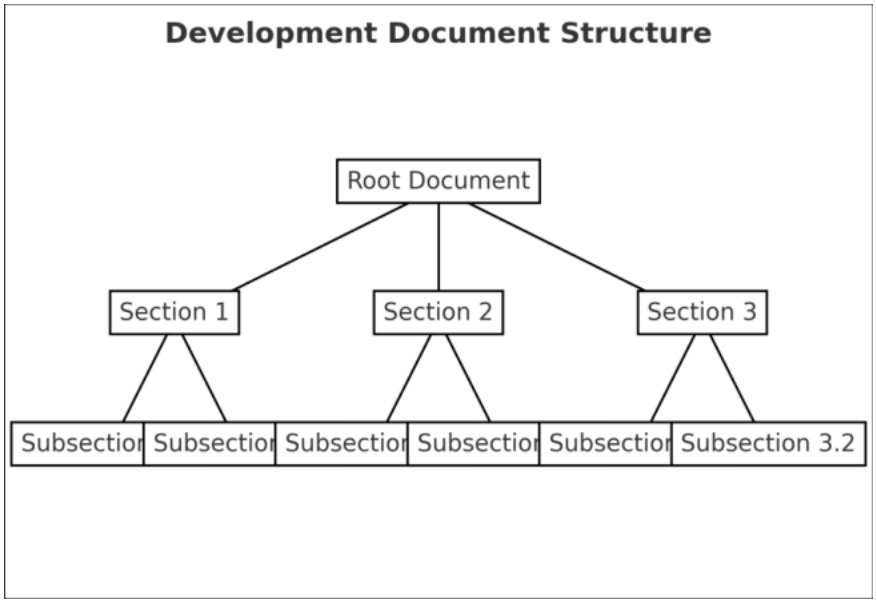


Figure 3-235 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-314 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

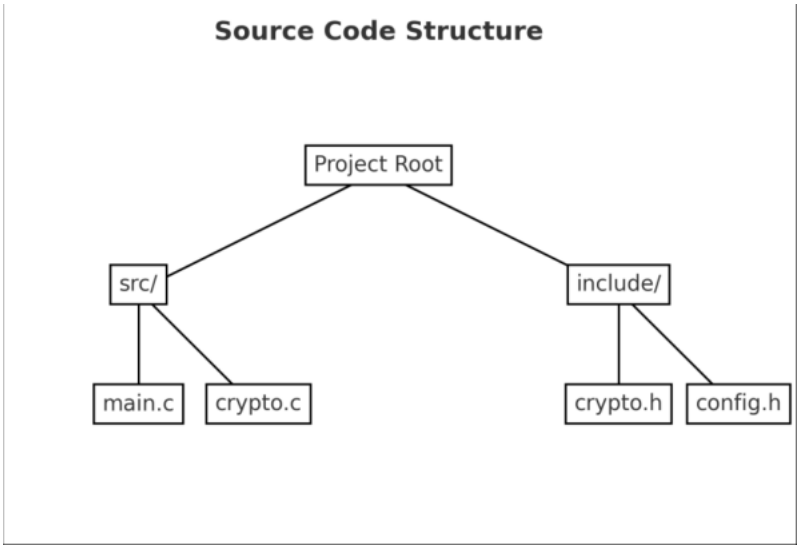


Figure 3-236 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-315 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

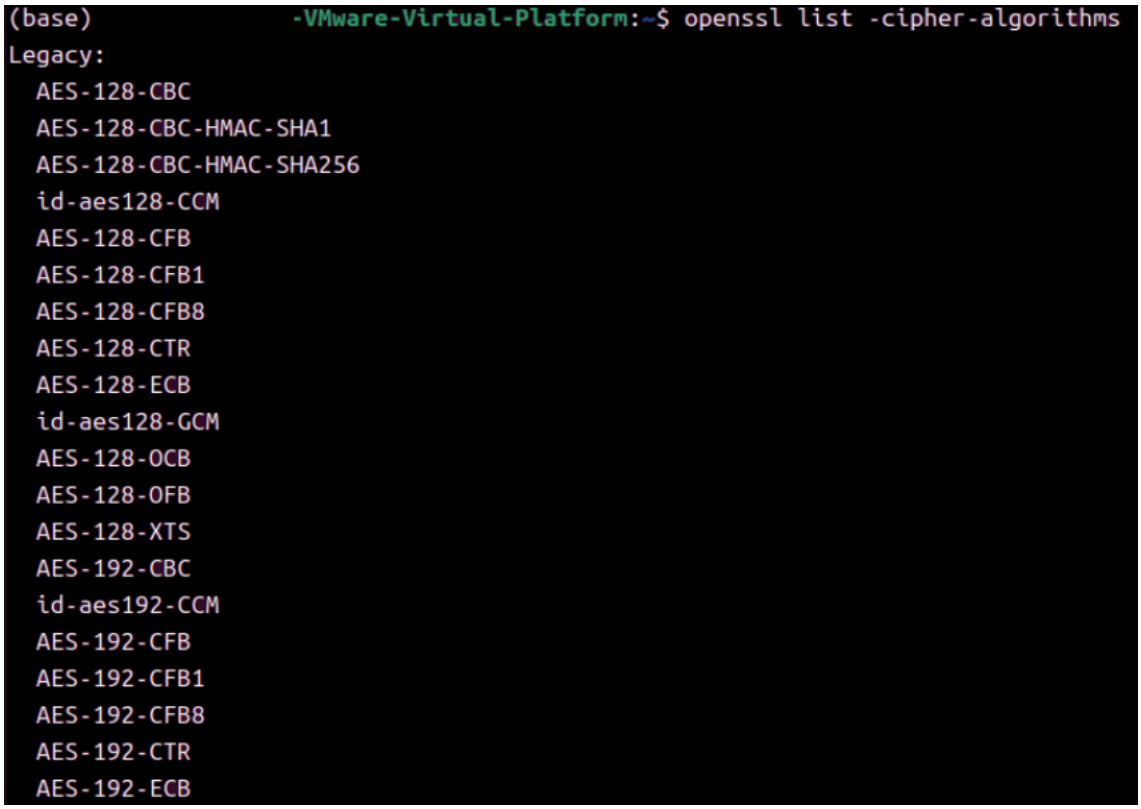


Figure 3-237 그림 제목

5.4.3 판정근거

Table 3-316 TE06.05.02 시험결과 판정근거

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

5.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.5 TE06.05.03

5.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.05.03	SSP 에 대해 인가되지 않은 접근 시도	암호모듈 검사

5.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-317 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

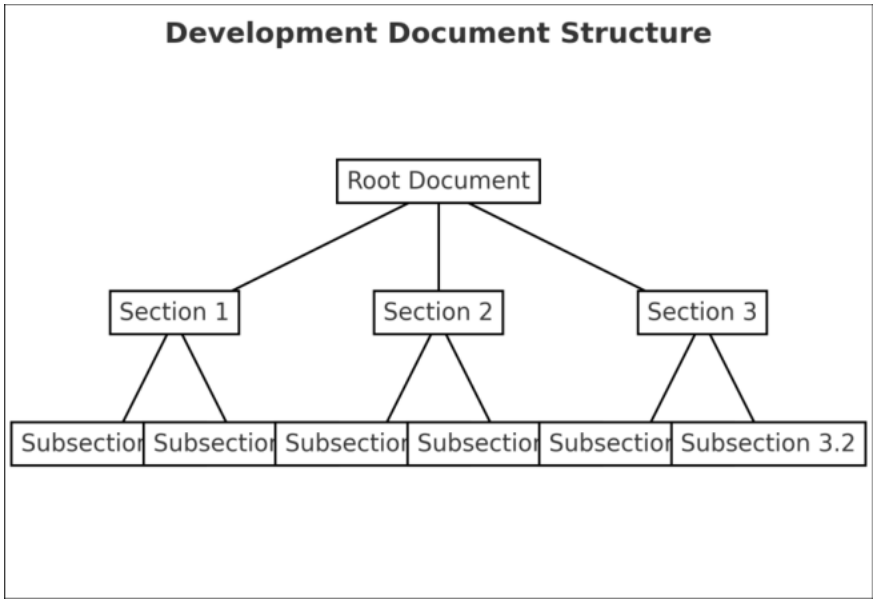


Figure 3-238 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-318 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

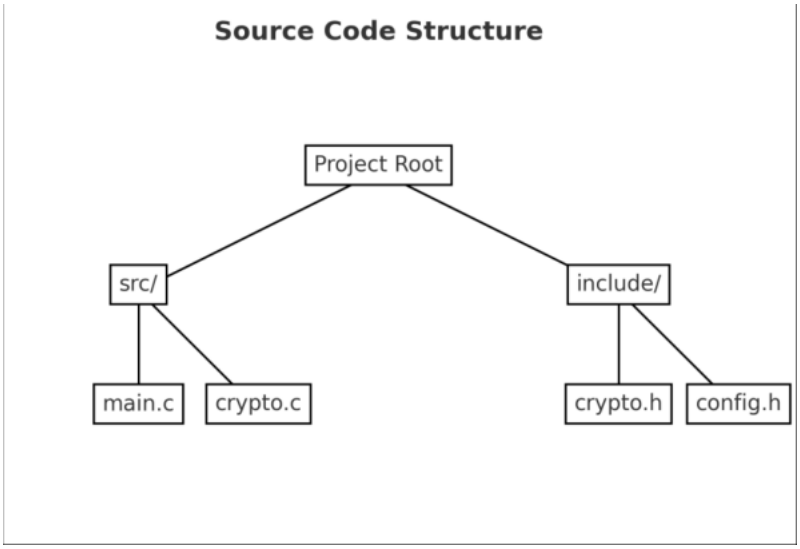


Figure 3-239 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-319 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

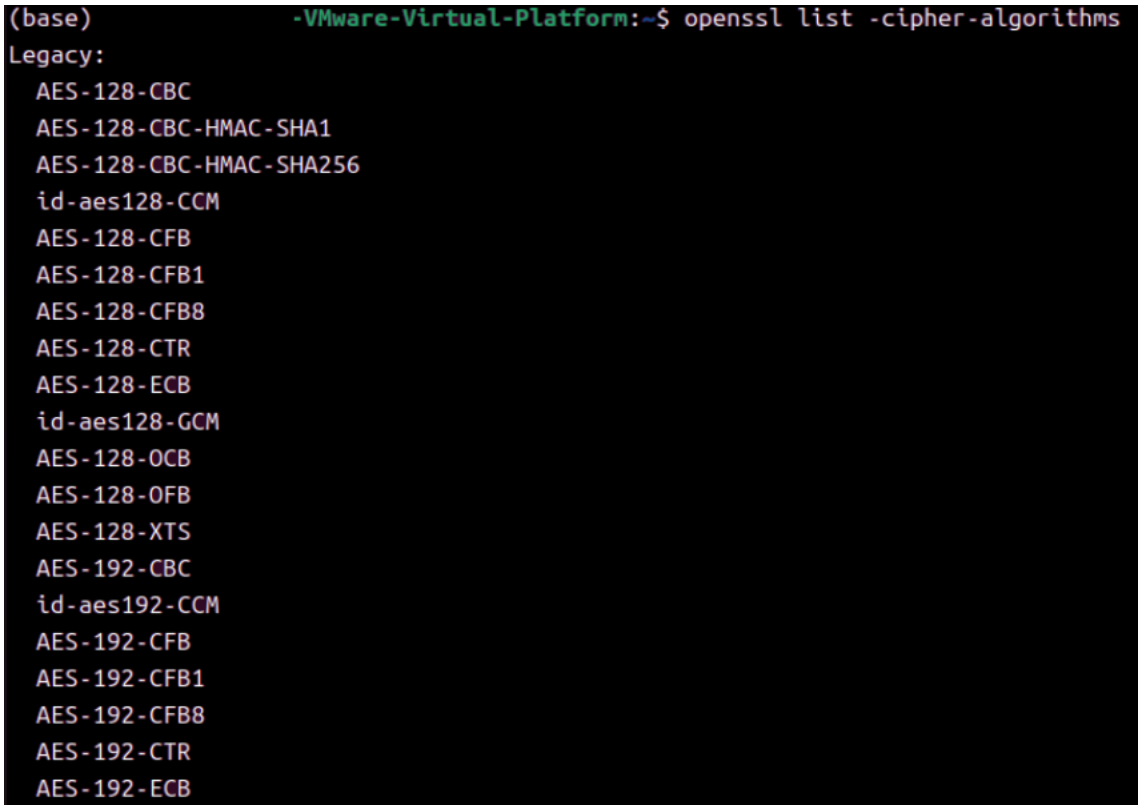


Figure 3-240 그림 제목

5.5.3 판정근거

Table 3-320 TE06.05.03 시험결과 판정근거

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

5.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.6 TE06.06.01

5.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.06.01	인가되지 않은 CSP 접근과 변경을 방지하기 위한 운영환경의 메커니즘	개발문서 검토

5.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-321 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

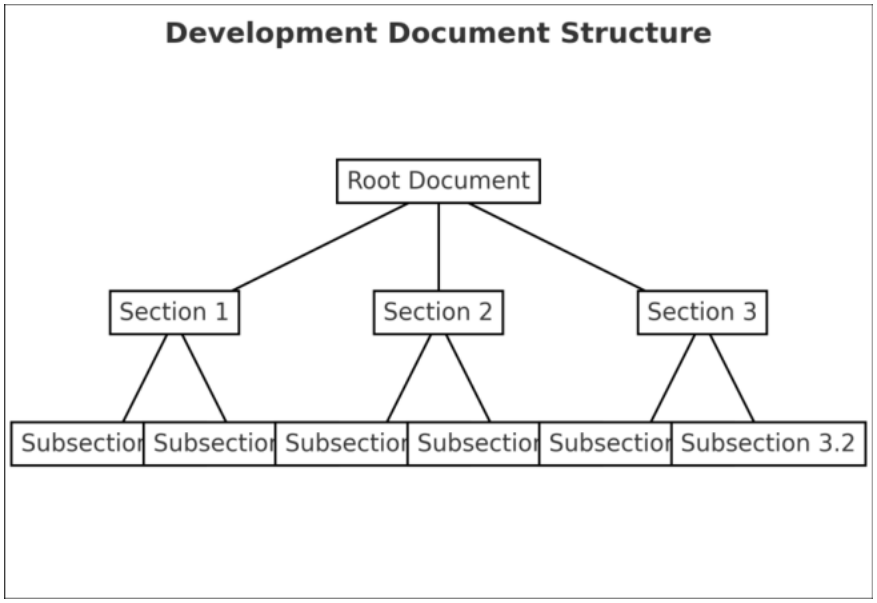


Figure 3-241 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-322 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

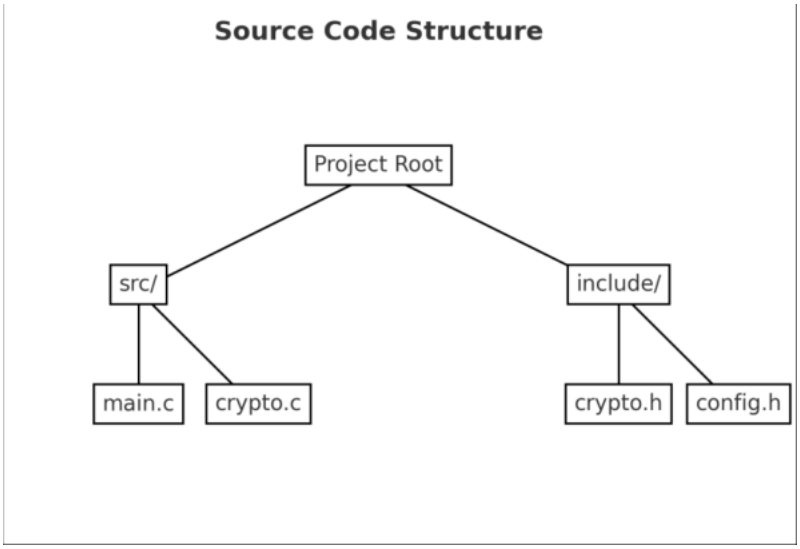


Figure 3-242 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-323 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

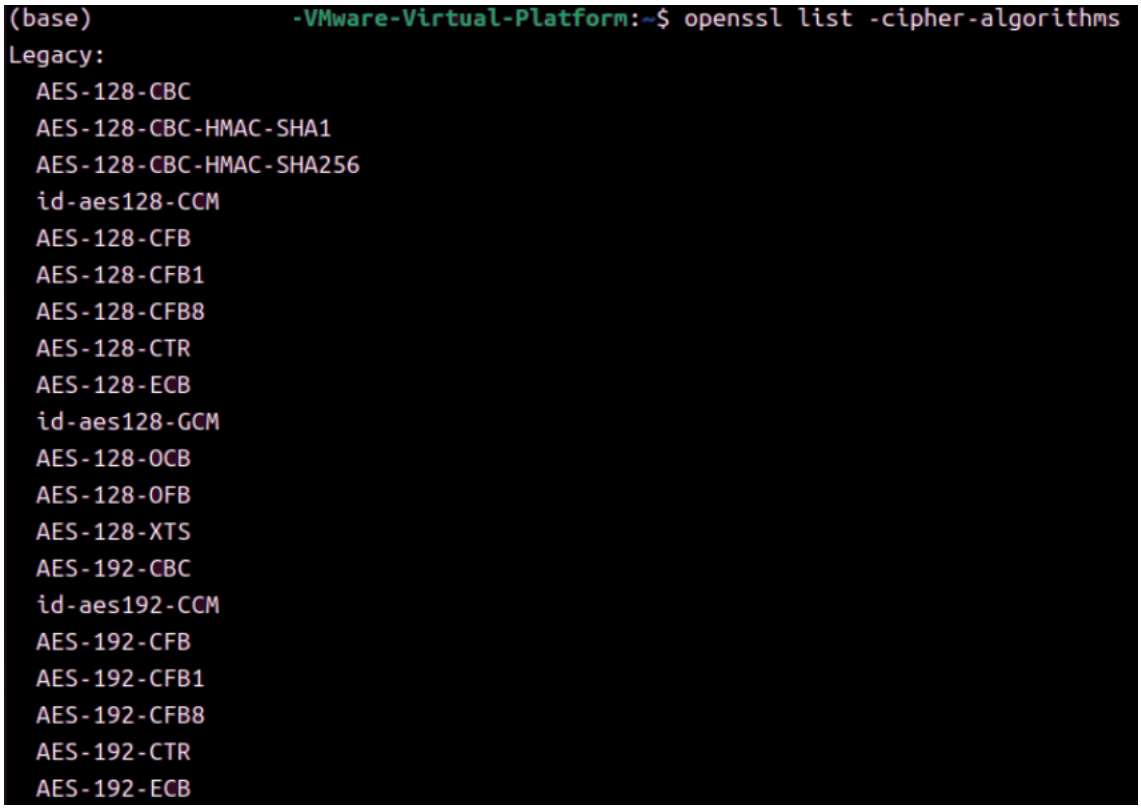


Figure 3-243 그림 제목

5.6.3 판정근거

Table 3-324 TE06.06.01 시험결과 판정근거

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

5.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.7 TE06.06.02

5.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.06.02	CSP 에 대해 인가되지 않은 접근 시도	암호모듈 검사

5.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-325 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

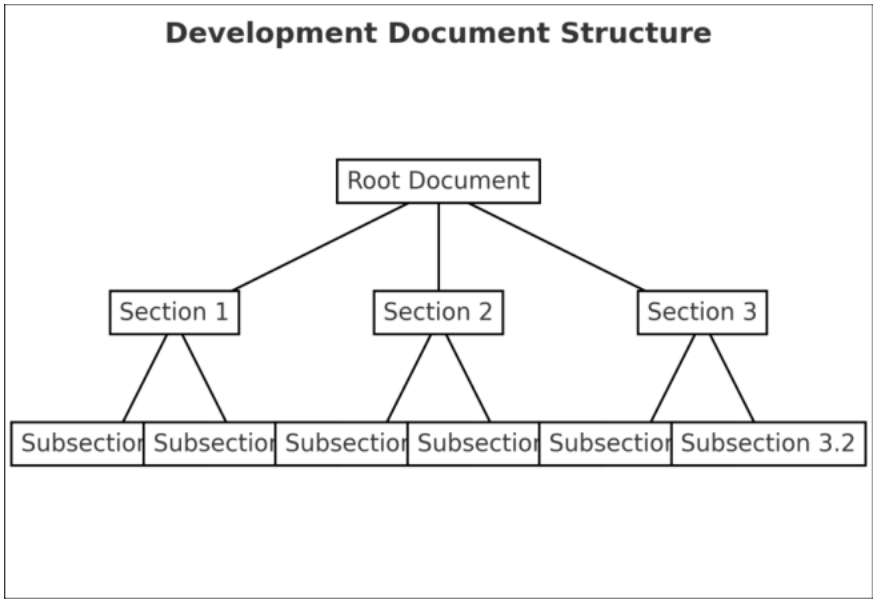


Figure 3-244 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-326 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

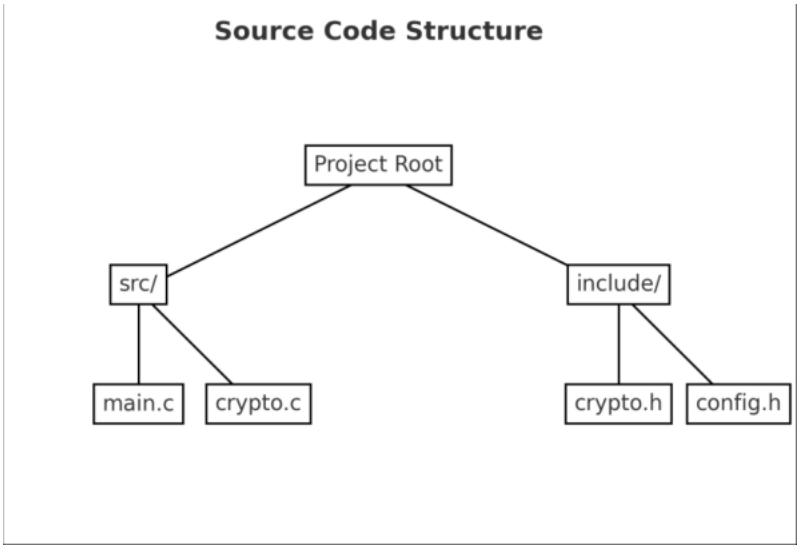


Figure 3-245 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-327 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

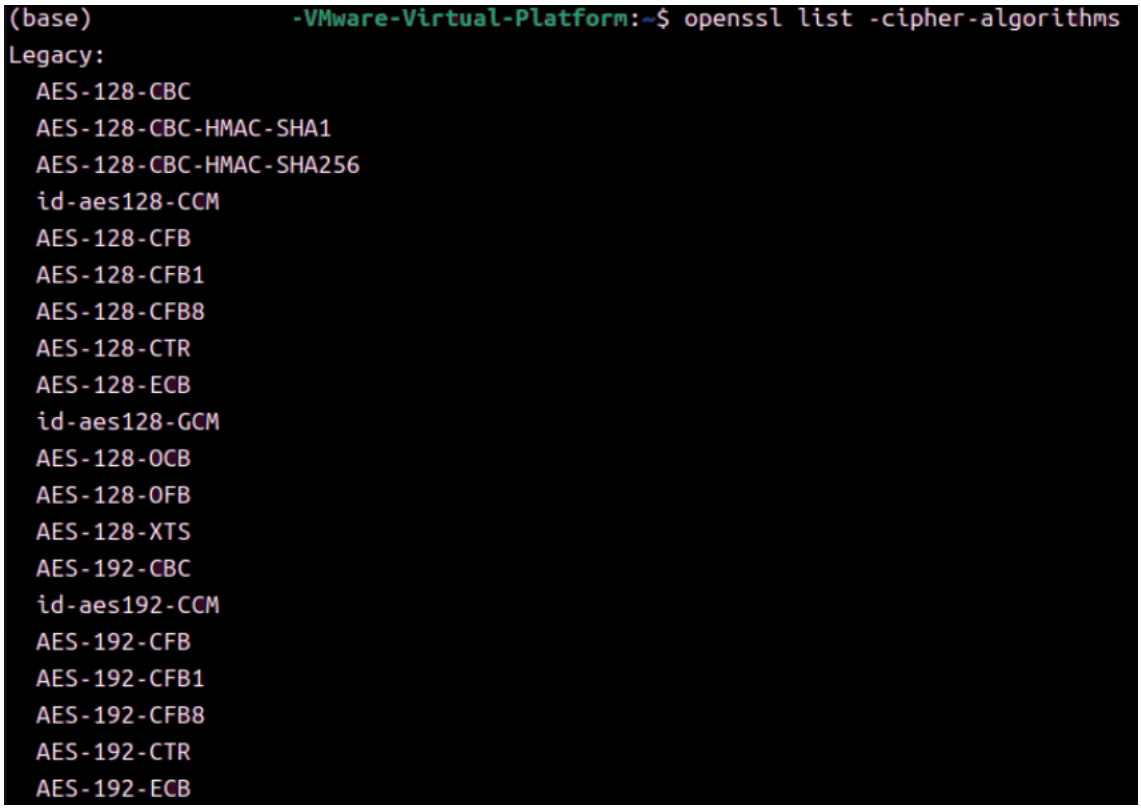


Figure 3-246 그림 제목

5.7.3 판정근거

Table 3-328 TE06.06.02 시험결과 판정근거

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

5.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.8 TE06.07.01

5.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.07.01	개발문서에 운영환경에 대한 규제 포함	개발문서 검토

5.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-329 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

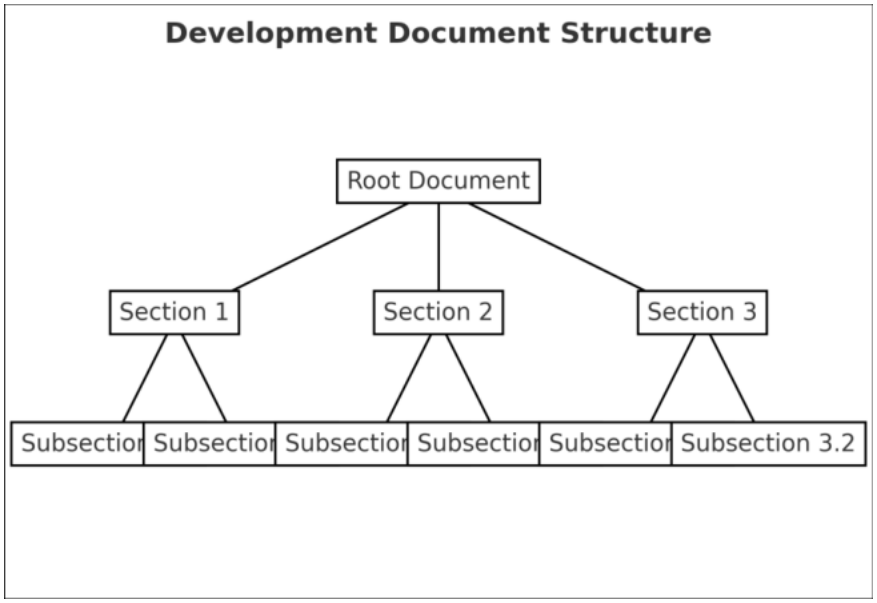


Figure 3-247 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-330 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

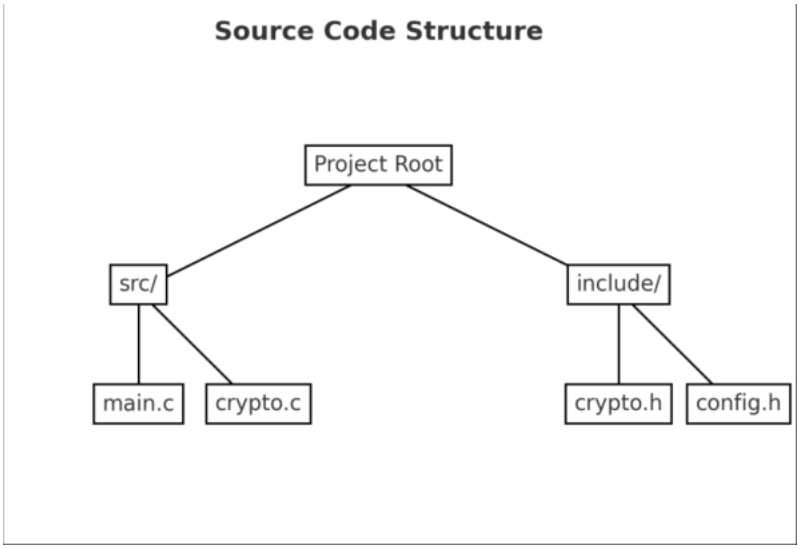


Figure 3-248 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-331 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

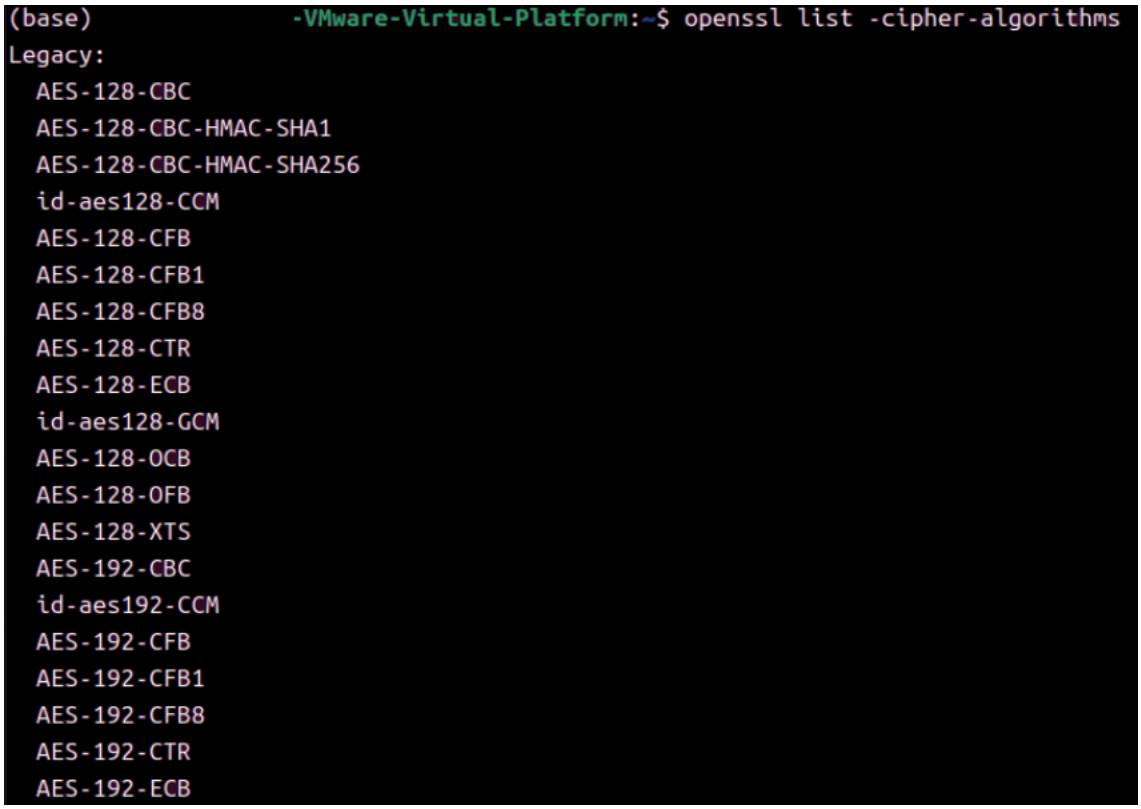


Figure 3-249 그림 제목

5.8.3 판정근거

Table 3-332 TE06.07.01 시험결과 판정근거

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

5.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.9 TE06.07.02

5.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.07.02	보안정책문서에 운영환경에 대한 규제 포함	개발문서 검토

5.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-333 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

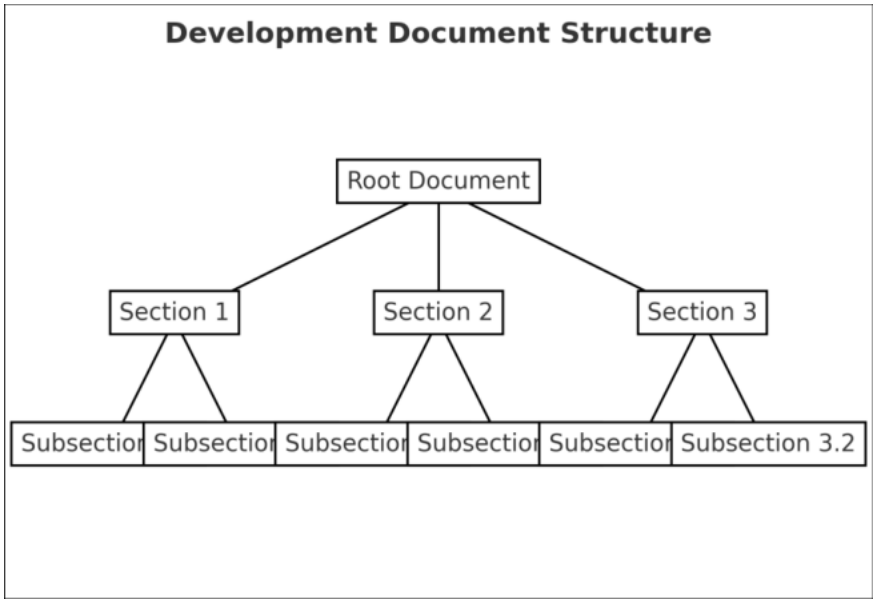


Figure 3-250 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-334 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

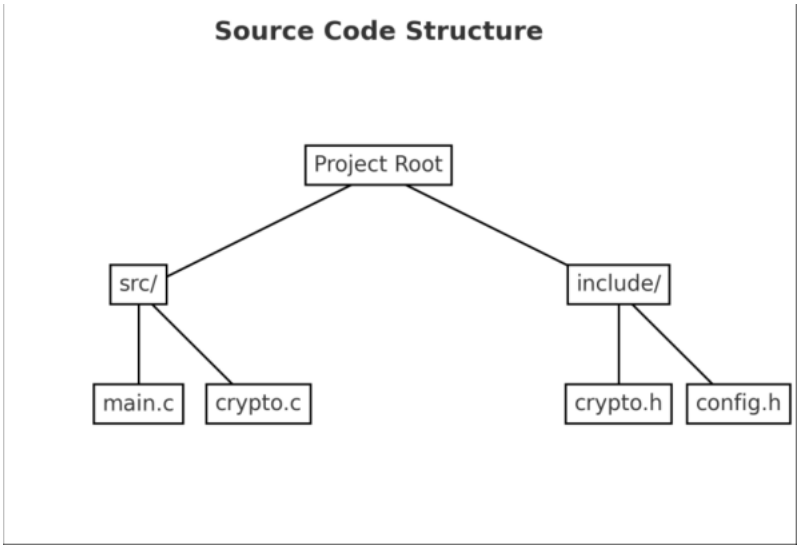


Figure 3-251 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-335 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

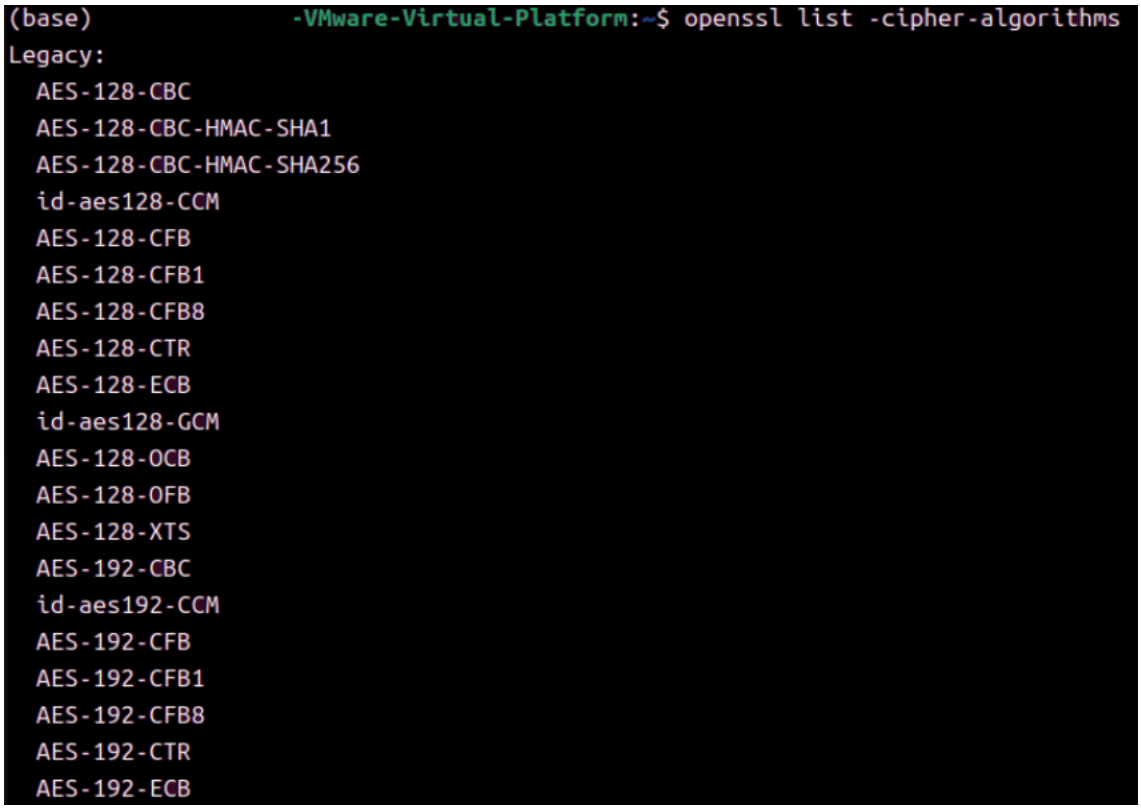


Figure 3-252 그림 제목

5.9.3 판정근거

Table 3-336 TE06.07.02 시험결과 판정근거

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

5.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.10 TE06.08.01

5.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.08.01	암호모듈에 의해 생성된 프로세스는 암호모듈만 소유	개발문서 검토

5.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-337 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

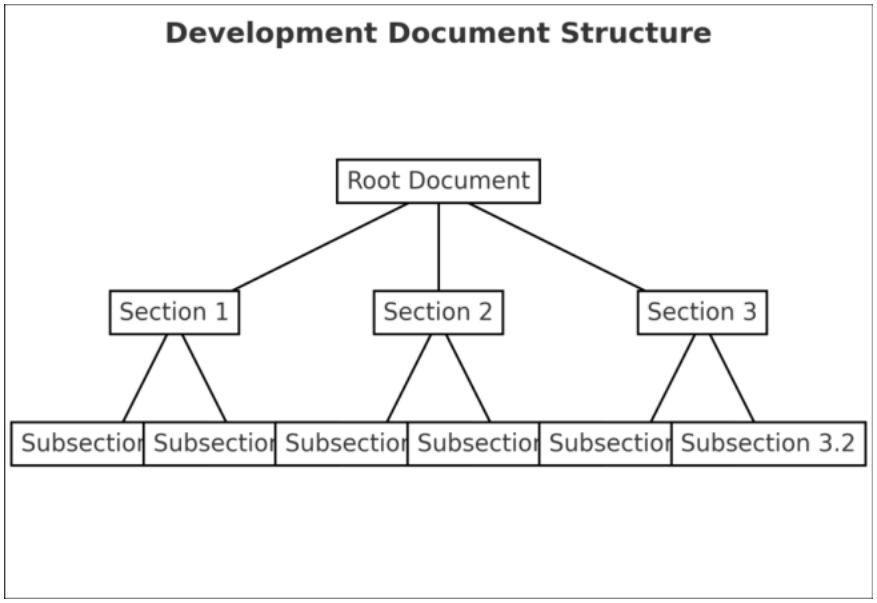


Figure 3-253 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-338 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

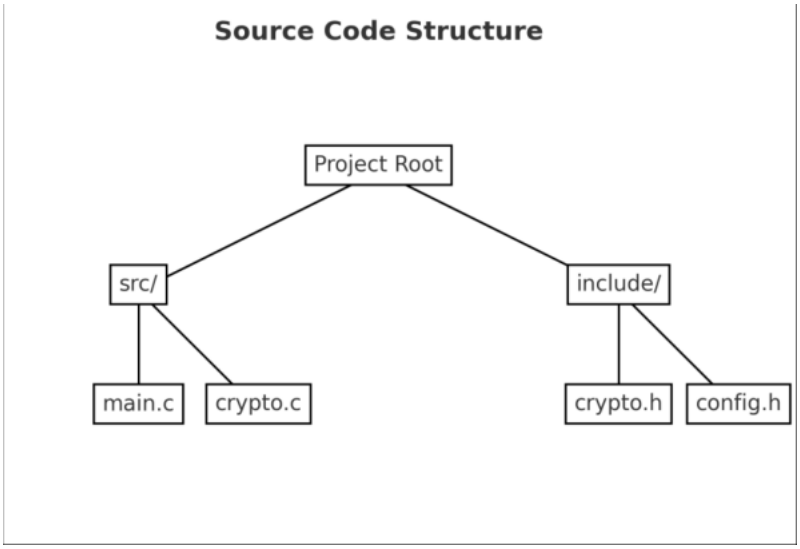


Figure 3-254 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-339 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

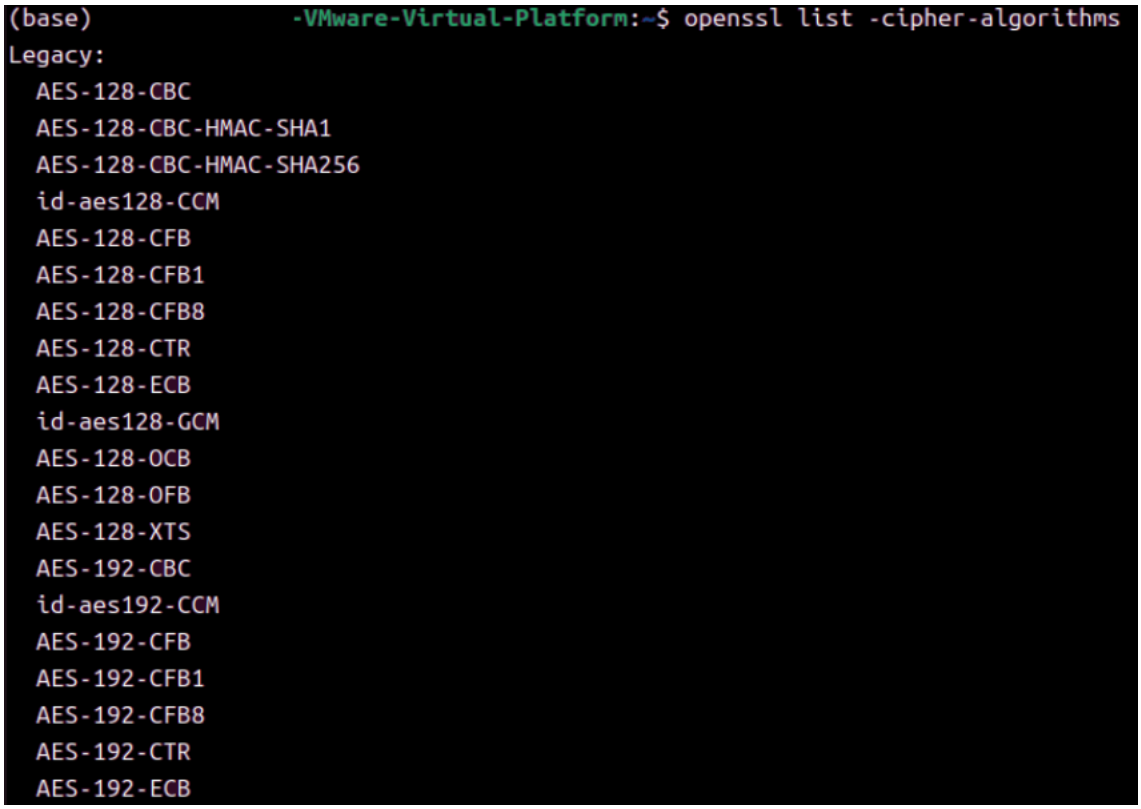


Figure 3-255 그림 제목

5.10.3 판정근거

Table 3-340 TE06.08.01 시험결과 판정근거

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

5.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.11 TE06.08.02

5.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.08.02	설명서나 관리적 절차가 아닌 암호모듈 자체에 의해 수행	개발문서 검토

5.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-341 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

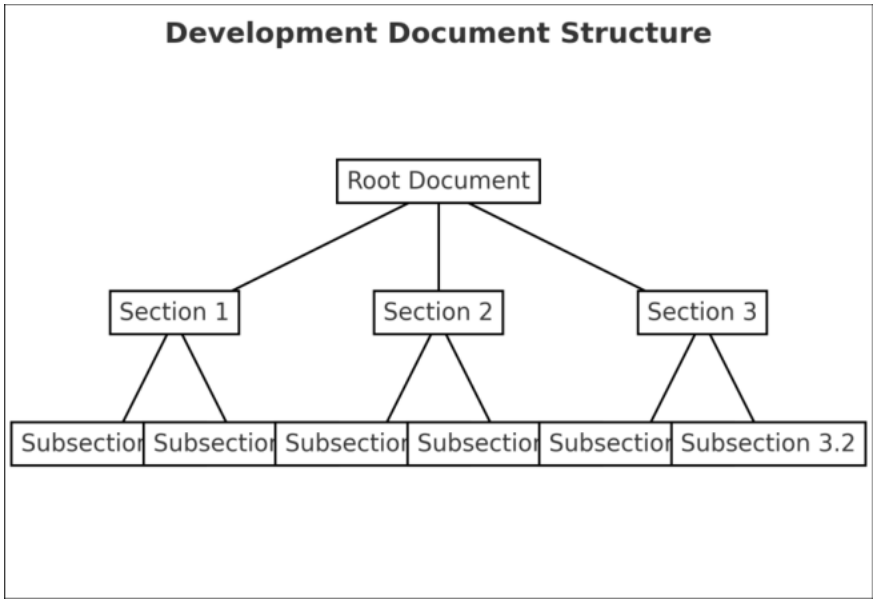


Figure 3-256 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-342 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

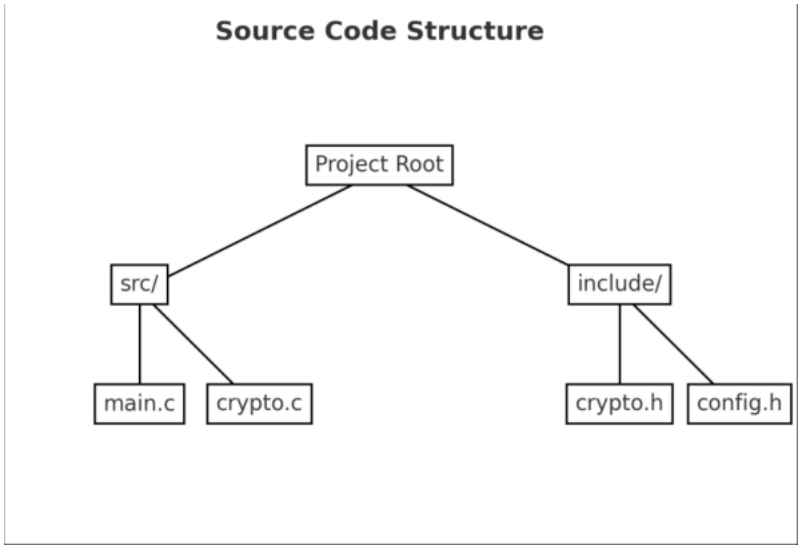


Figure 3-257 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-343 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

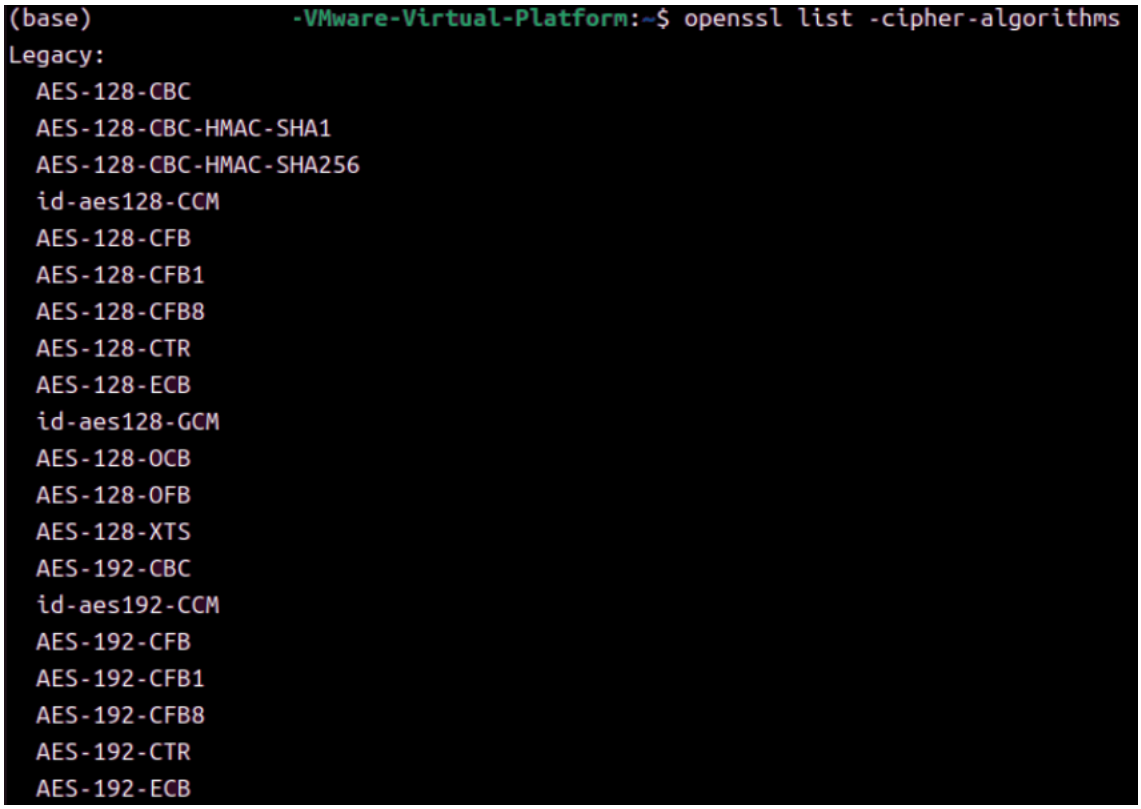


Figure 3-258 그림 제목

5.11.3 판정근거

Table 3-344 TE06.08.02 시험결과 판정근거

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

5.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

5.12 TE06.08.03

5.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE06.08.03	암호모듈이 생성한 프로세스에 대해 소유권 확보 시도	암호모듈 검사

5.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-345 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

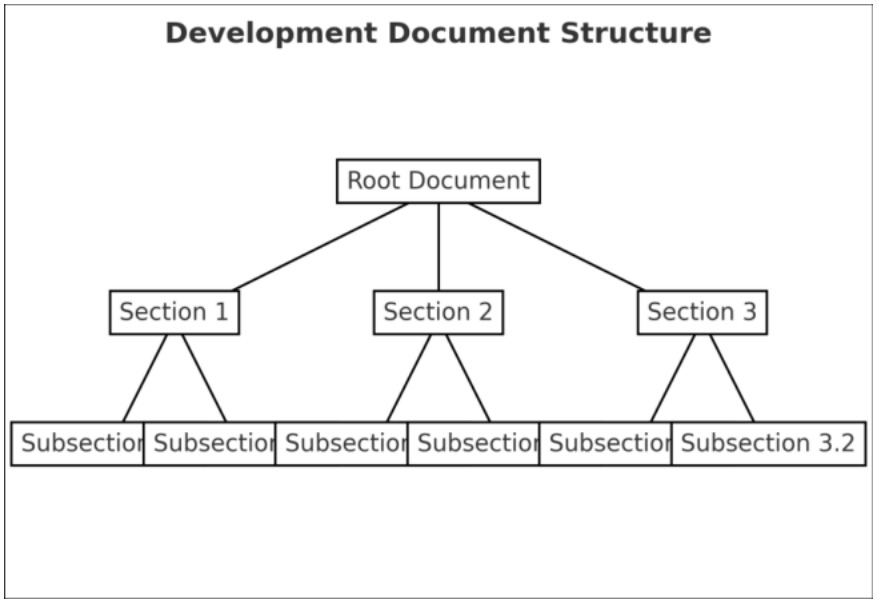


Figure 3-259 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-346 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

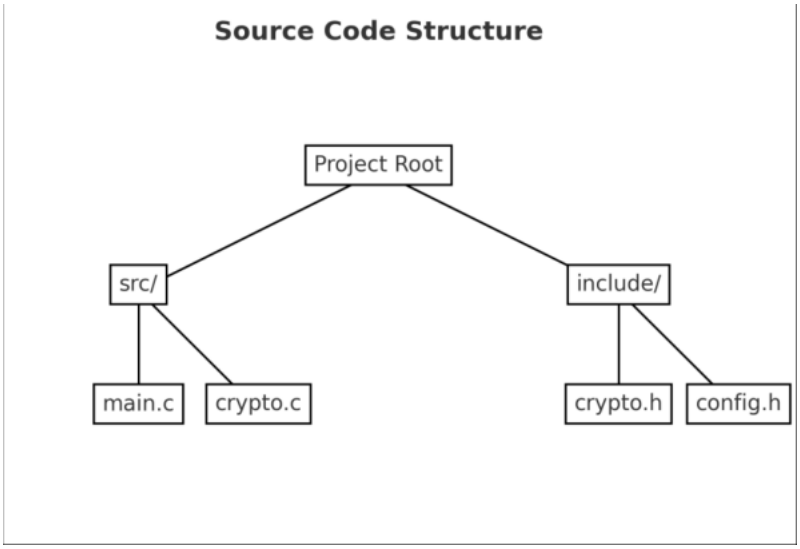


Figure 3-260 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-347 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

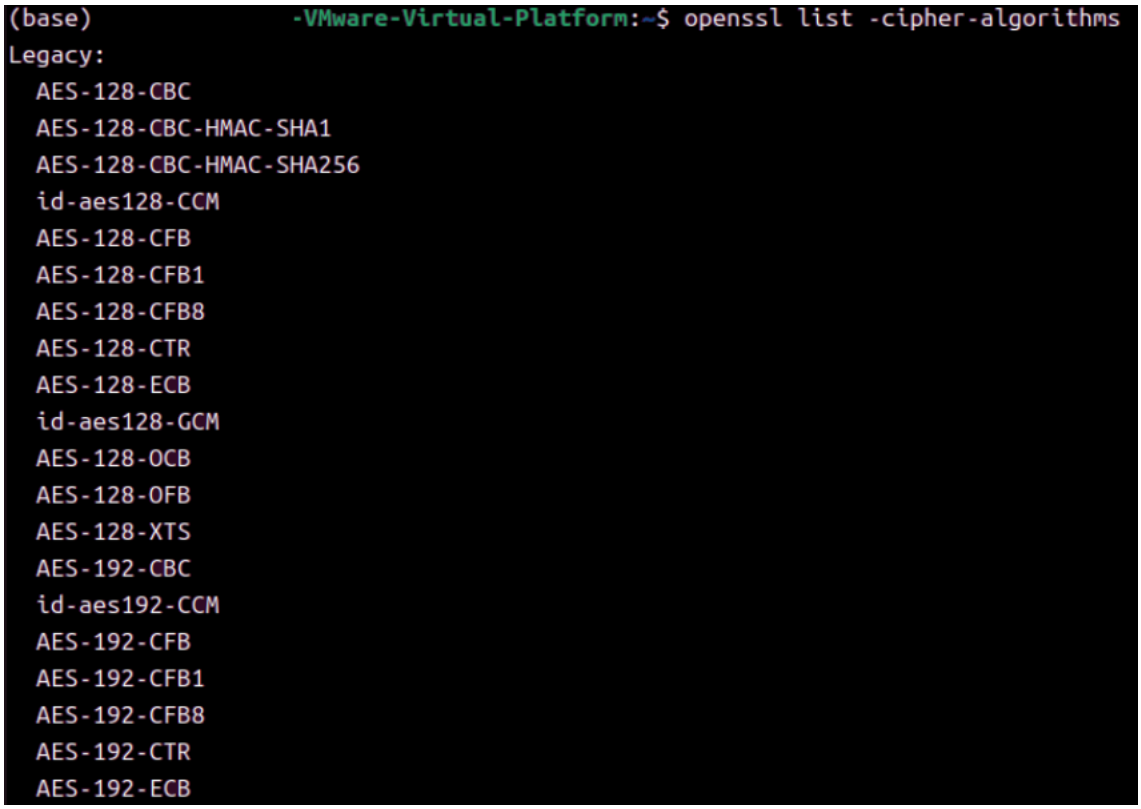


Figure 3-261 그림 제목

5.12.3 판정근거

Table 3-348 TE06.08.03 시험결과 판정근거

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

5.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6. 중요 보안매개변수 관리 (AS09)

□ 중요보안매개변수 (SSP) 는 핵심보안매개변수 (CSP) 와 공개보안매개변수 (PSP) 로 구분된다 .

□ 핵심보안매개변수는 인가되지 않은 접근 , 사용 , 노출 , 변경 및 대체에 보호가 필요하다 .

□ 공개보안매개변수는 인가되지 않은 변경 및 대체에 대한 보호가 필요하다 .

6.1 AS09 시험항목

AS	TE	확인사항
AS09.01	1, 2, 3	CSP 에 대한 보호방법
AS09.02	1, 2	PSP 에 대한 보호방법
AS09.04	1	난수발생기의 상태 정보 , 키 생성 중간 값의 CSP 간주
AS09.05	1	개발문서의 최소 문서 요구사항 만족 여부
AS09.06	1, 2, 3	검증대상 난수발생기 사용
AS09.07	1	엔트로피 입력으로 생성된 데이터의 CSP 간주
AS09.08	1, 2	엔트로피 연산량
AS09.09	1, 2	SSP 생성방법
AS09.10	1, 2	자동화된 SSP 설정
AS09.19	1, 2	CSP, 키 요소 및 인증 데이터 평문 또는 암호화 입 · 출력
AS09.29	1, 2	제로화된 SSP 복구 불가능

6.3 TE09.01.01

6.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.01.01	CSP 비인가 접근 , 사용 , 노출 , 변경 , 대체 보호	개발문서 검토

6.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-349 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

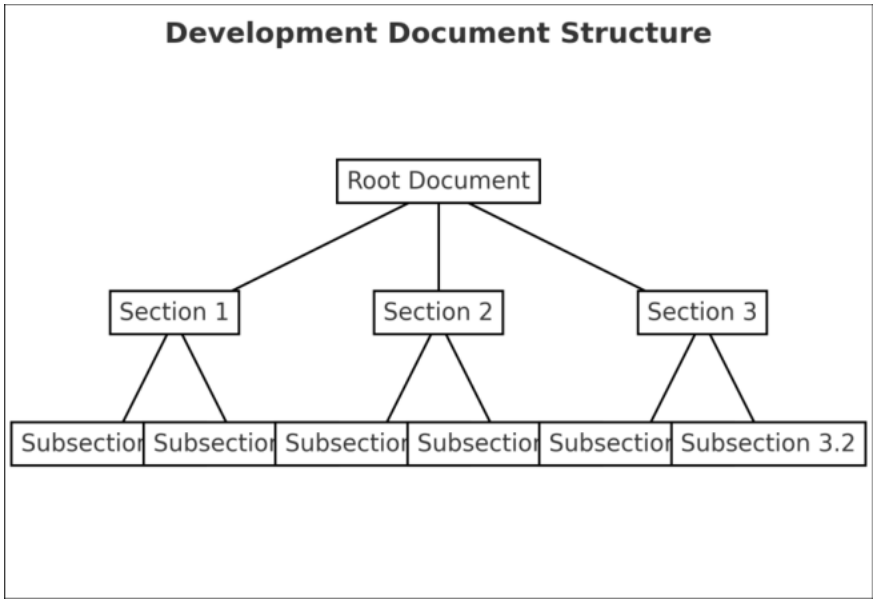


Figure 3-262 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-350 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

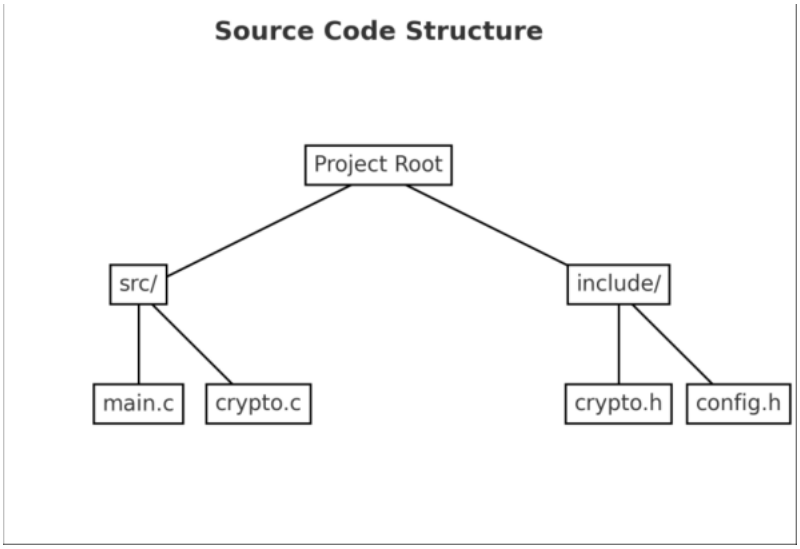


Figure 3-263 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-351 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

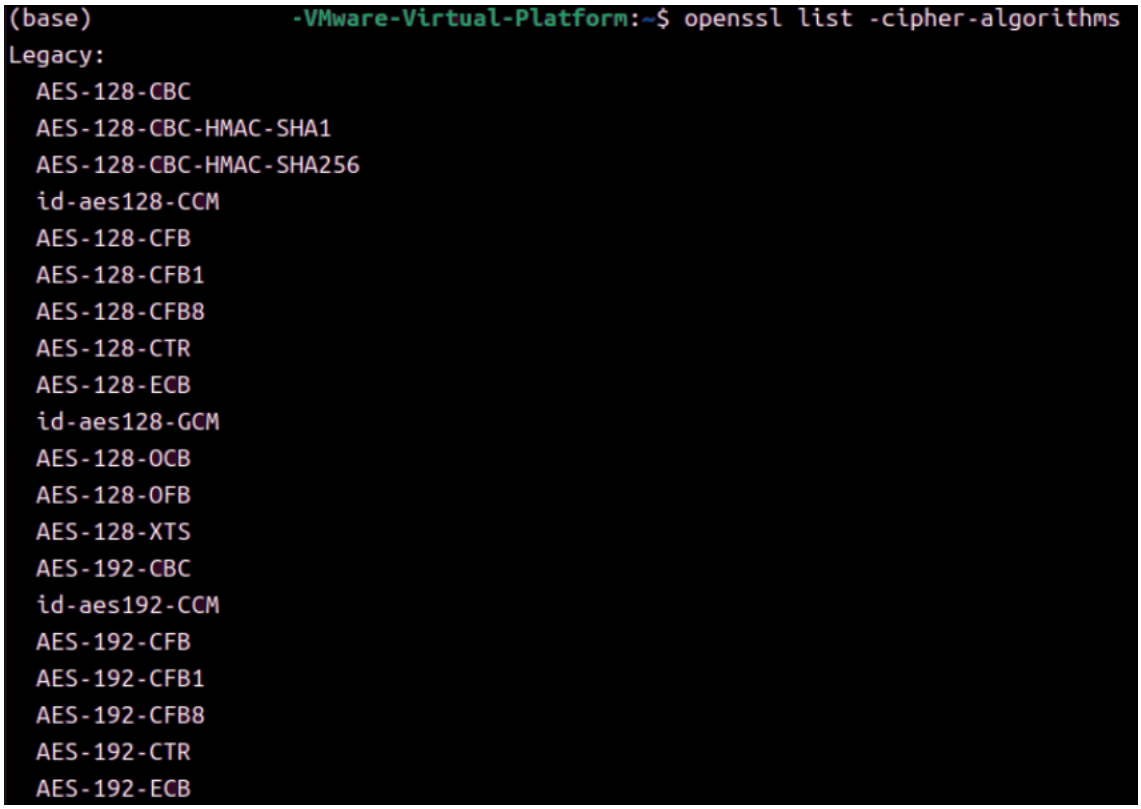


Figure 3-264 그림 제목

6.3.3 판정근거

Table 3-352 TE09.01.01 시험결과 판정근거

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

6.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.4 TE09.01.02

6.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.01.02	CSP 보호 메커니즘 우회 접근 거부	소스코드 검토 , 암호모듈 검사

6.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-353 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

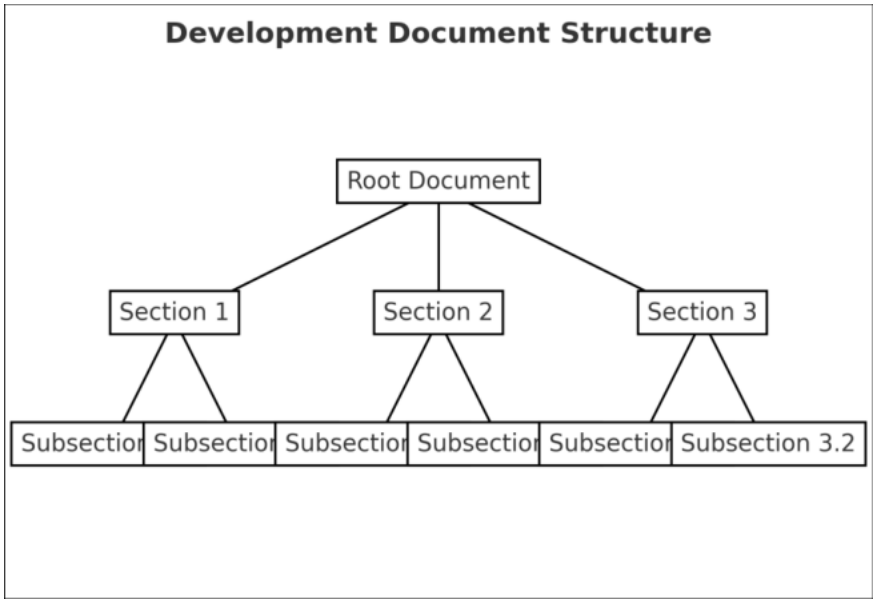


Figure 3-265 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-354 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

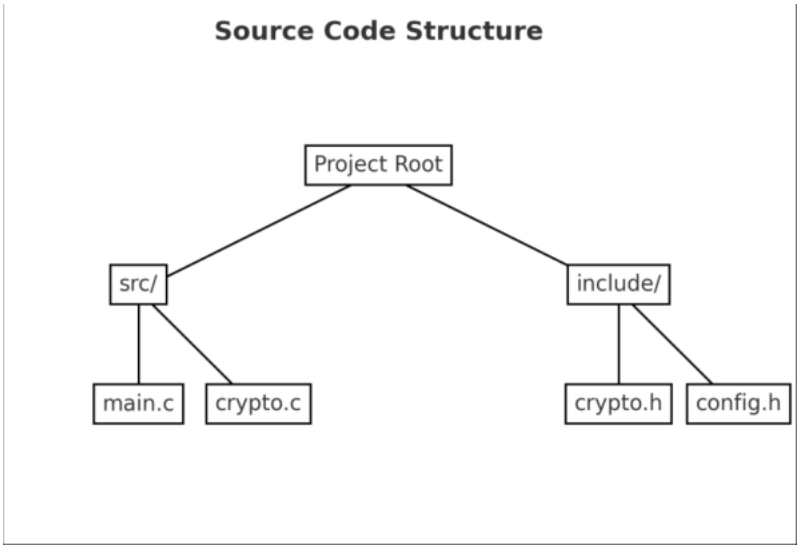


Figure 3-266 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-355 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

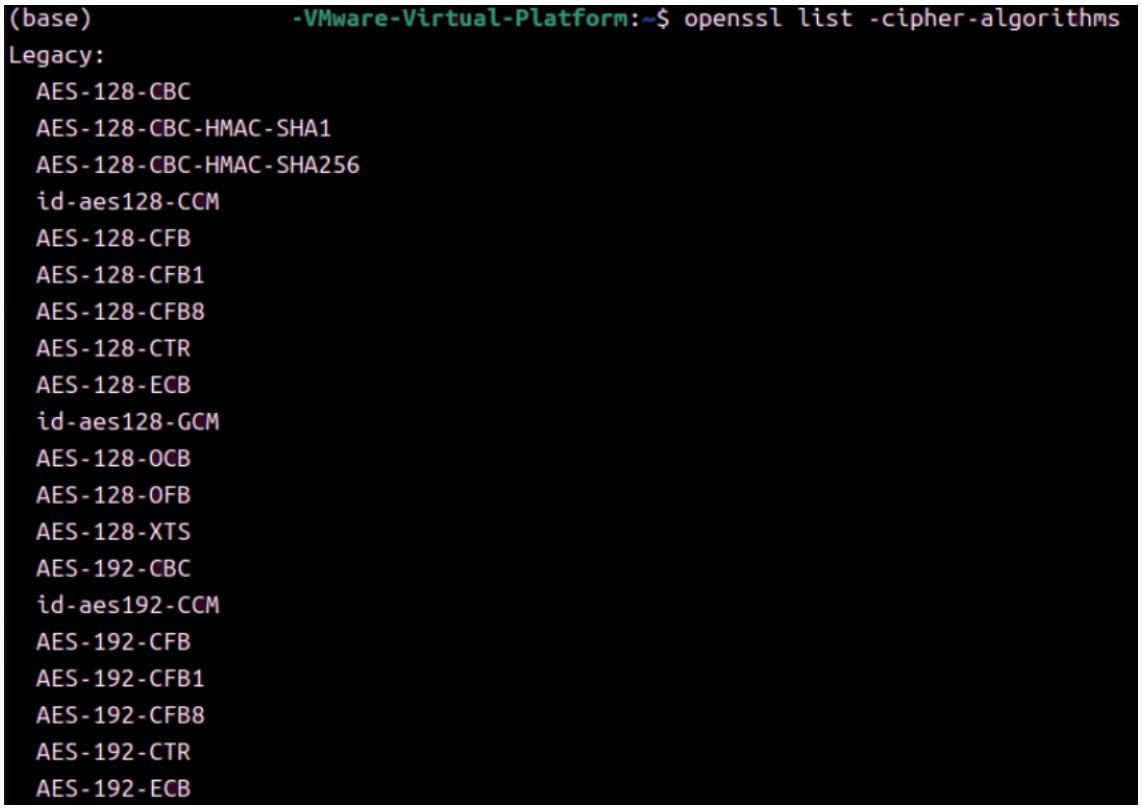


Figure 3-267 그림 제목

6.4.3 판정근거

Table 3-356 TE09.01.02 시험결과 판정근거

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

6.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.5 TE09.01.03

6.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.01.03	명세되지 않은 방법으로 CSP 변경 보호	소스코드 검토 , 암호모듈 검사

6.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-357 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

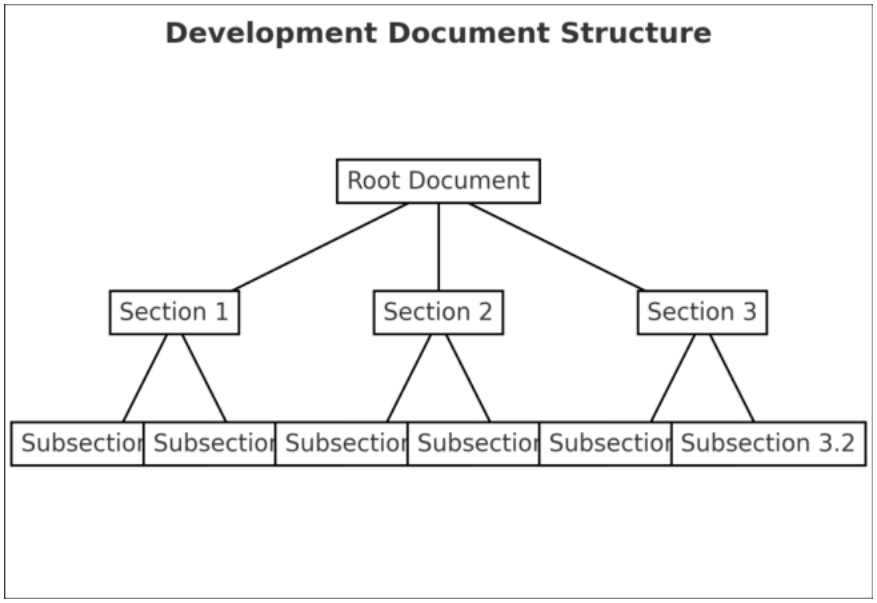


Figure 3-268 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-358 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

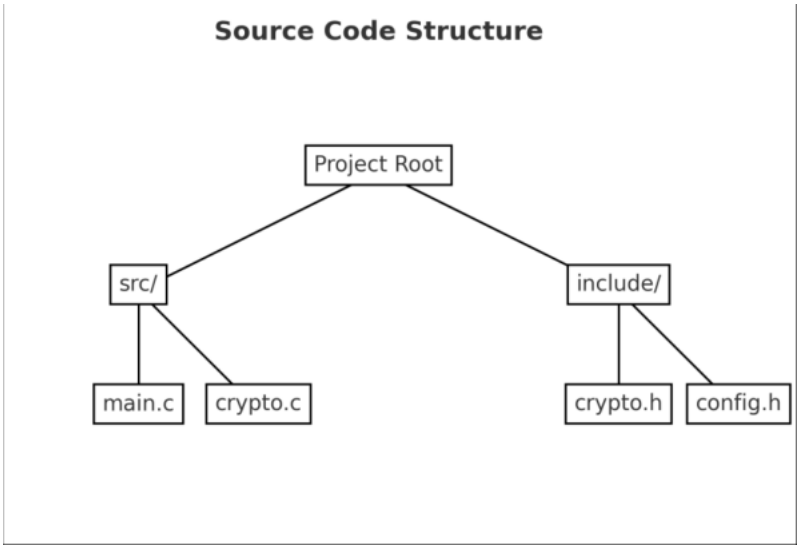


Figure 3-269 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-359 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

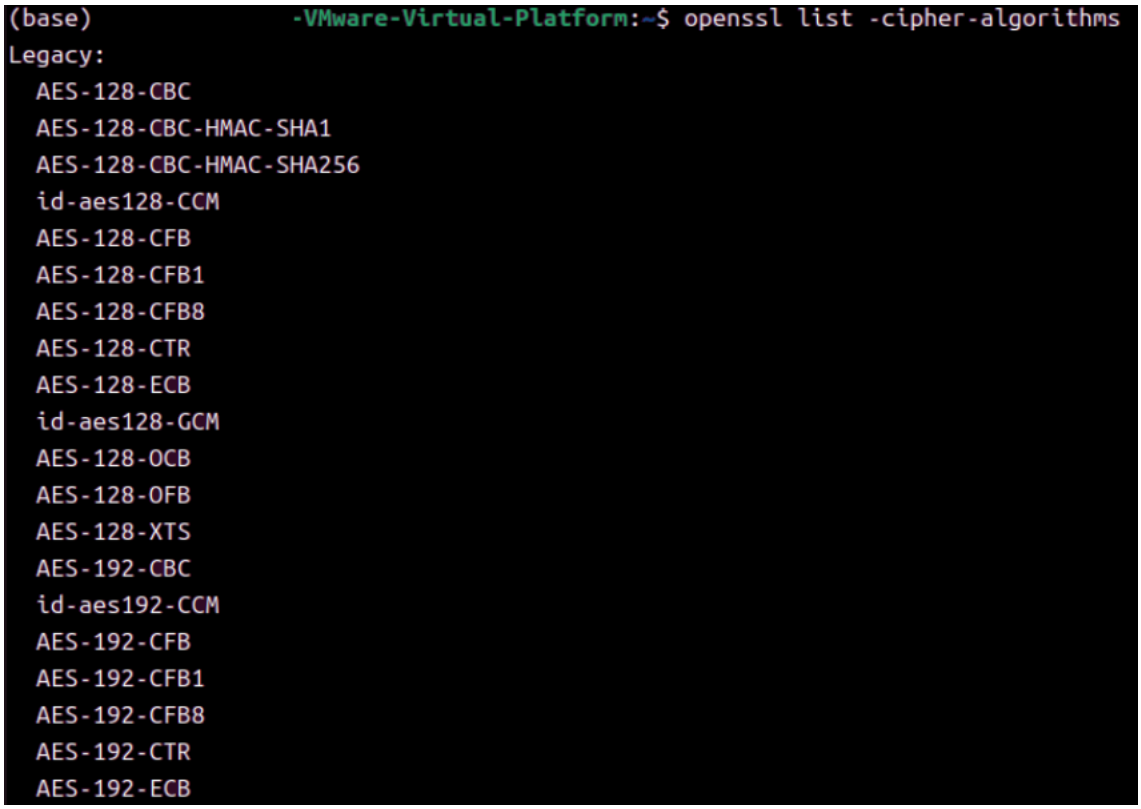


Figure 3-270 그림 제목

6.5.3 판정근거

Table 3-360 TE09.01.03 시험결과 판정근거

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

6.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.6 TE09.02.01

6.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.02.01	PSP 비인가 변경 , 대체 보호	개발문서 검토

6.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-361 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

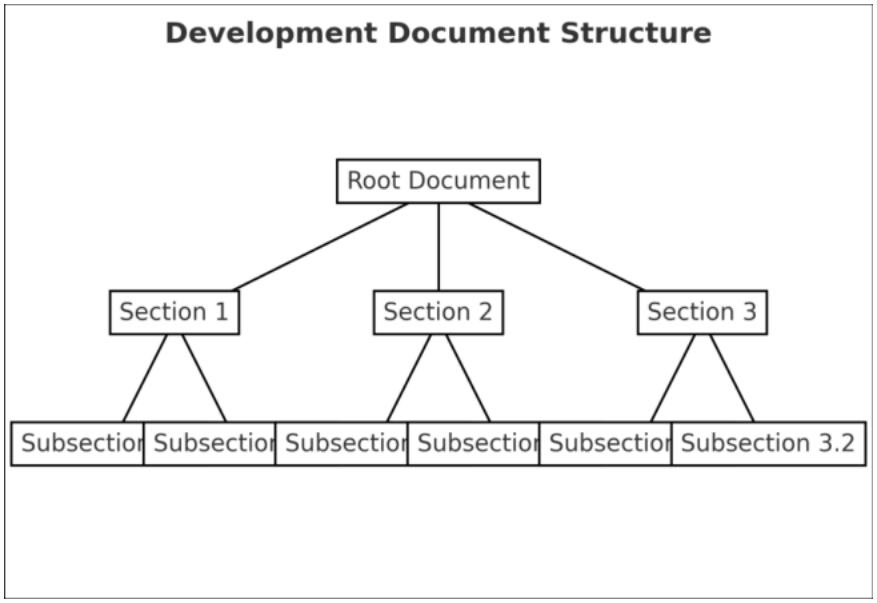


Figure 3-271 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-362 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

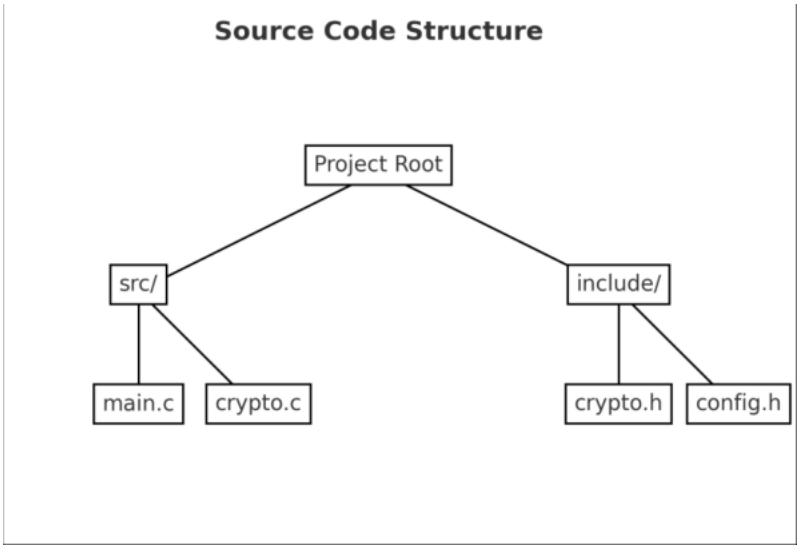


Figure 3-272 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-363 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

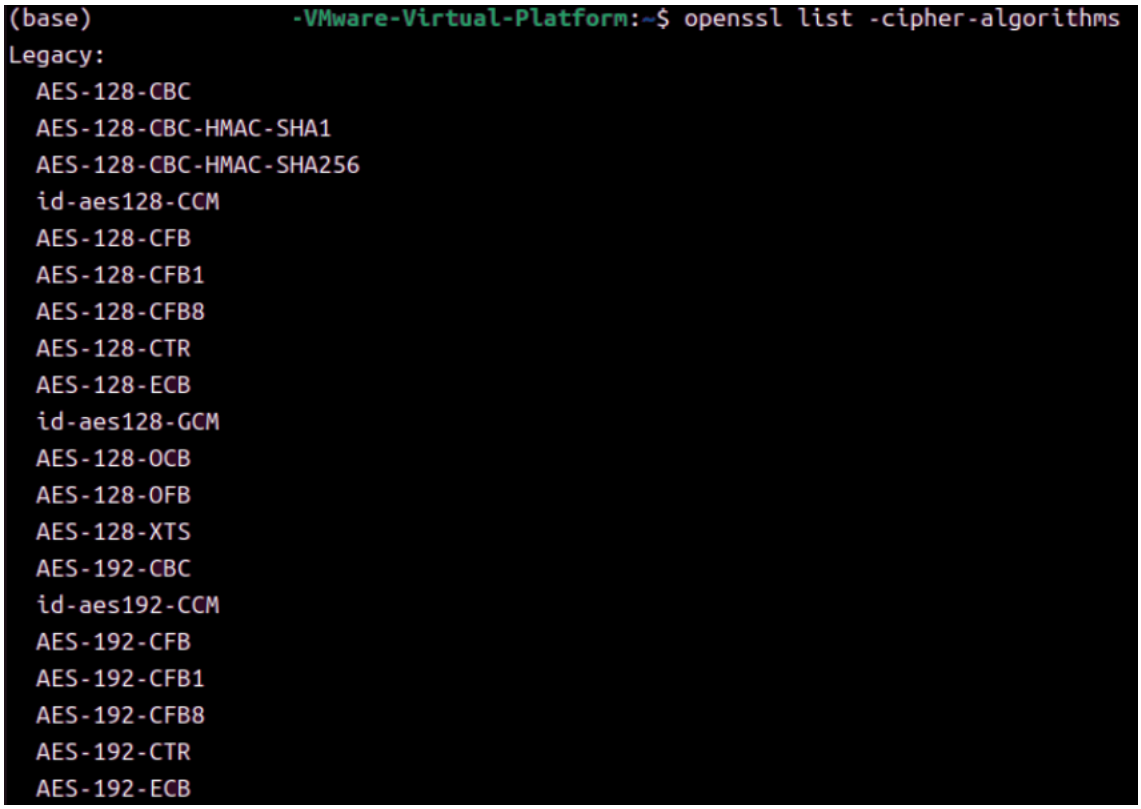


Figure 3-273 그림 제목

6.6.3 판정근거

Table 3-364 TE09.02.01 시험결과 판정근거

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

6.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.7 TE09.02.02

6.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.02.02	명세되지 않은 방법으로 PSP 변경 보호	소스코드 검토 , 암호모듈 검사

6.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-365 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

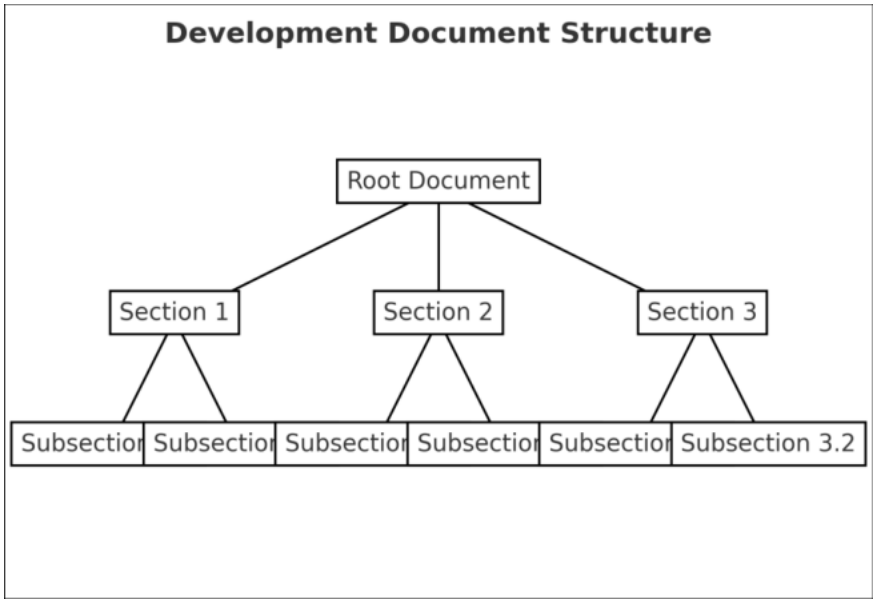


Figure 3-274 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-366 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

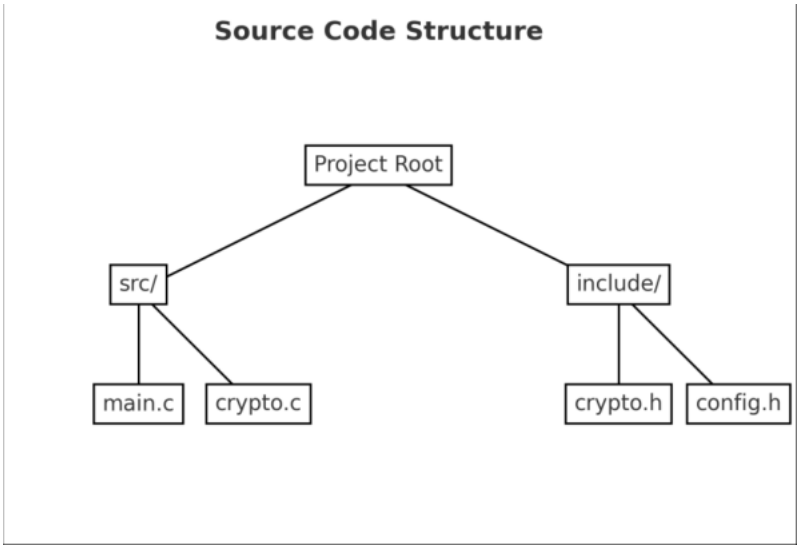


Figure 3-275 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-367 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

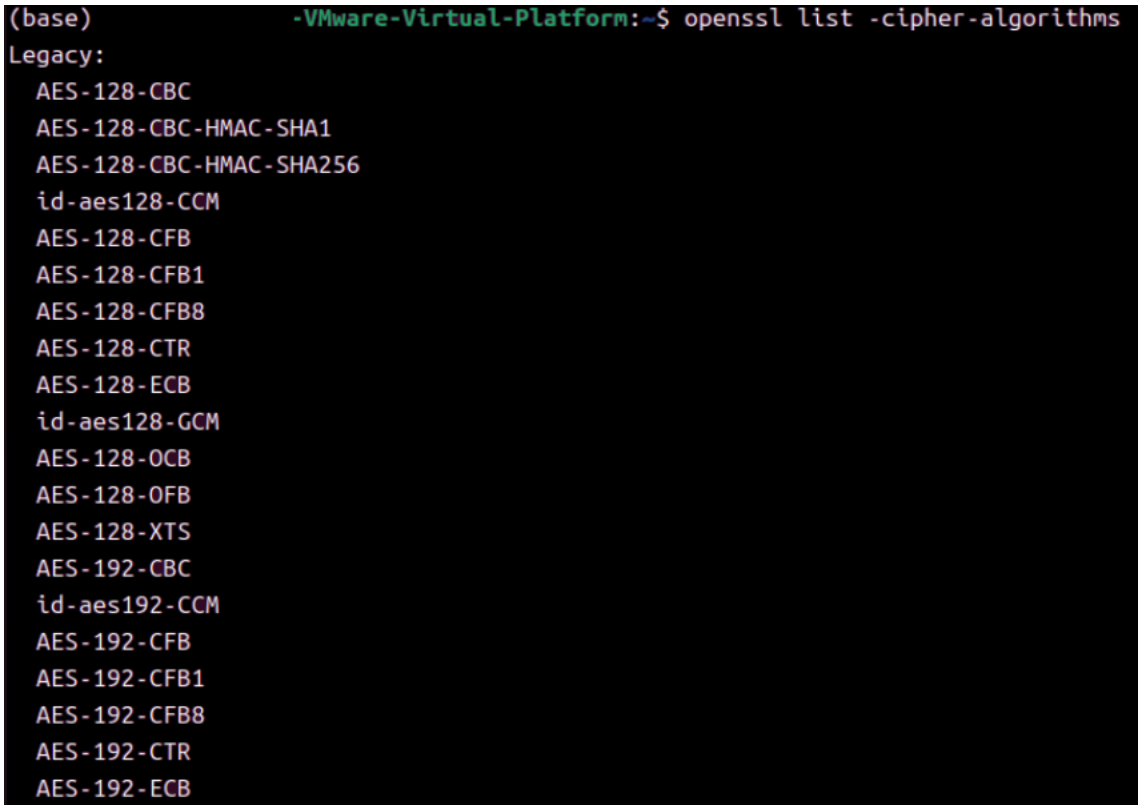


Figure 3-276 그림 제목

6.7.3 판정근거

Table 3-368 TE09.02.02 시험결과 판정근거

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

6.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.8 TE09.04.01

6.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.04.01	패스워드 해시값 , 난수발생기 상태 정보 , 키 생성 중간값의 CSP 간주	개발문서 검토 , 소스코드 검토 , 암호모듈 검사

6.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-369 표 제목

유형		중요보안매개변수	생성	합의	주입	출력	저장	제로화
블록암호	CSP	비밀키 및 라운드키	○	X	X	X	X	○
	PSP	IV 및 CTR	○	X	X	X	X	○
메시지인증	CSP	비밀키	○	X	X	X	X	○
난수발생기	CSP	엔트로피 입력	○	X	X	X	X	○
	CSP	내부상태 (V, C)	○	X	X	X	X	○
공개키 암호	CSP	개인키 파라미터 (d, p, q, dP, dQ, qInv)	○	X	X	X	X	○

전자서명	CSP	시드	○	X	X	X	X	○
	PSP	공개키 파라미터 (e, n)	○	X	X	X	X	○
	CSP	서명키 파라미터 (d, p, q, dP, dQ, qInv)	○	X	X	X	X	○
	CSP	솔트	○	X	X	X	X	○
	PSP	검증키 파라미터 (e, n)	○	X	X	X	X	○

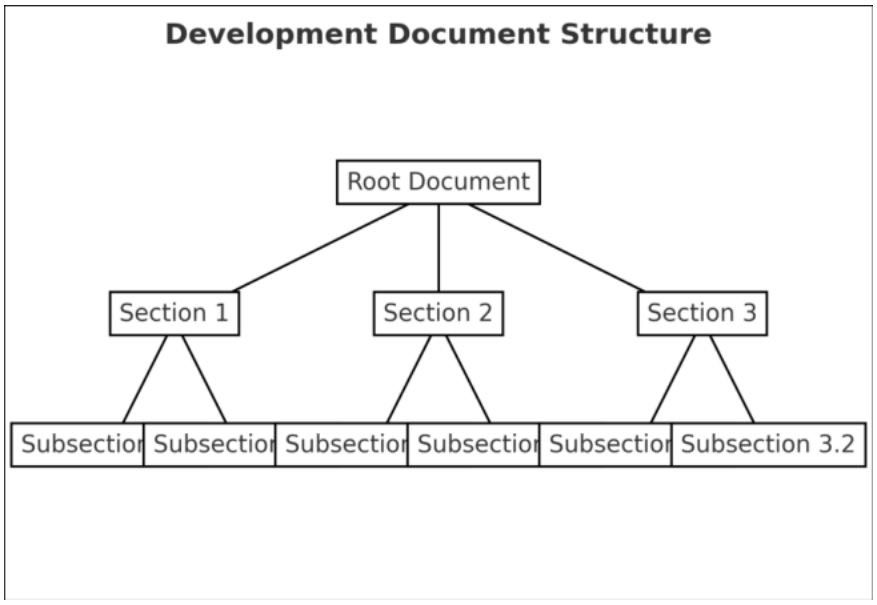


Figure 3-277 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-370 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

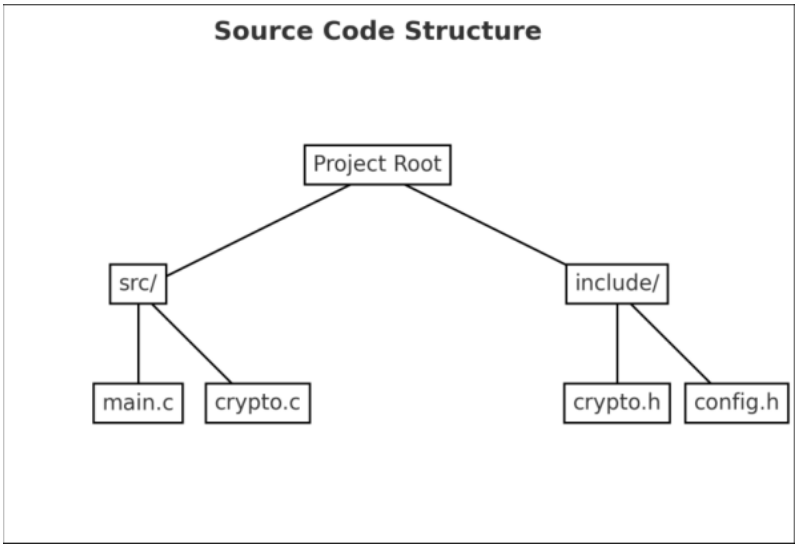


Figure 3-278 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-371 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

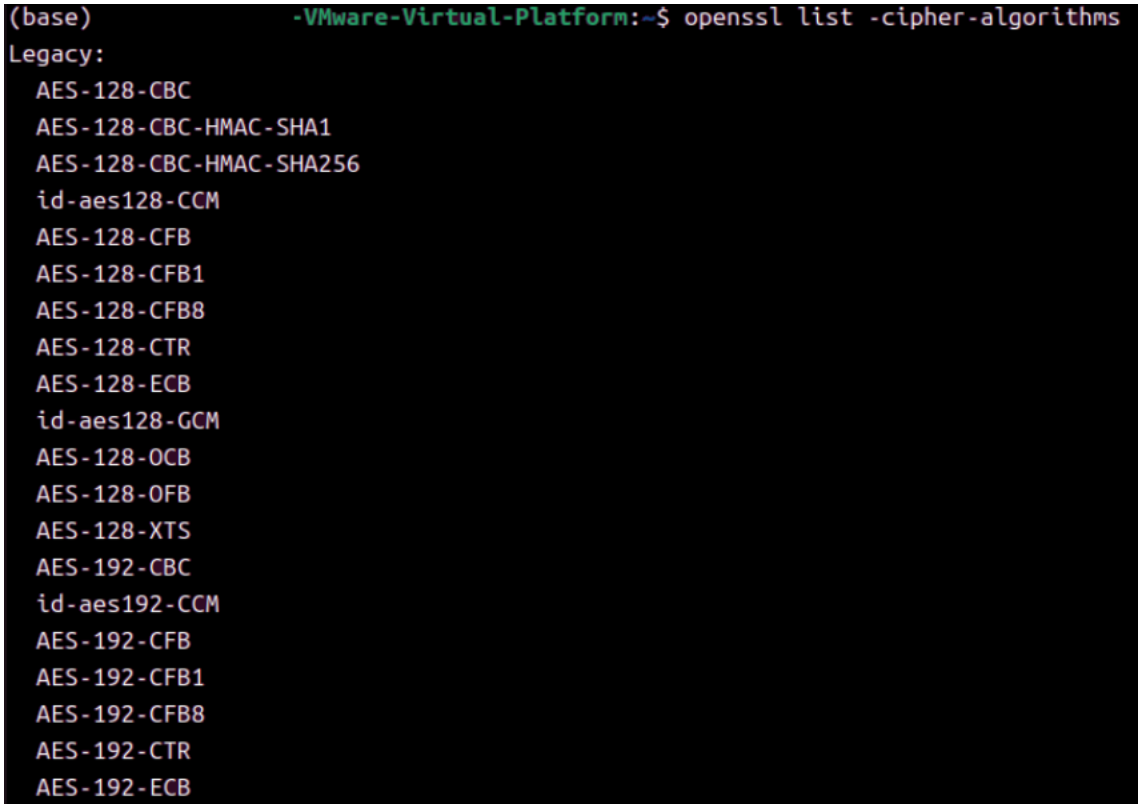


Figure 3-279 그림 제목

6.8.3 판정근거

Table 3-372 TE09.04.01 시험결과 판정근거

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

6.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.9 TE09.05.01

6.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.05.01	KS X ISO/IEC 19790 A.2.9 요구사항 충족하는 개발문서 제공	개발문서 검토

6.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-373 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

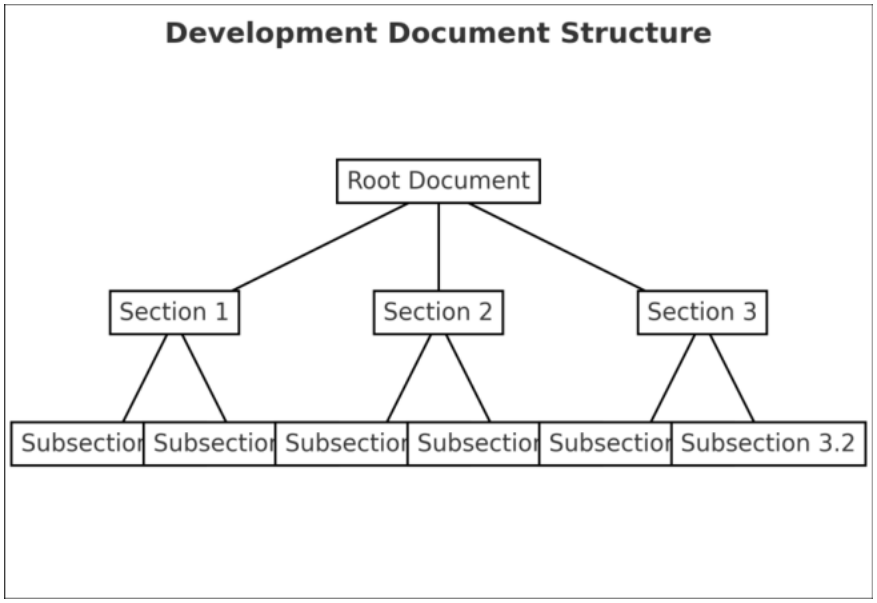


Figure 3-280 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-374 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

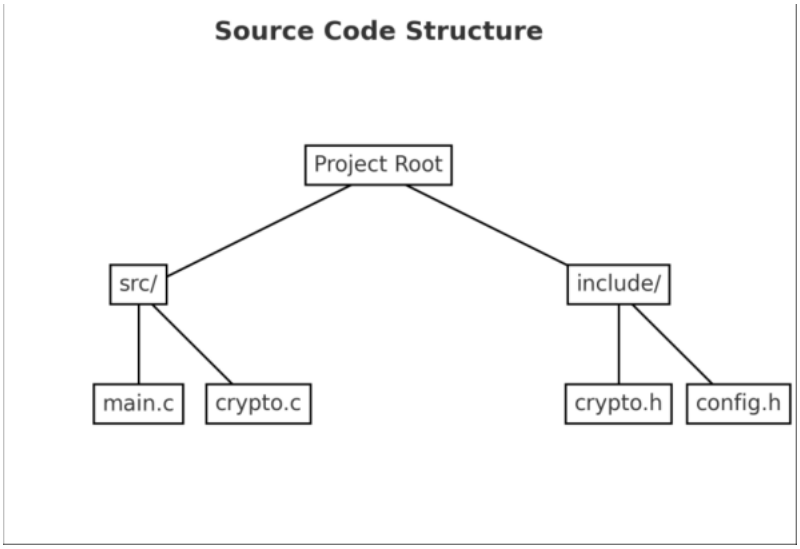


Figure 3-281 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-375 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

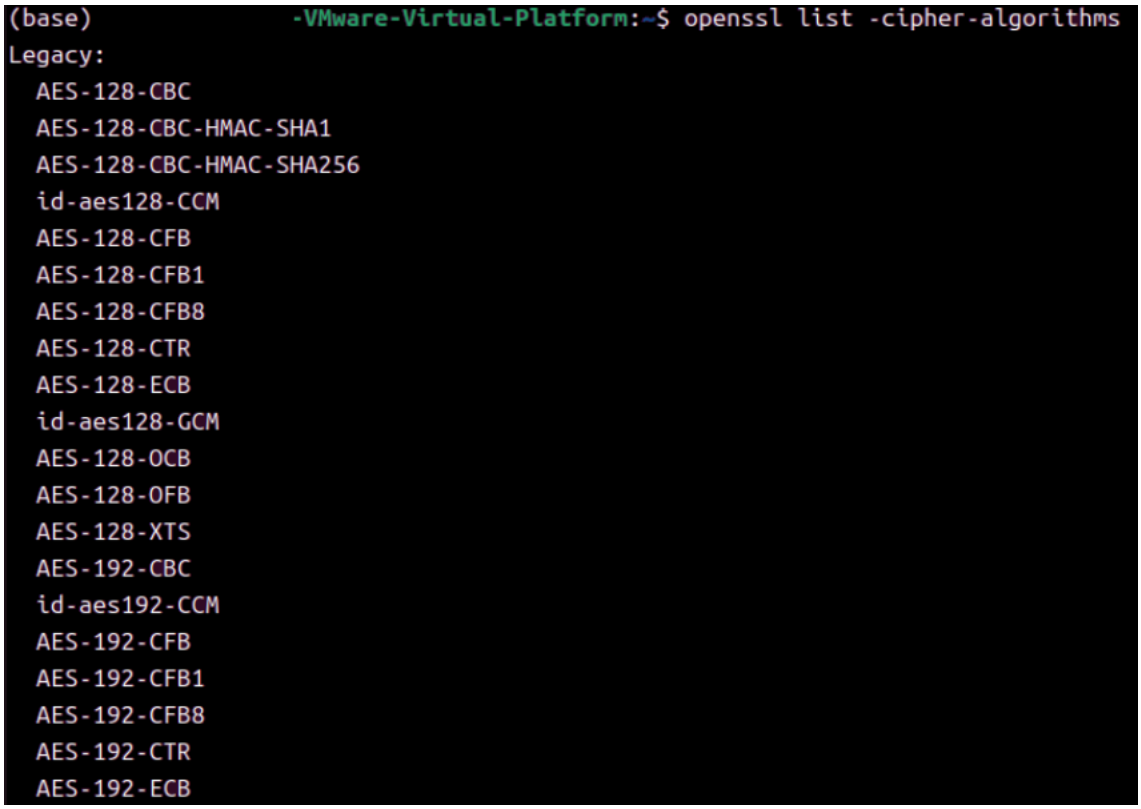


Figure 3-282 그림 제목

6.9.3 판정근거

Table 3-376 TE09.05.01 시험결과 판정근거

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

6.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.10 TE09.06.01

6.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.06.01	사용된 모든 난수발생기 및 사용법 명세	개발문서 검토

6.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-377 표 제목

난수발생기	상세 내용	용도
Hash_DRBG	- 해시 : SHA-256 - 유도함수 : 사용 - 예측내성 : 항상 지원 - 개별화 문자열 입력 : 미지원 - 추가 입력 : 미지원 - 난수 최대 출력 길이 : 2^16 바이트 이하 - 보안 강도 : 201	- 블록암호 비밀키 생성 - 블록암호 IV, CTR 생성 - 메시지 인증 비밀키 생성 - 공개키 쌍 생성 - 공개키 암호화 시드 생성 - 전자서명 키 쌍 생성 - 전자서명 서명 솔트 생성 - 난수 생성

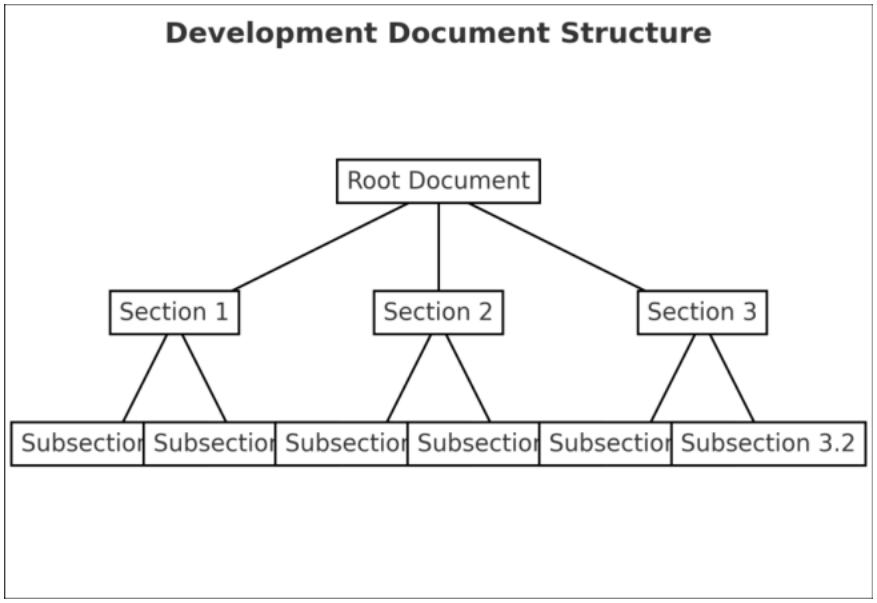


Figure 3-283 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-378 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

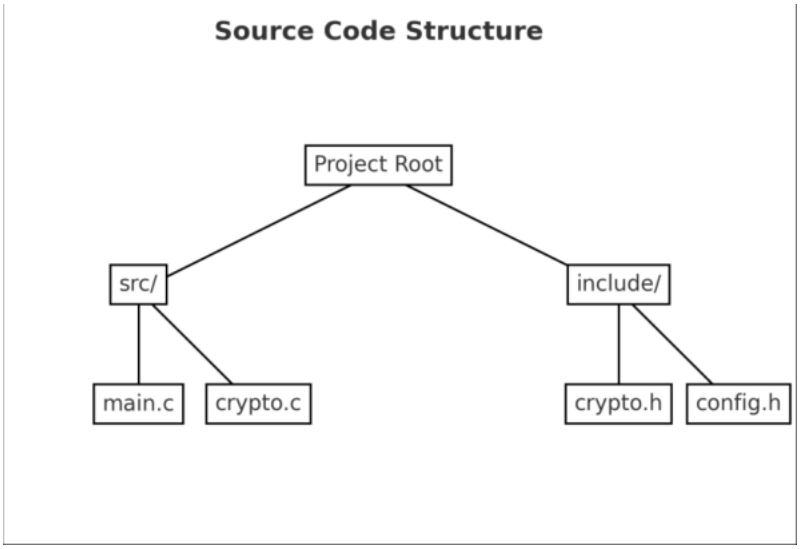


Figure 3-284 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-379 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

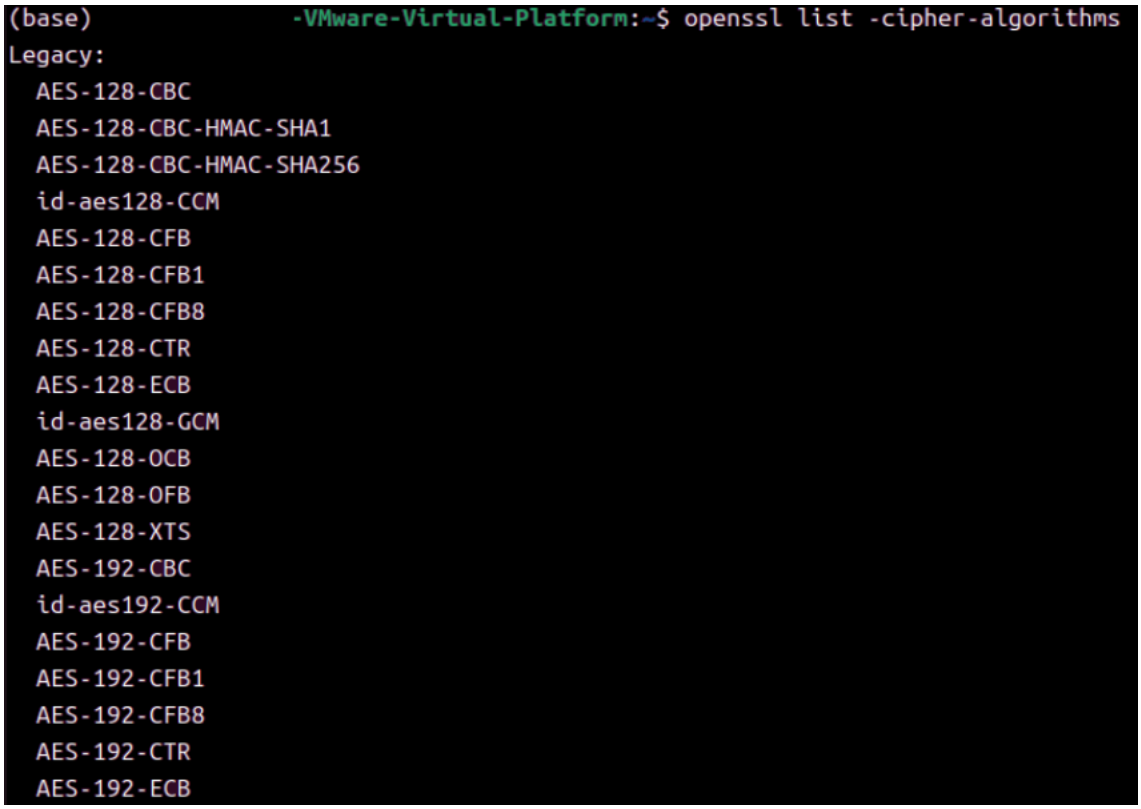


Figure 3-285 그림 제목

6.10.3 판정근거

Table 3-380 TE09.06.01 시험결과 판정근거

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

6.10.4 판정결과

판정 : <“ 통과 ” 또는 “ 실패 ”>

6.11 TE09.06.02

6.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.06.02	사용된 모든 난수발생기의 검증대상 난수발생기 목록 준수	개발문서 검토

6.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-381 표 제목

No	서비스	용도	관련 API	소스코드 정보
1				
2				
3				
4				
5				

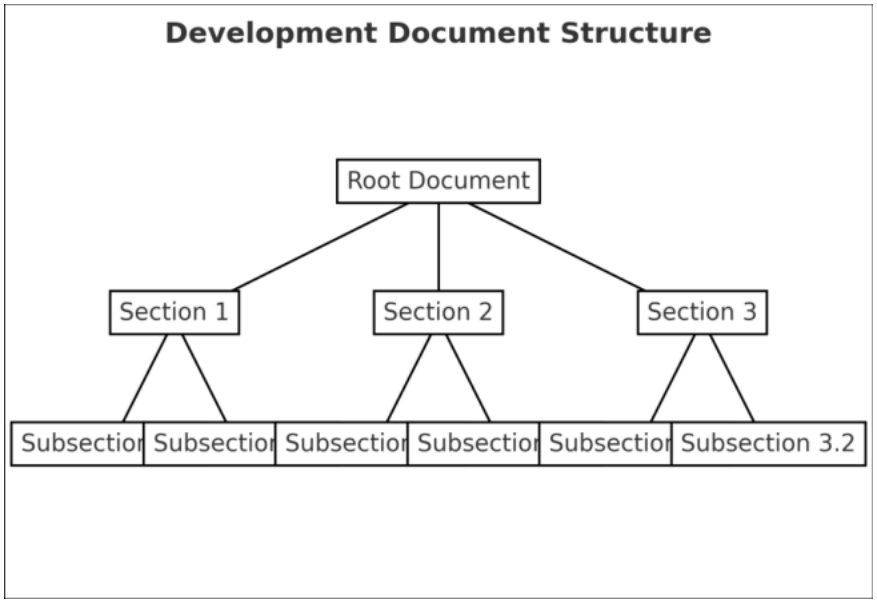


Figure 3-286 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-382 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

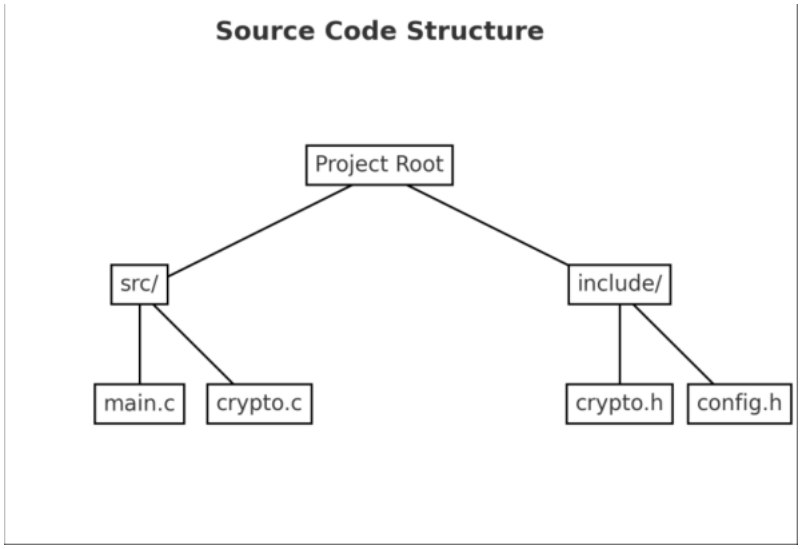


Figure 3-287 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-383 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

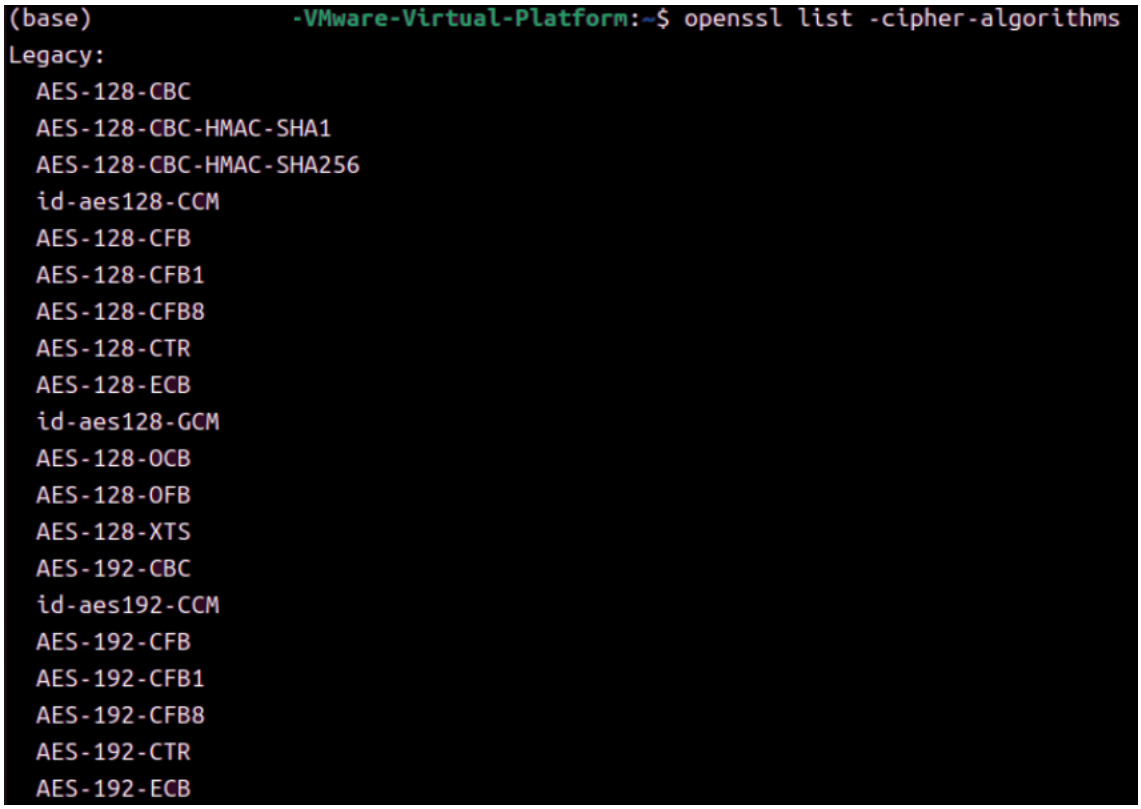


Figure 3-288 그림 제목

6.11.3 판정근거

Table 3-384 TE09.06.02 시험결과 판정근거

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

6.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.12 TE09.06.03

6.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.06.03	검증대상 난수 발생기로부터 제공된 난수 사용 여부	소스코드 검토

6.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-385 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

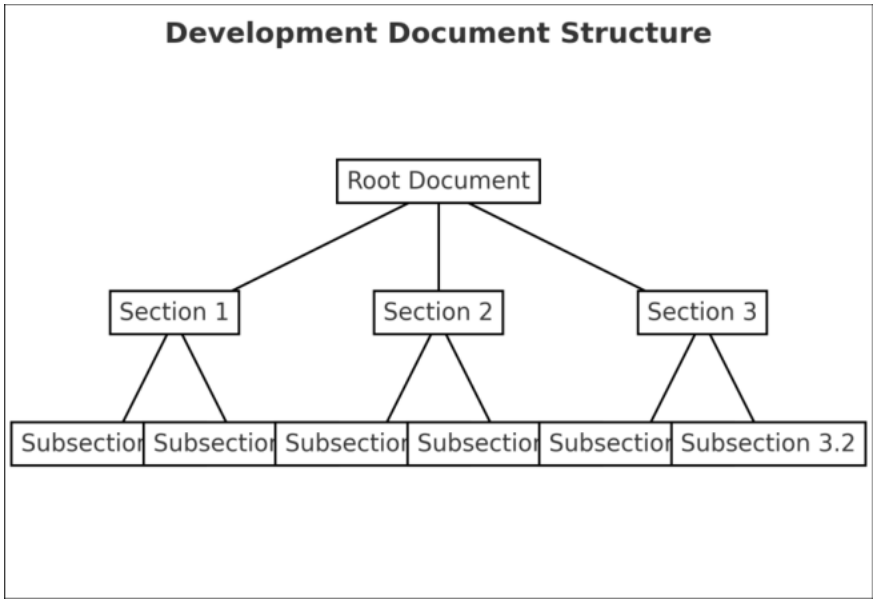


Figure 3-289 그림 제목

2) 소스코드 검토

라) 소스코드명

□ < 소스코드명 >

마) 소스코드 검토내용

□ < 개발문서 검토내용 설명 >

바) 증빙자료

□ < 증빙자료 내용 설명 >

Table 3-386 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

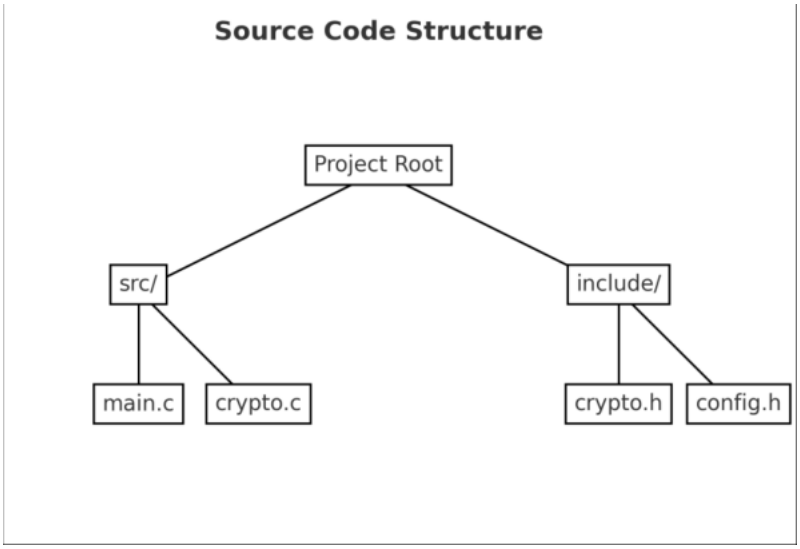


Figure 3-290 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-387 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

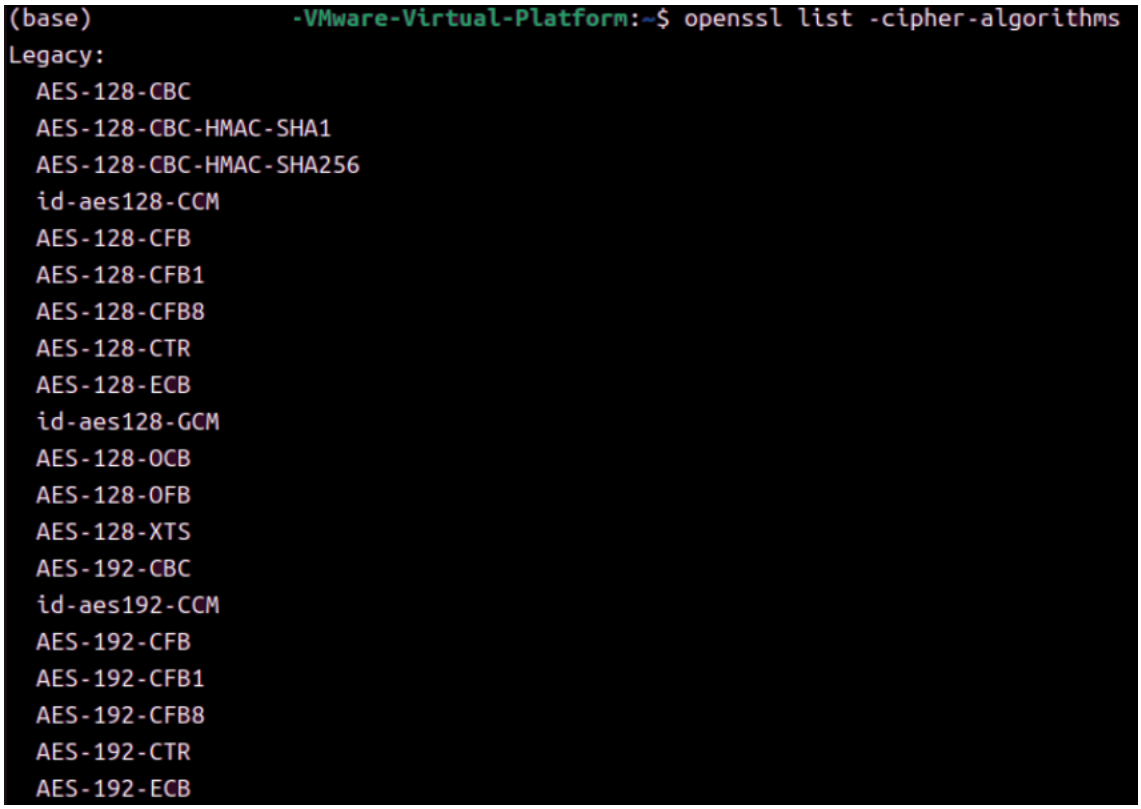


Figure 3-291 그림 제목

6.12.3 판정근거

Table 3-388 TE09.06.03 시험결과 판정근거

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

6.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.13 TE09.07.01

6.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.07.01	암호 경계 외부에서 수집된 엔트로피로 생성된 데이터의 CSP 간주	개발문서 검토

6.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-389 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

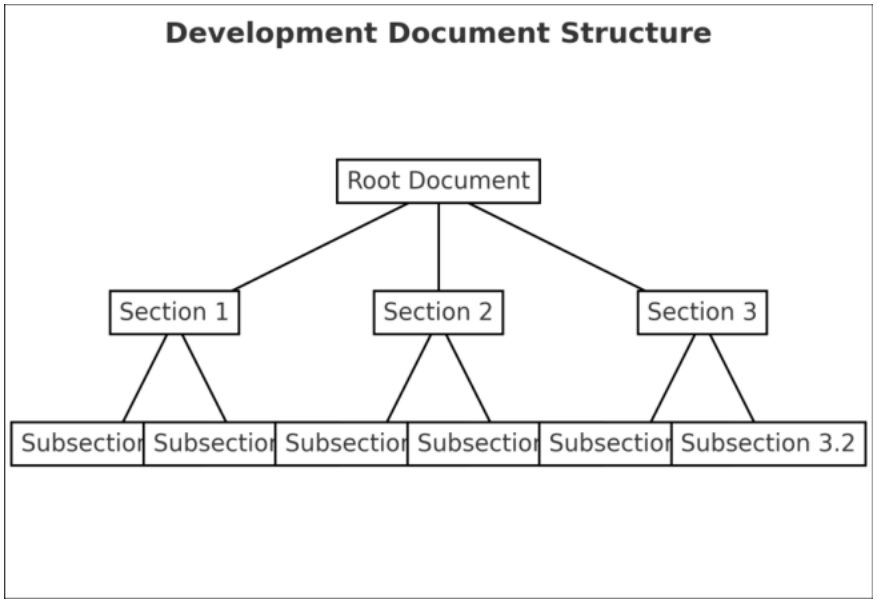


Figure 3-292 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-390 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

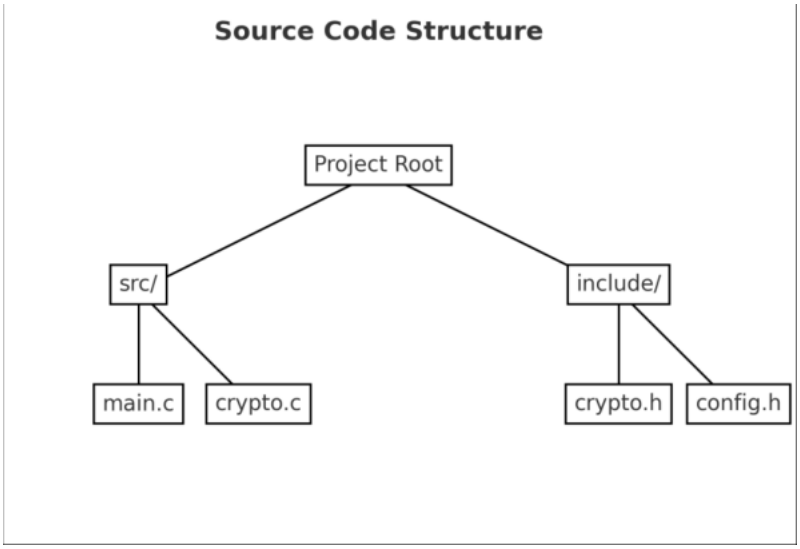


Figure 3-293 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-391 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

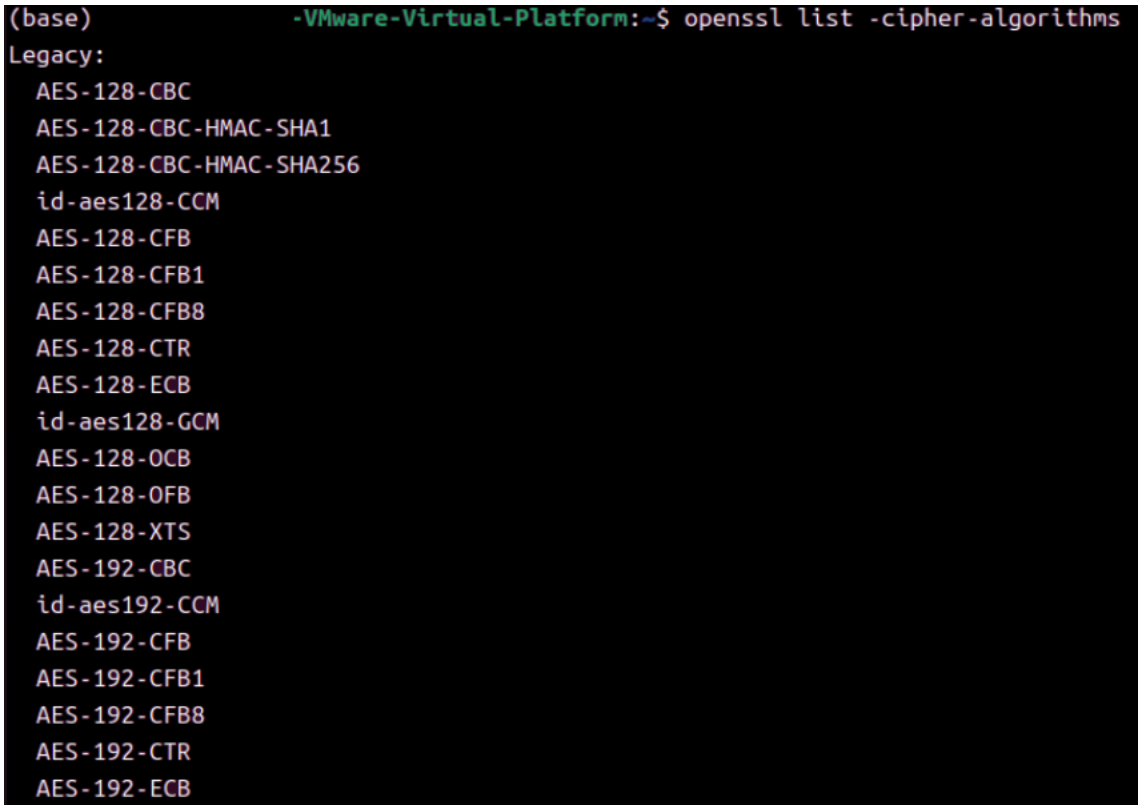


Figure 3-294 그림 제목

6.13.3 판정근거

Table 3-392 TE09.07.01 시험결과 판정근거

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

6.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.14 TE09.08.01

6.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.08.01	엔트로피 연산량 명세	개발문서 검토

6.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-393 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

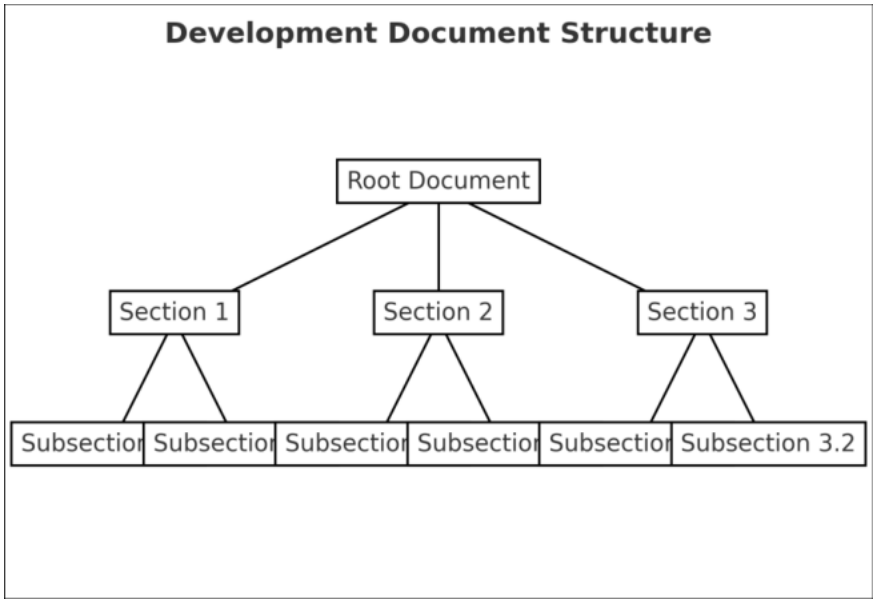


Figure 3-295 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-394 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

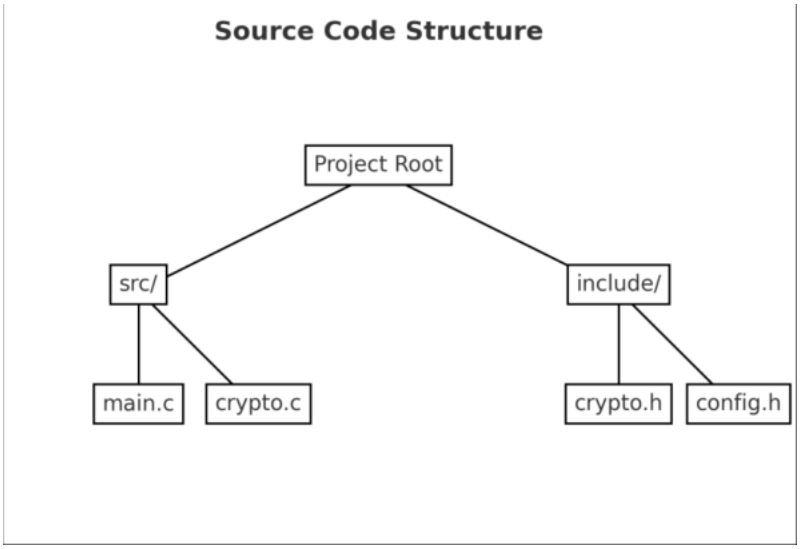


Figure 3-296 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-395 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

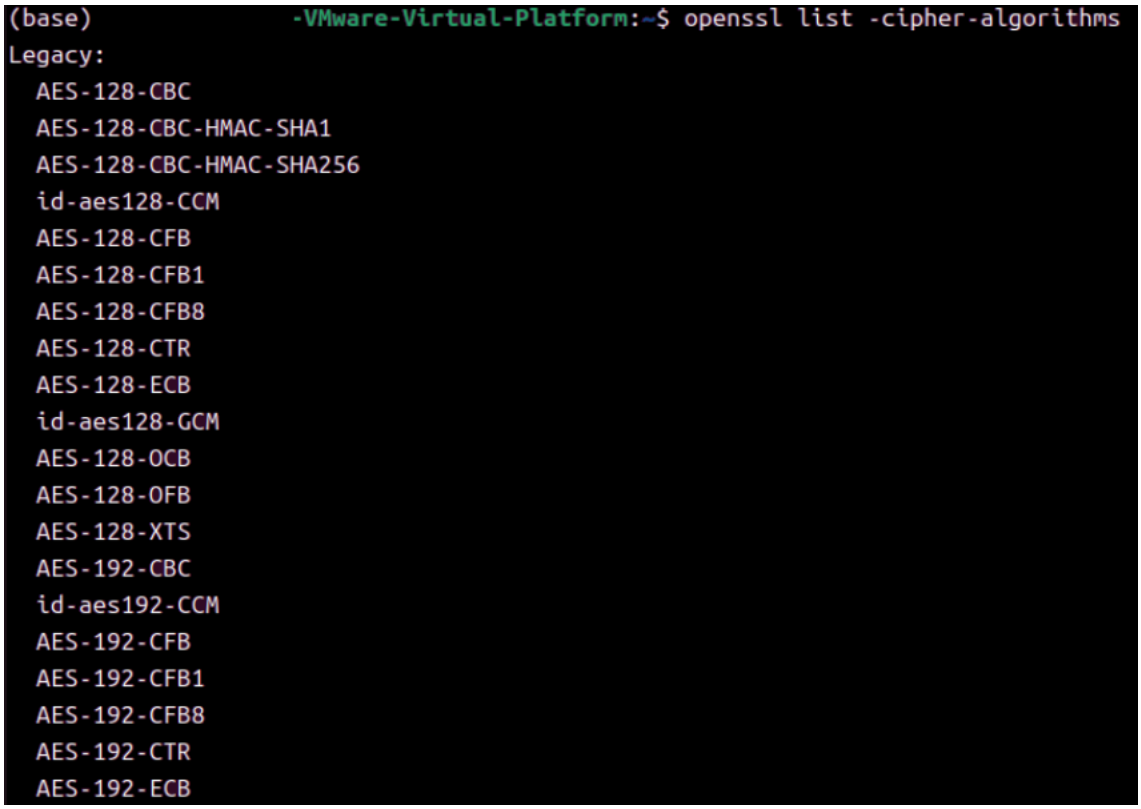


Figure 3-297 그림 제목

6.14.3 판정근거

Table 3-396 TE09.08.01 시험결과 판정근거

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

6.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.15 TE09.08.02

6.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.08.02	벤더 제공 근거의 정확성	소스코드 검토

6.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-397 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

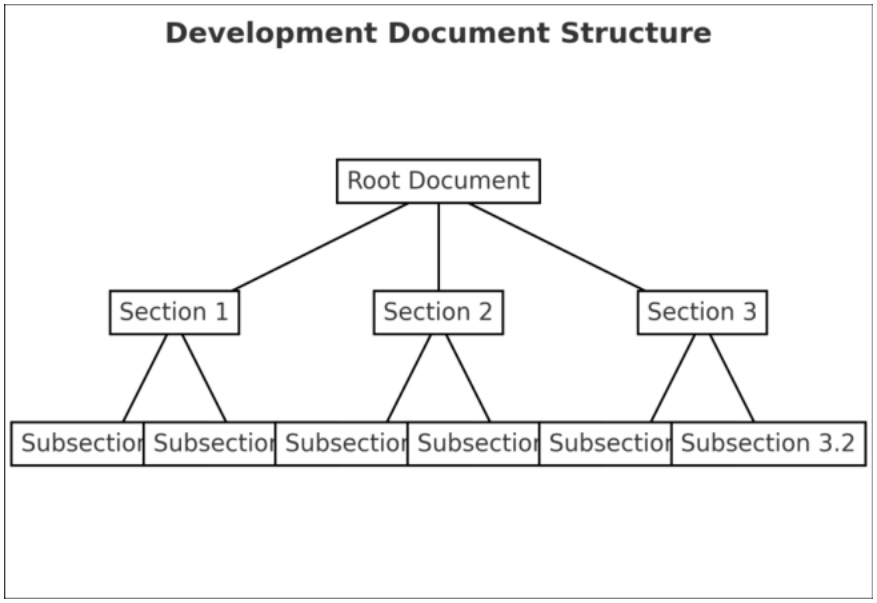


Figure 3-298 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-398 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

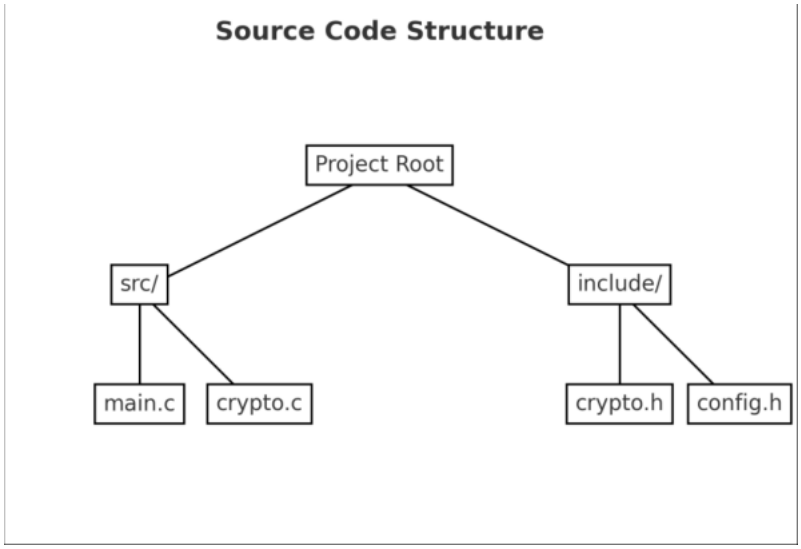


Figure 3-299 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-399 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

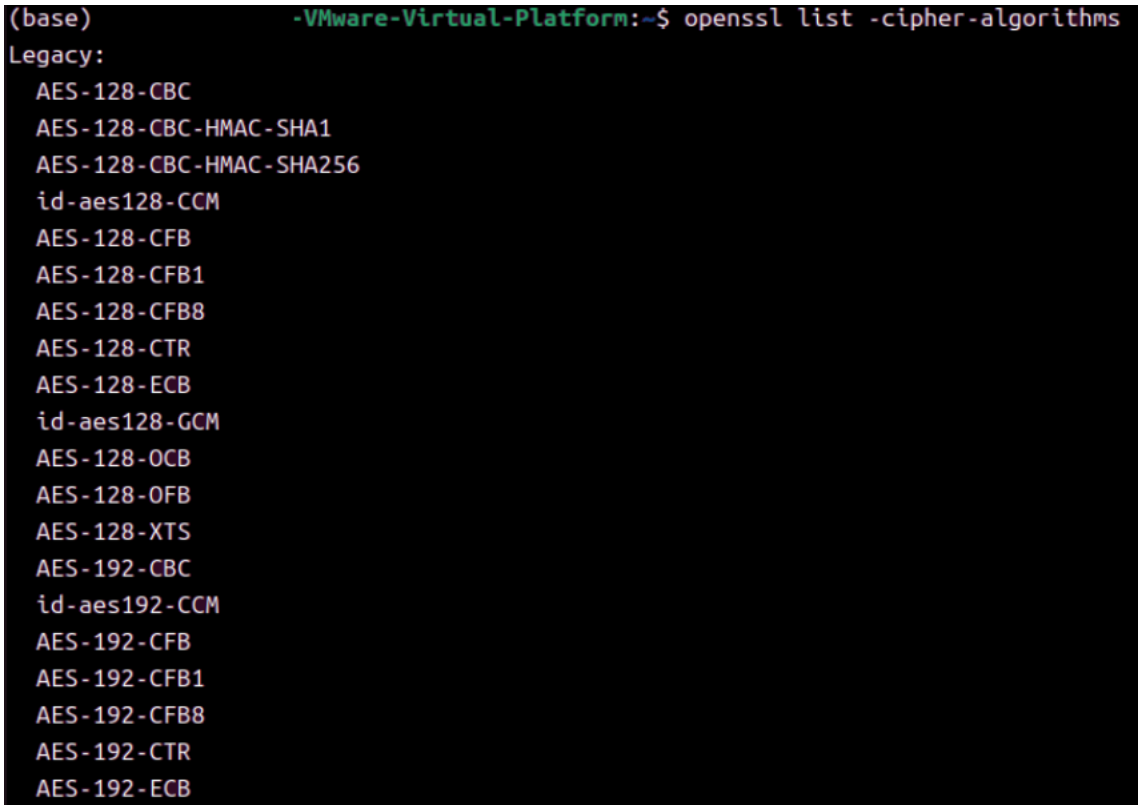


Figure 3-300 그림 제목

6.15.3 판정근거

Table 3-400 TE09.08.02 시험결과 판정근거

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

6.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.16 TE09.09.01

6.16.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.09.01	SSP 생성 및 사용 방법 명세	개발문서 검토

6.16.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-401 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

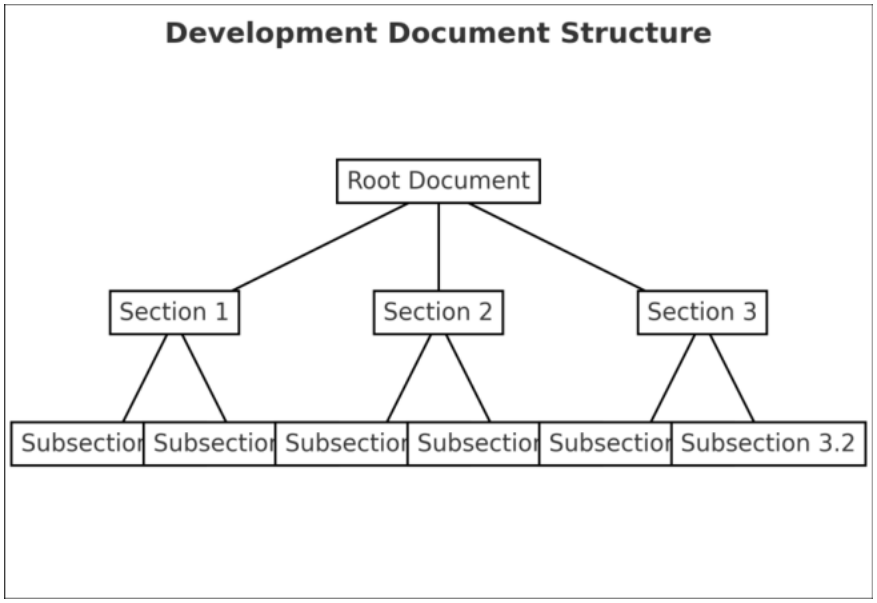


Figure 3-301 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-402 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

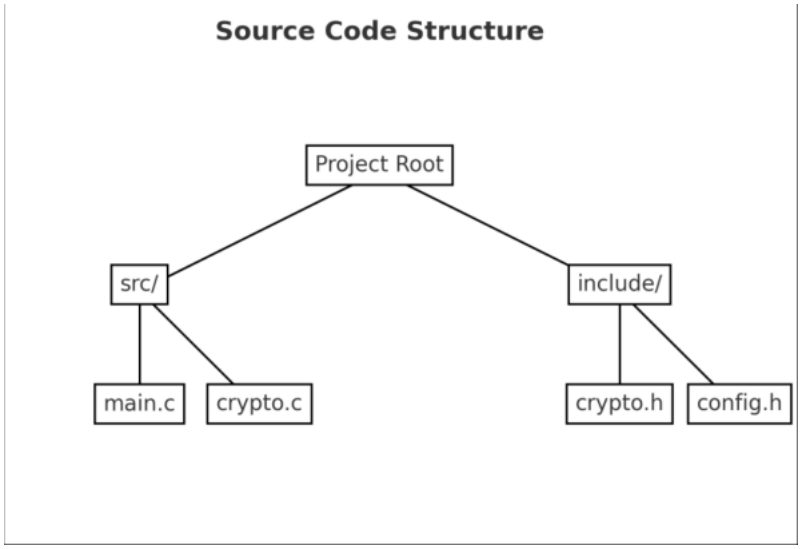


Figure 3-302 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-403 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

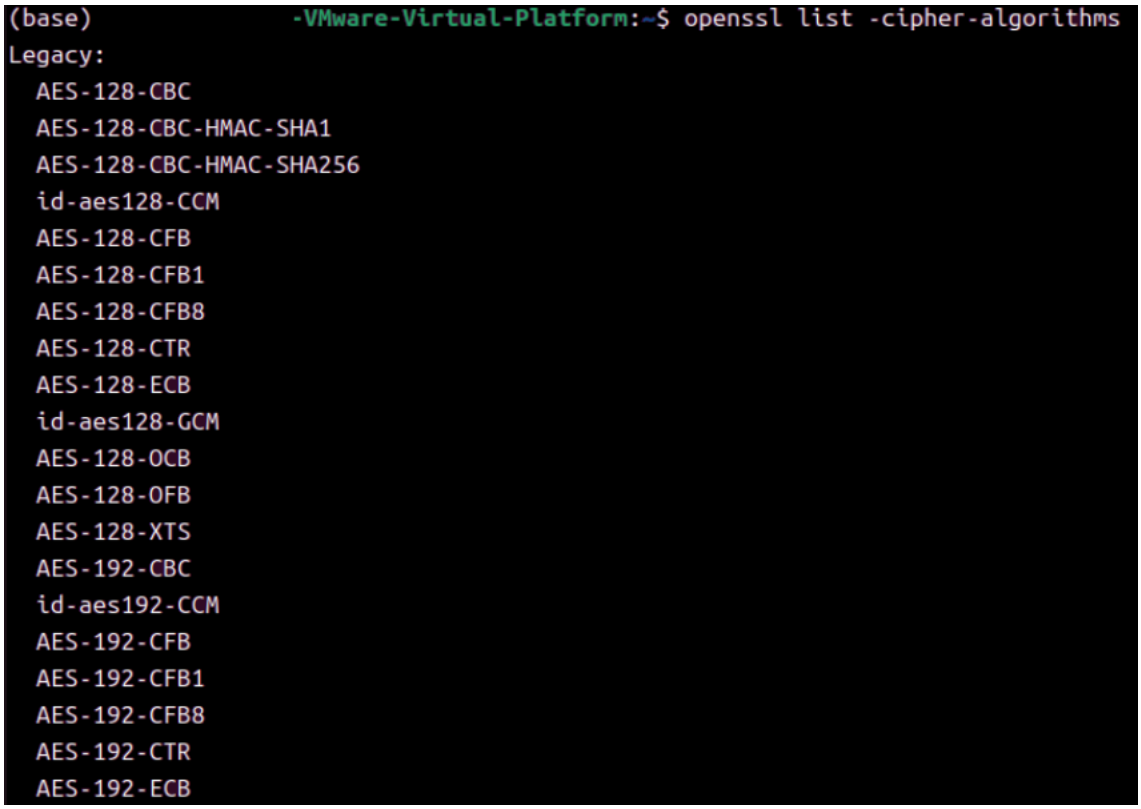


Figure 3-303 그림 제목

6.16.3 판정근거

Table 3-404 TE09.09.01 시험결과 판정근거

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

6.16.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.17 TE09.09.02

6.17.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.09.02	SSP 생성 방법의 KS X ISO/IEC 19790 부속서 D 준수 여부	소스코드 검토

6.17.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-405 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

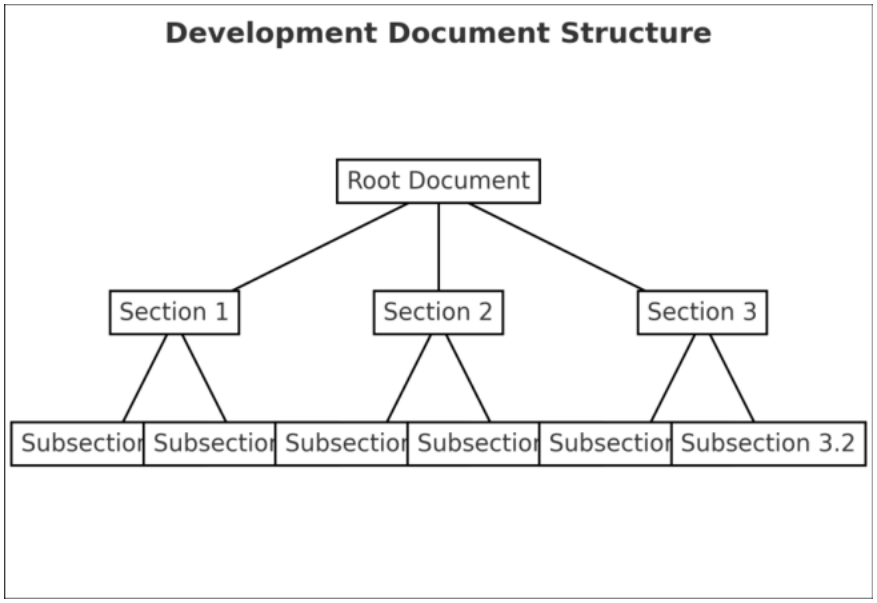


Figure 3-304 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-406 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

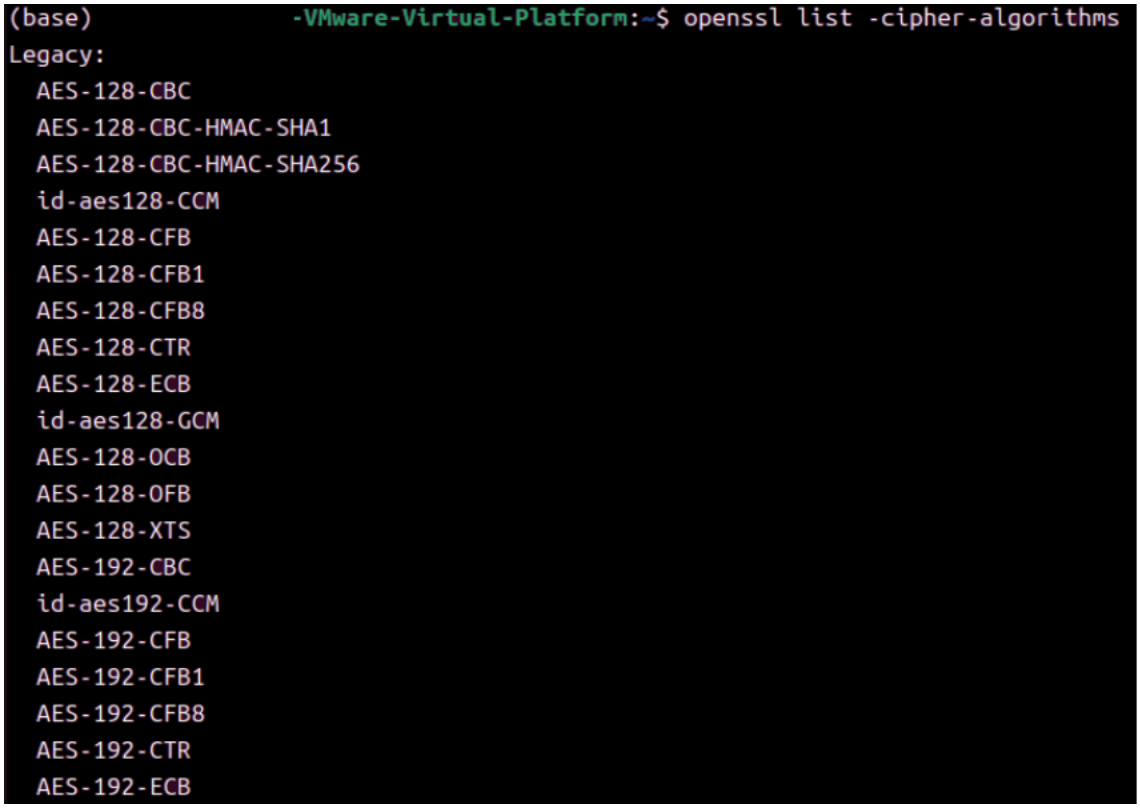


Figure 3-305 그림 제목

Table 3-407 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

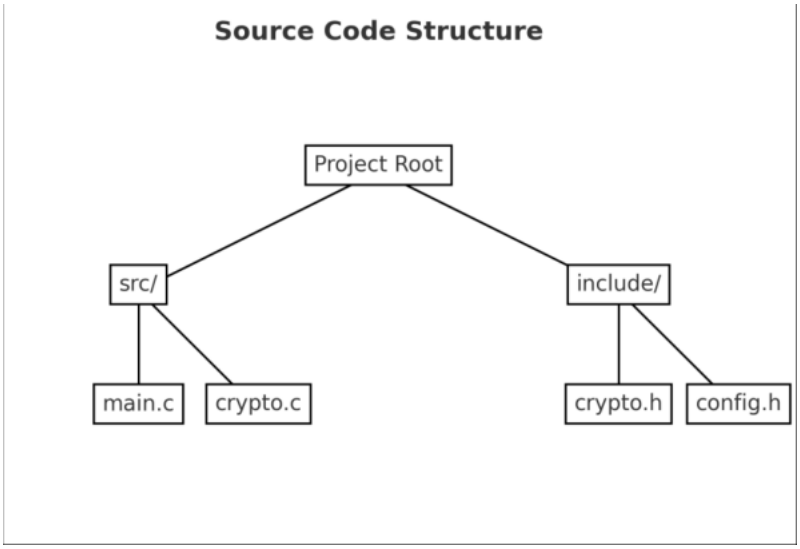


Figure 3-306 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-408 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

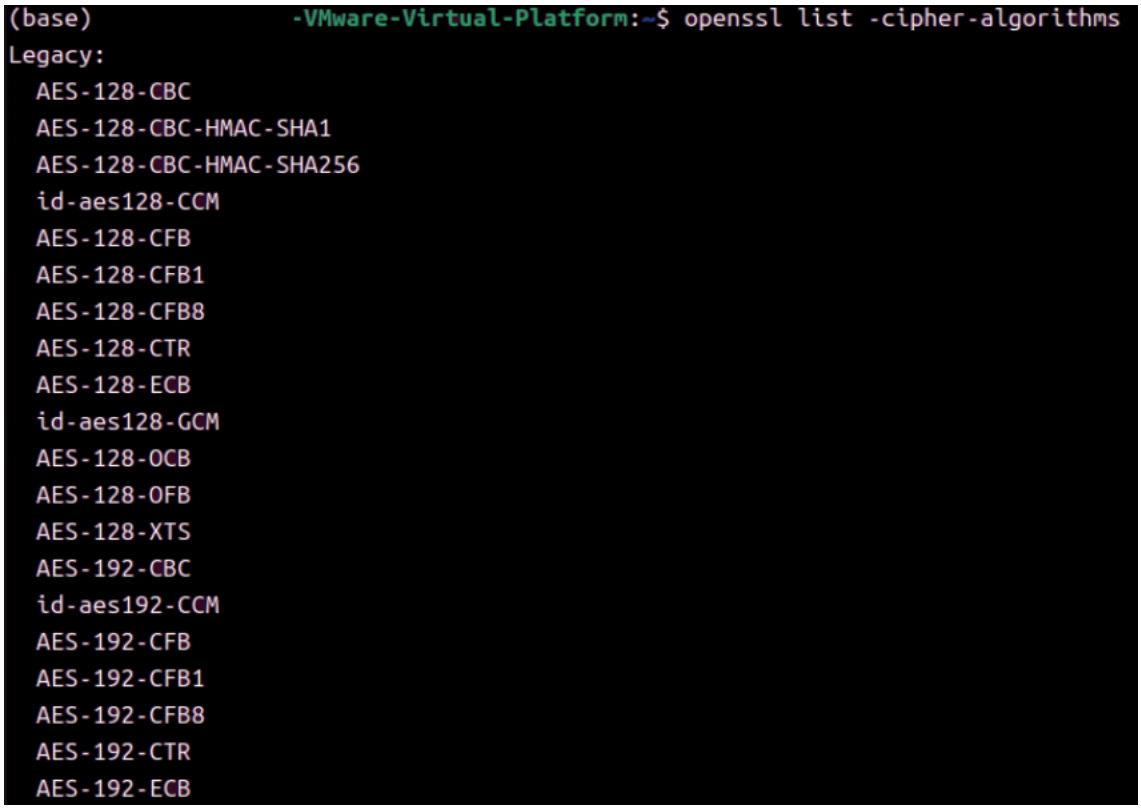


Figure 3-307 그림 제목

6.17.3 판정근거

Table 3-409 TE09.09.02 시험결과 판정근거

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

6.17.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.18 TE09.10.01

6.18.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.10.01	자동화된 SSP 설정 및 사용 방법 명세	개발문서 검토

6.18.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-410 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

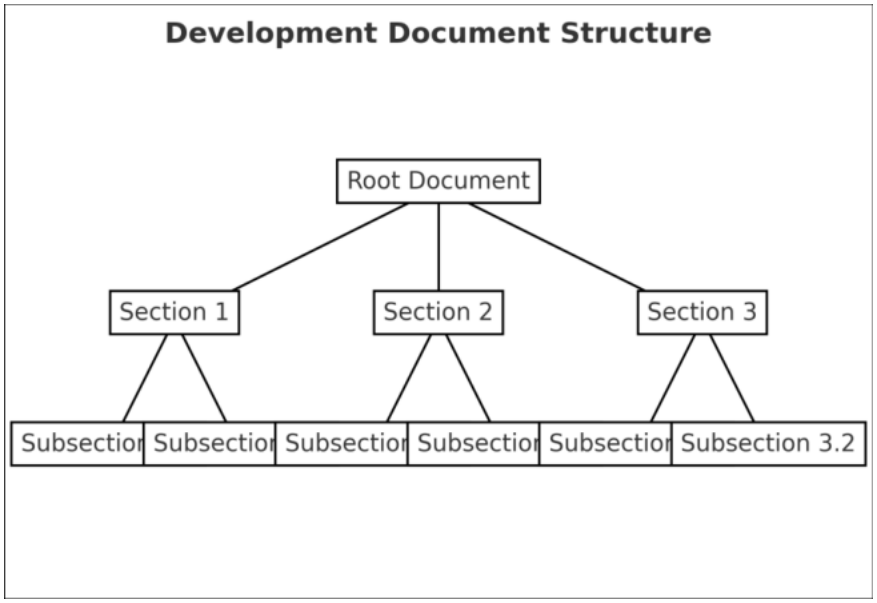


Figure 3-308 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-411 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

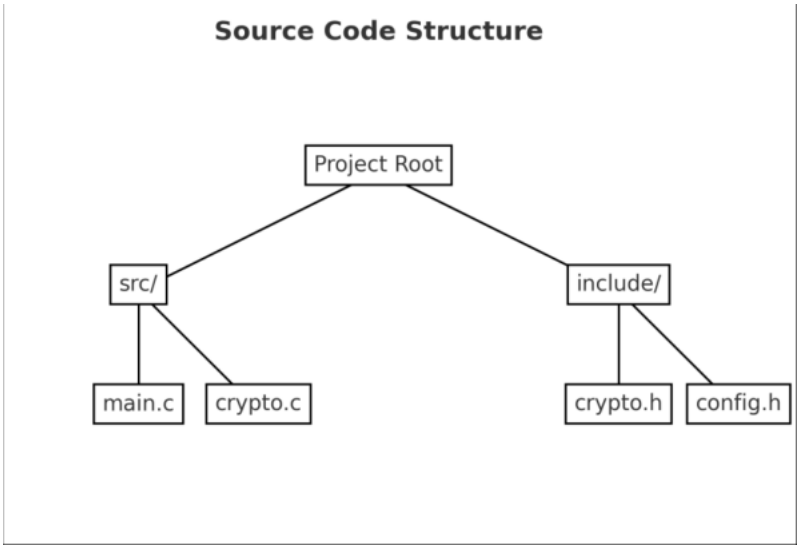


Figure 3-309 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-412 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

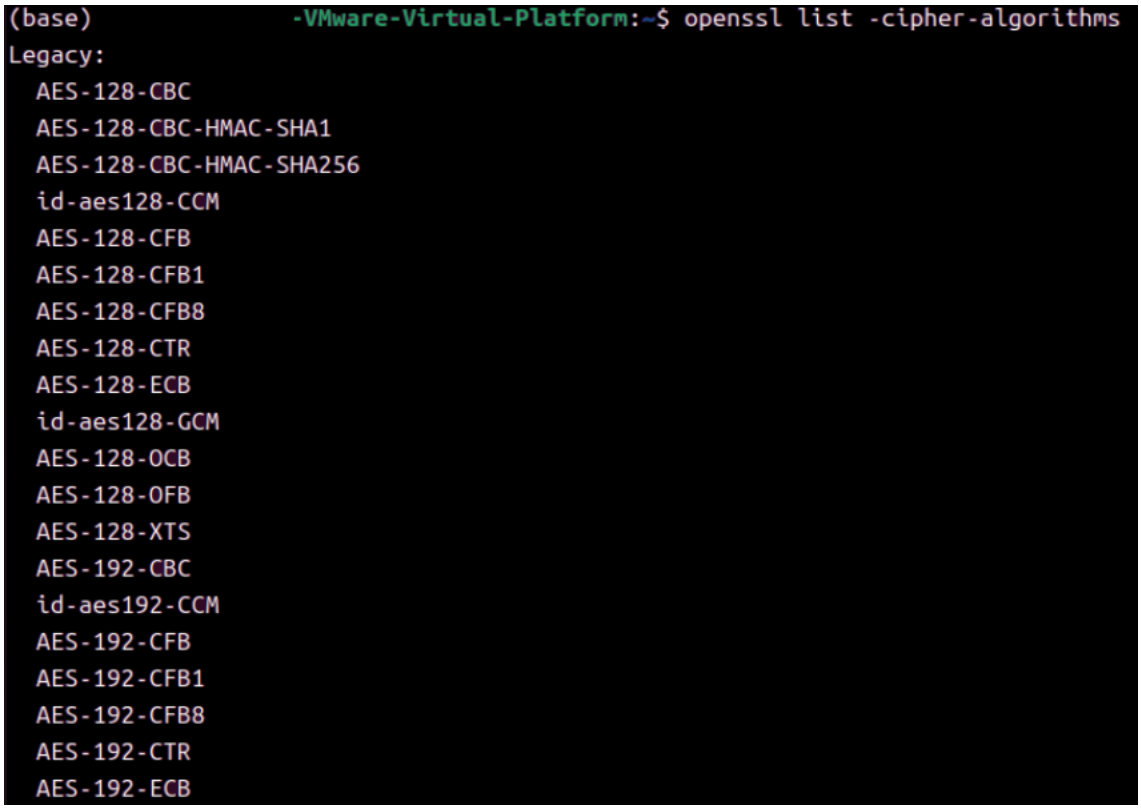


Figure 3-310 그림 제목

6.18.3 판정근거

Table 3-413 TE09.10.01 시험결과 판정근거

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

6.18.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.19 TE09.10.02

6.19.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.10.02	자동화된 SSP 설정 방법의 KS X ISO/IEC 19790 부속서 D 준수 여부	개발문서 검토

6.19.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-414 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

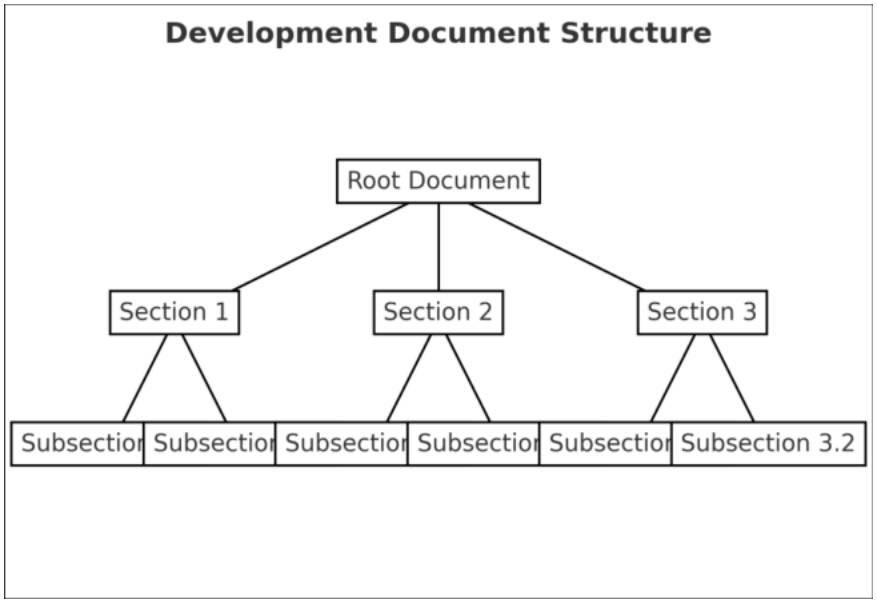


Figure 3-311 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-415 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

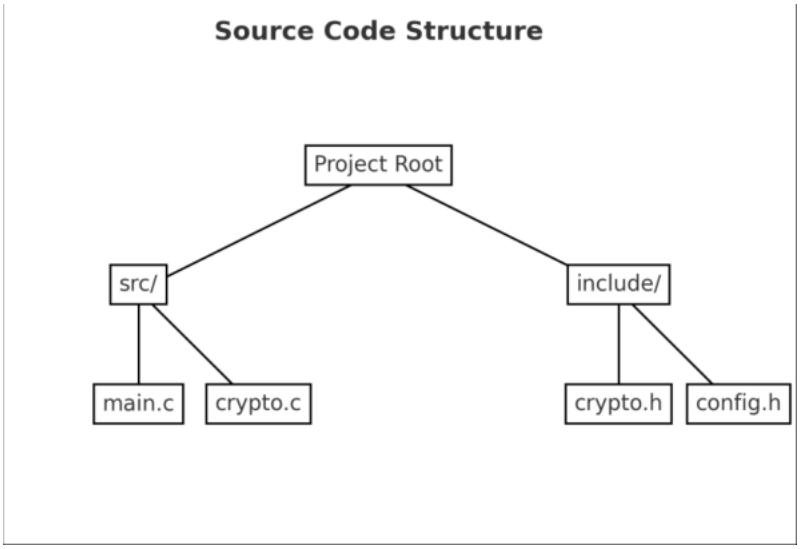


Figure 3-312 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-416 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

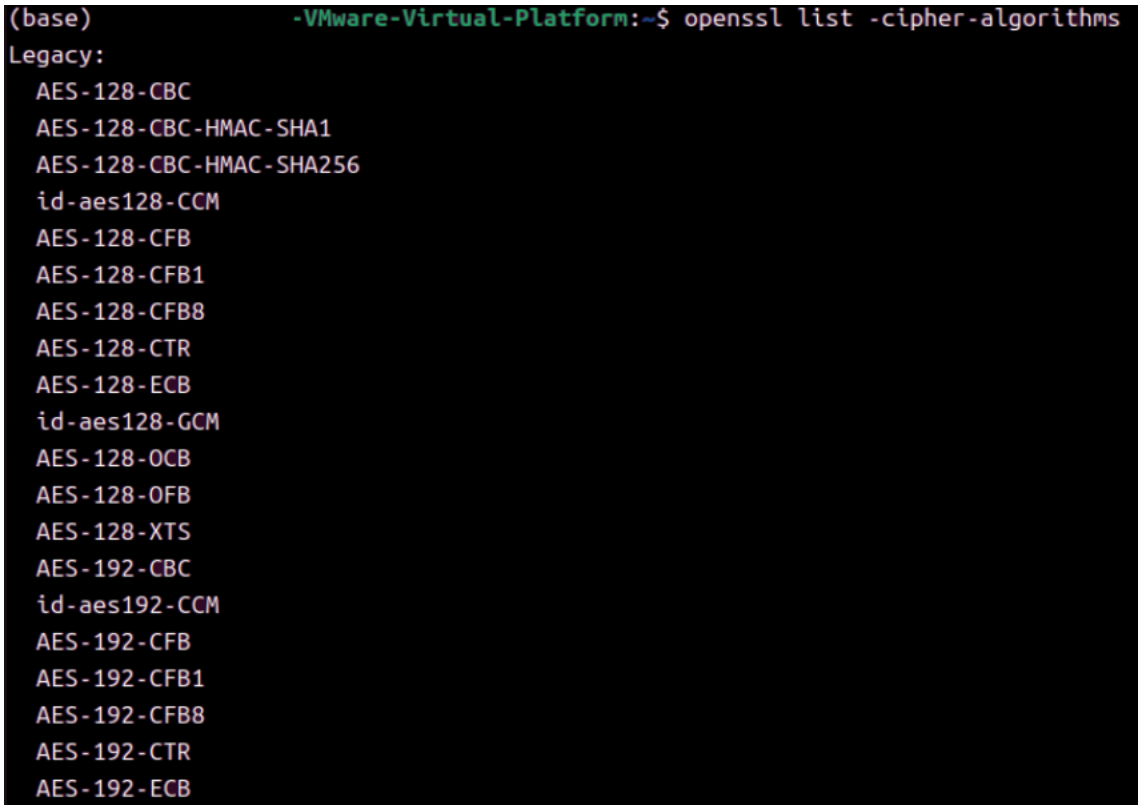


Figure 3-313 그림 제목

6.19.3 판정근거

Table 3-417 TE09.10.02 시험결과 판정근거

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

6.19.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.20 TE09.19.01

6.20.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.19.01	운영환경 내에서 보호되는 CSP, 키 요소 및 인증 데이터의 평문 입 · 출력	개발문서 검토

6.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-418 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

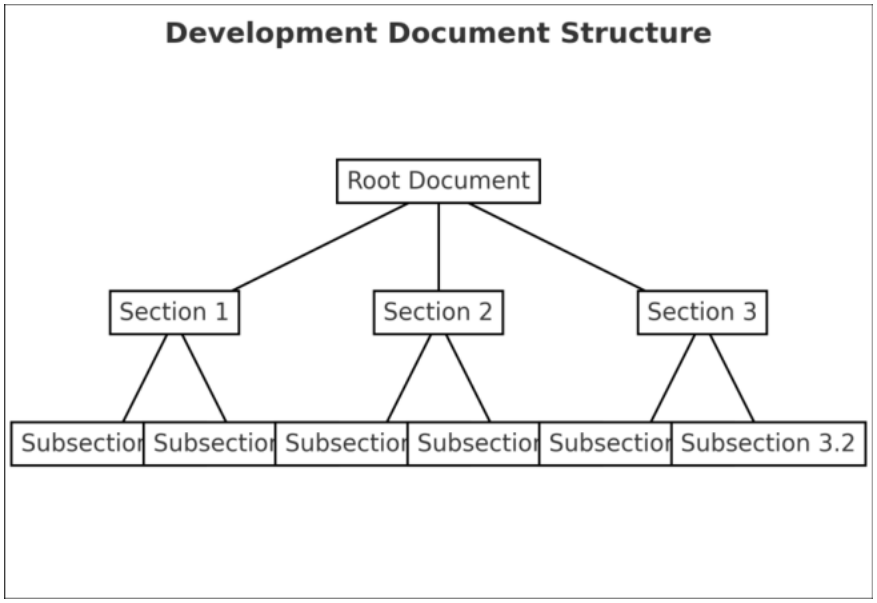


Figure 3-314 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-419 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

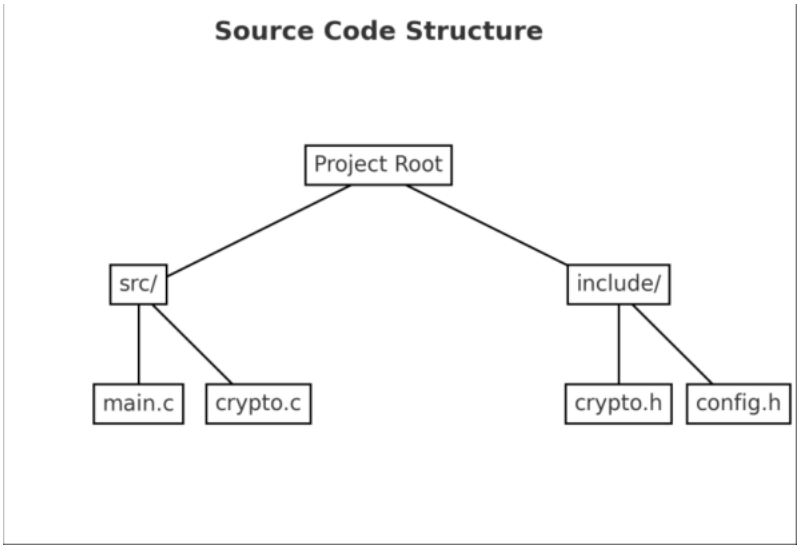


Figure 3-315 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-420 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

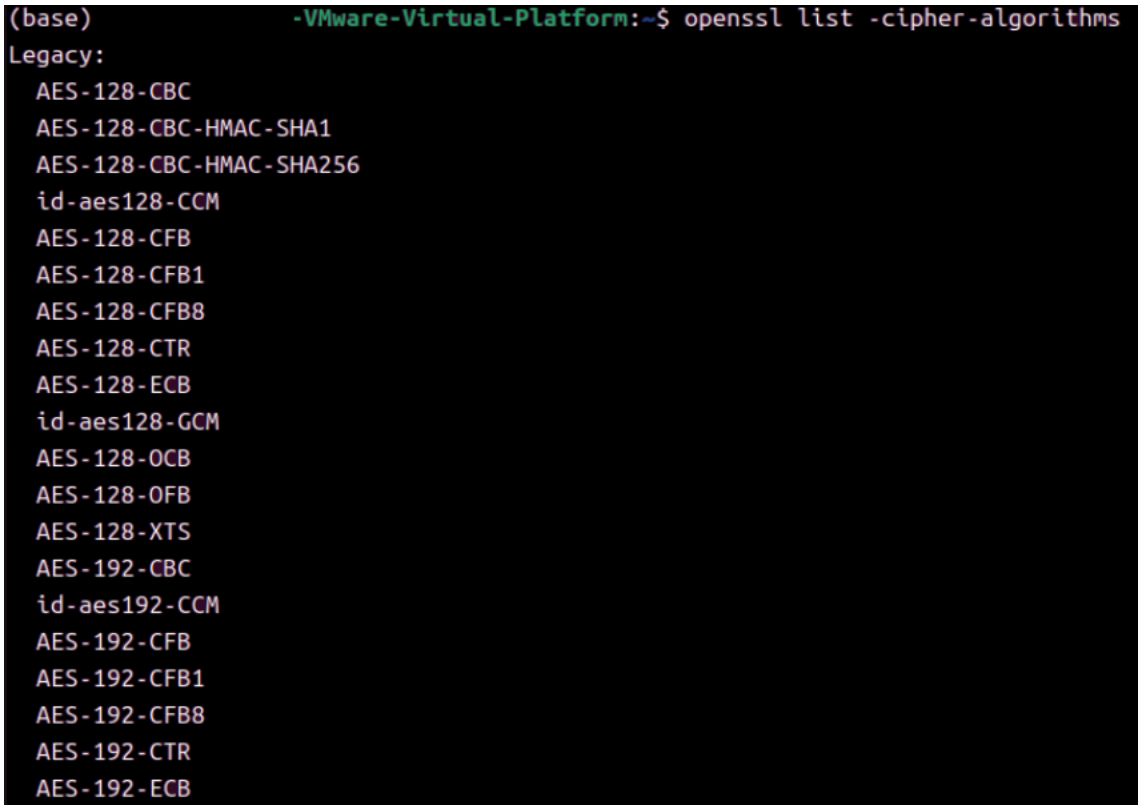


Figure 3-316 그림 제목

6.20.3 판정근거

Table 3-421 TE09.19.01 시험결과 판정근거

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

6.20.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.21 TE09.29.01

6.21.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.29.01	제로화된 SSP 복구 및 재사용 방지 명세	개발문서 검토

6.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-422 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

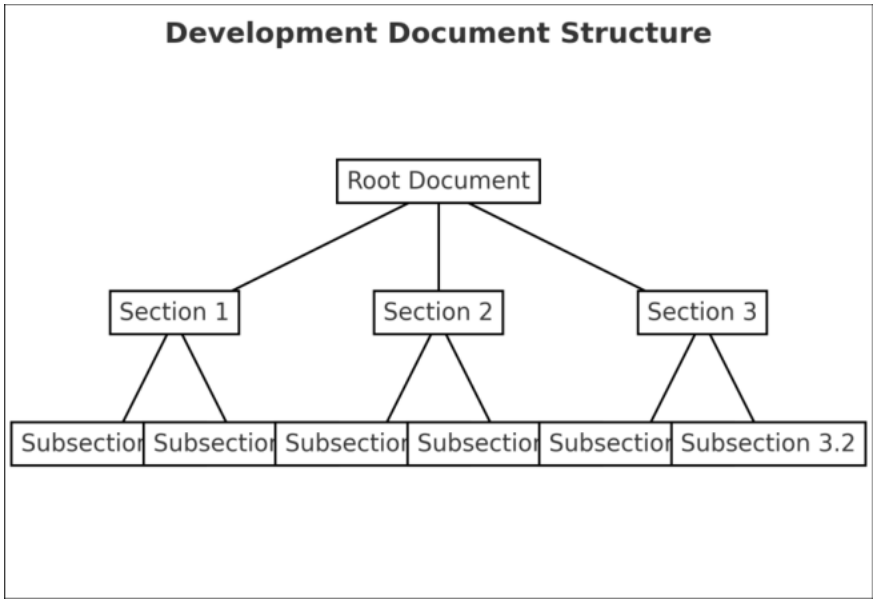


Figure 3-317 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-423 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

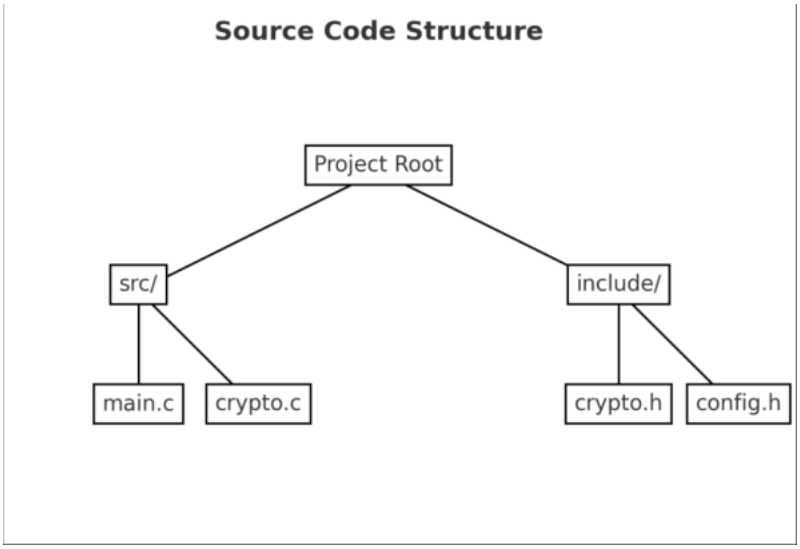


Figure 3-318 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-424 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

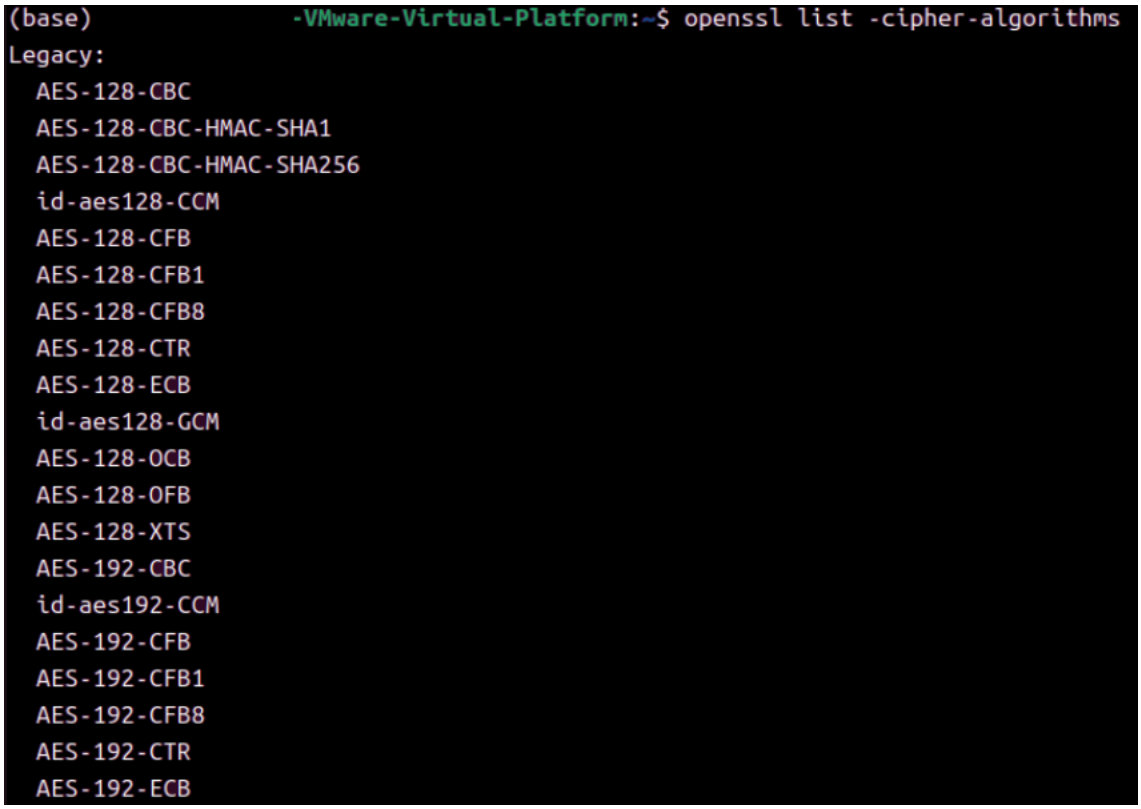


Figure 3-319 그림 제목

6.21.3 판정근거

Table 3-425 TE09.29.01 시험결과 판정근거

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

6.21.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

6.22 TE09.29.02

6.22.1 시험 요구사항

TE	주요 확인사항	확인방법
TE09.29.02	벤더 제공 근거의 정확성	소스코드 검토

6.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-426 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

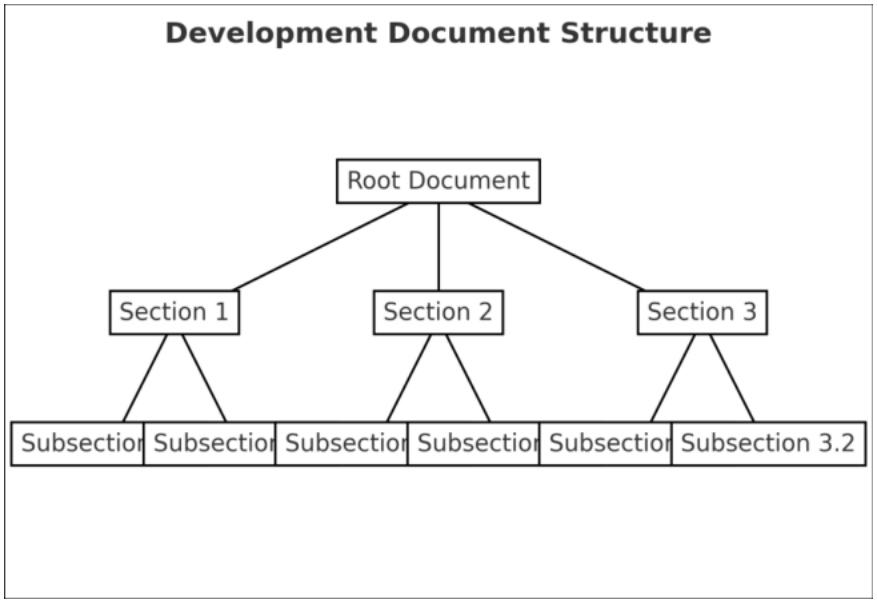


Figure 3-320 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-427 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

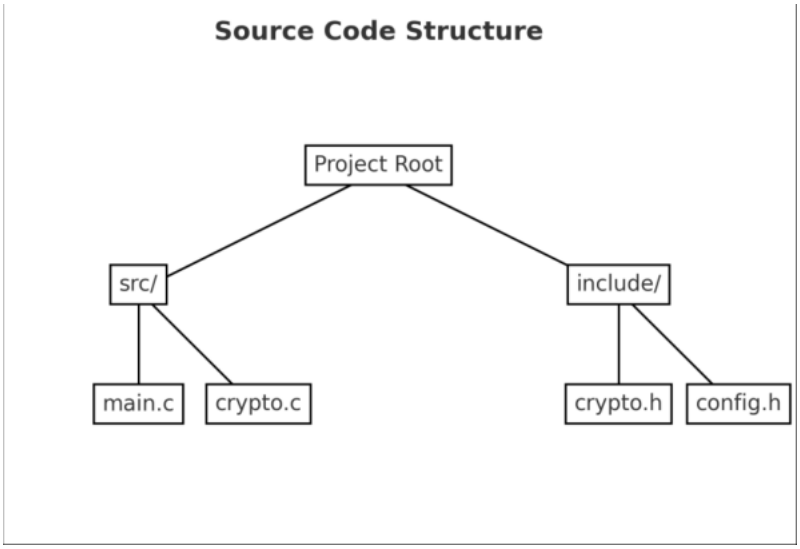


Figure 3-321 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-428 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

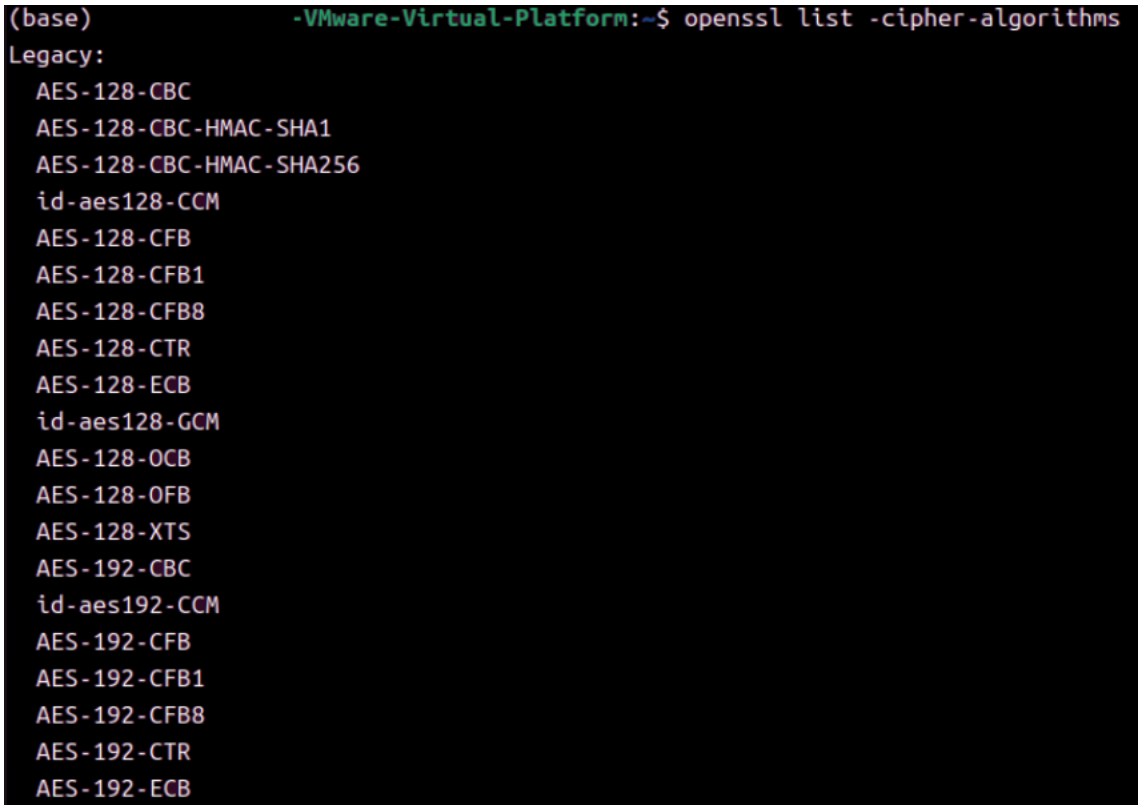


Figure 3-322 그림 제목

6.22.3 판정근거

Table 3-429 TE09.29.02 시험결과 판정근거

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

6.22.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7. 자가시험 (AS10)

□ 암호모듈이 올바른 기능을 수행하는지 확인하기 위해서 자가시험을 수행한다 .

□ 자가시험은 동작 전 자가시험과 조건부 자가시험으로 구분된다 .

7.1 AS10 시험항목

AS	TE	확인사항
AS10.07	1 ~ 5	자가시험 목록 및 오류 조건
AS10.08	1, 2, 3	오류 진입 후 오류 표시
AS10.09	1, 2, 3	오류 상태에서의 제어 및 데이터 출력 금지
AS10.10	1, 2	자가시험 완료 후 함수 및 알고리즘 사용
AS10.11	1	자가시험 실패 시 오류 상태 미 출력 시 개발문서에 기술
AS10.15	1, 2	동작 전 자가시험
AS10.17	1, 2, 4, 6	검증대상 무결성 검증기술
AS10.20	1	검증대상 무결성 검증기술에 사용되는 알고리즘에 대한 검증
AS10.24	1, 2	동작 전 자가시험에 포함되는 핵심 기능
AS10.25	1, 2	조건부 자가시험
AS10.27	1	최초로 사용되기 이전에 조건부 알고리즘 자가시험 수행
AS10.28	1	KAT 시험
AS10.29	1	검증대상 알고리즘의 자가시험 대상의 파라미터 크기
AS10.33	1, 2	암호알고리즘 비교시험
AS10.34	1, 2	오류 탐지 시험
AS10.35	1, 2, 3	조건부 키 쌍 일치시험
AS10.53	1, 2, 3	주기적 자가 시험

7.2 TE10.07.01

7.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.07.01	자가시험 목록 확인	개발문서 검토

7.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-430 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

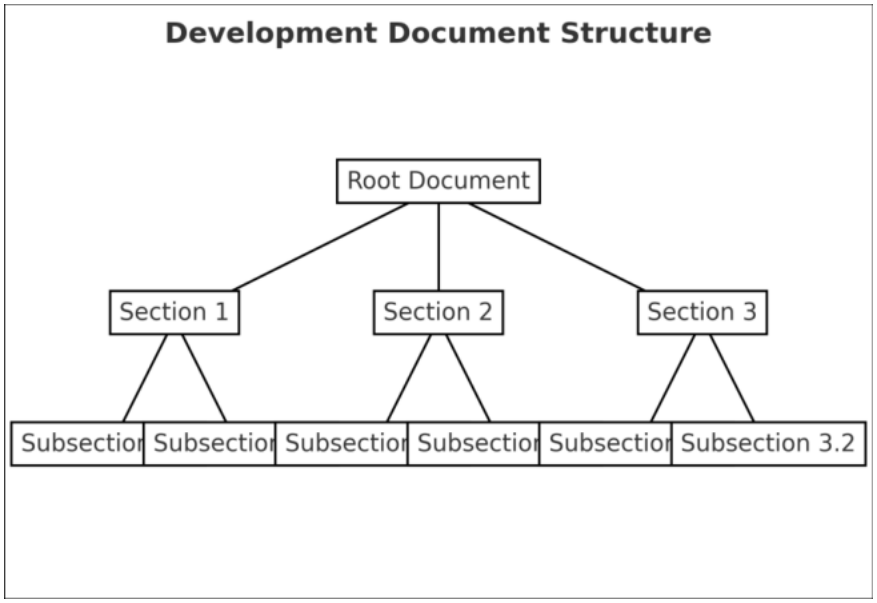


Figure 3-323 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-431 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

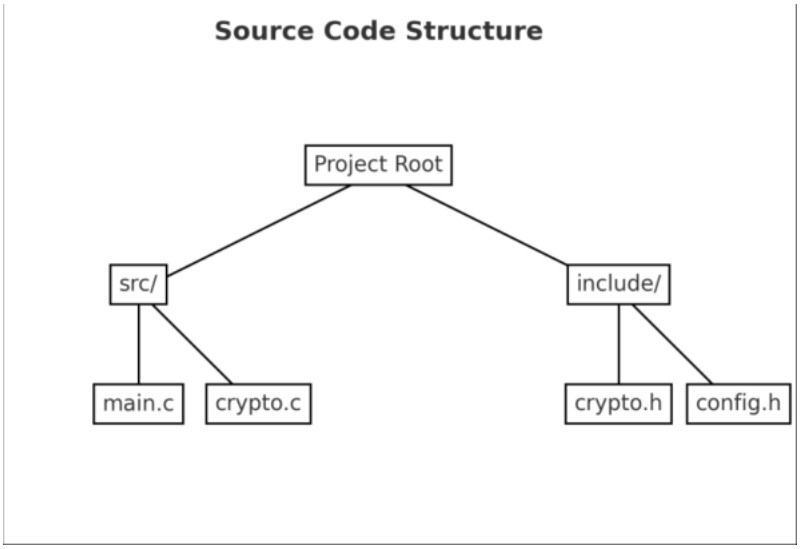


Figure 3-324 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-432 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

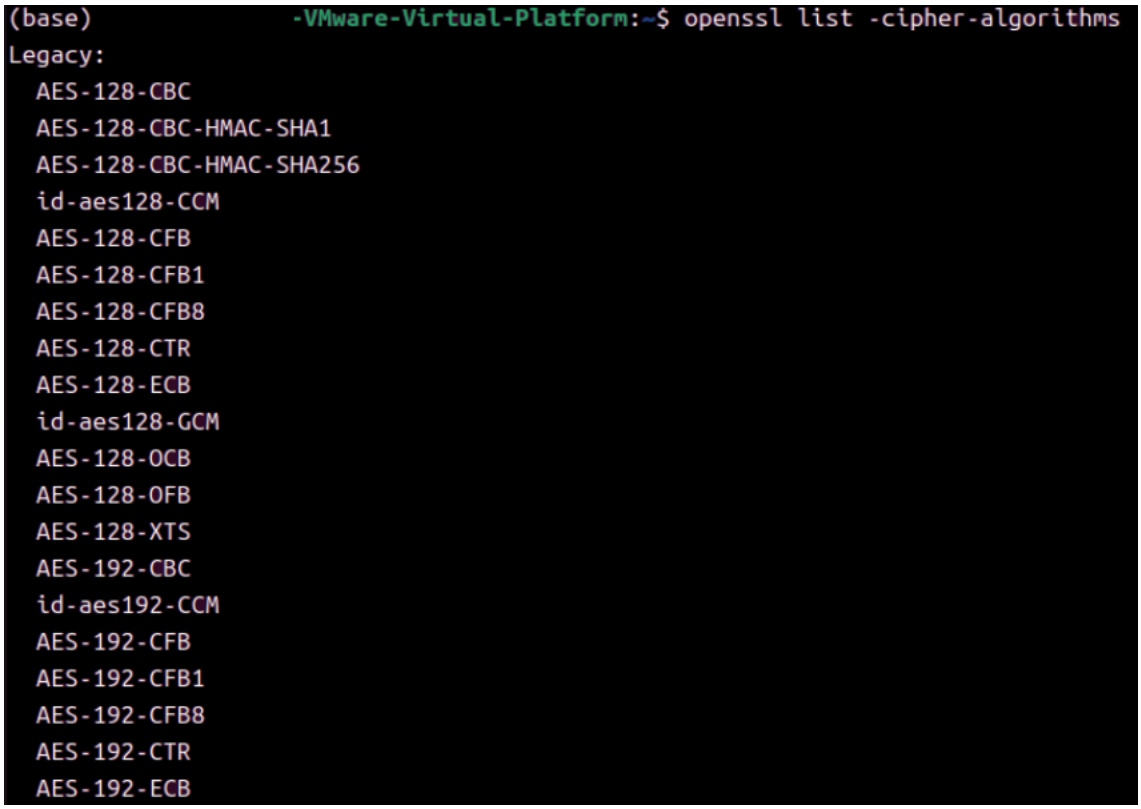


Figure 3-325 그림 제목

7.2.3 판정근거

Table 3-433 TE10.07.01 시험결과 판정근거

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

7.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.3 TE10.07.02

7.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.07.02	오류 조건과 해당 자가시험 정보 명세	개발문서 검토

7.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-434 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

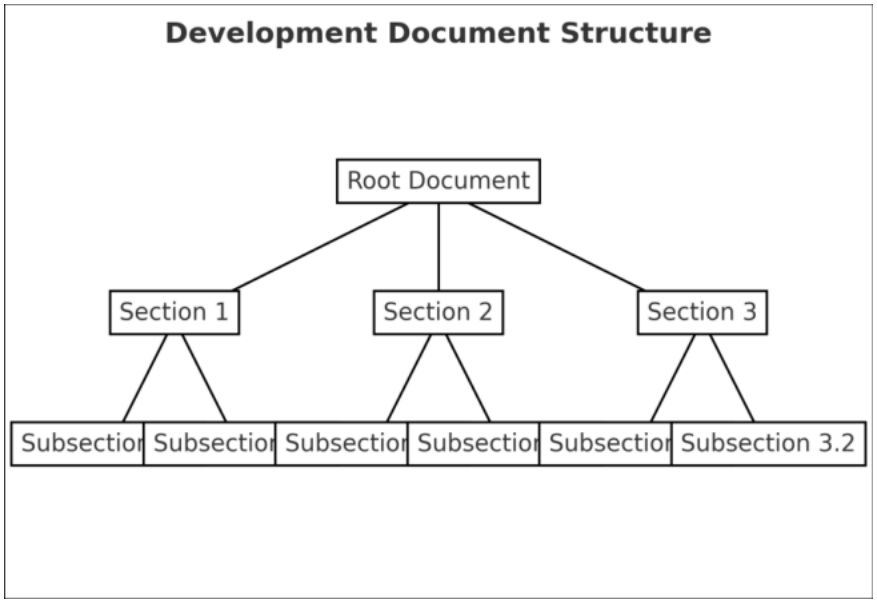


Figure 3-326 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-435 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

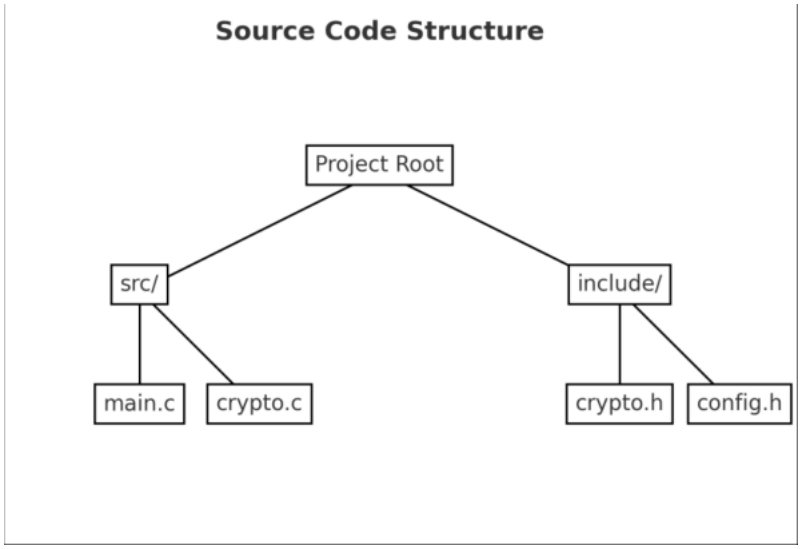


Figure 3-327 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-436 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

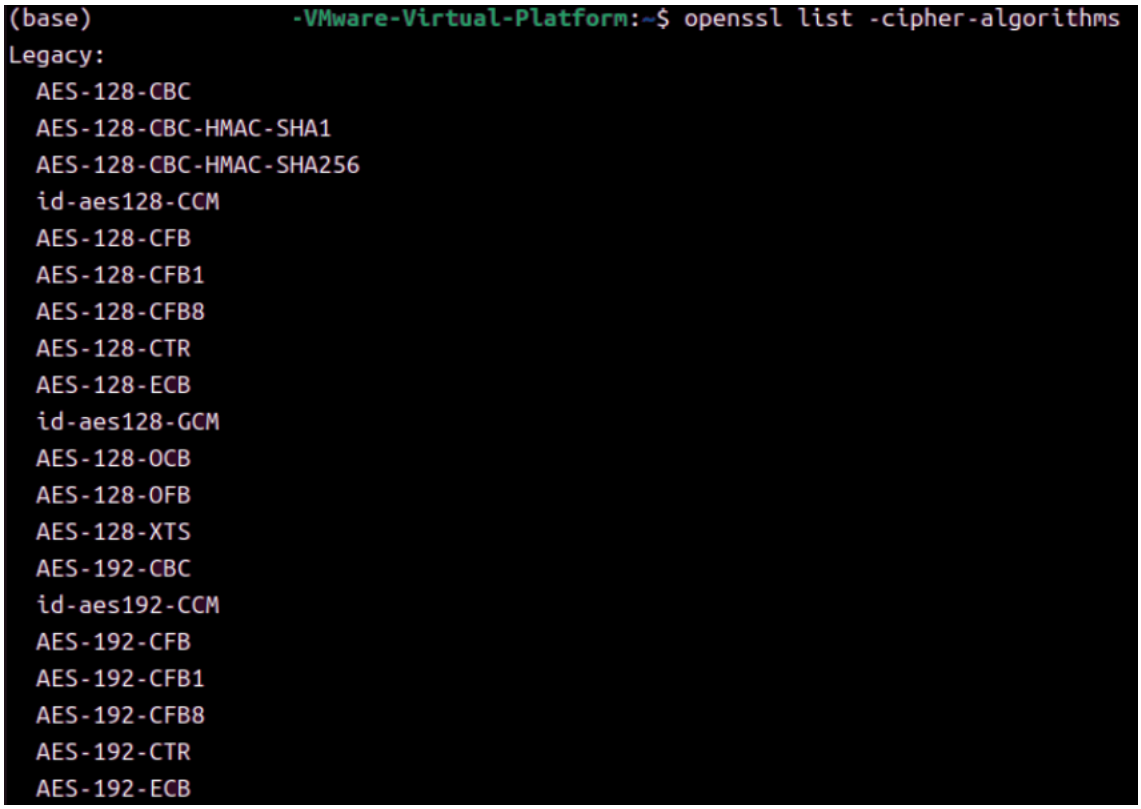


Figure 3-328 그림 제목

7.3.3 판정근거

Table 3-437 TE10.07.02 시험결과 판정근거

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

7.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.4 TE10.07.03

7.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.07.03	오류 유발 및 오류 발생 확인	암호모듈 검사

7.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-438 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

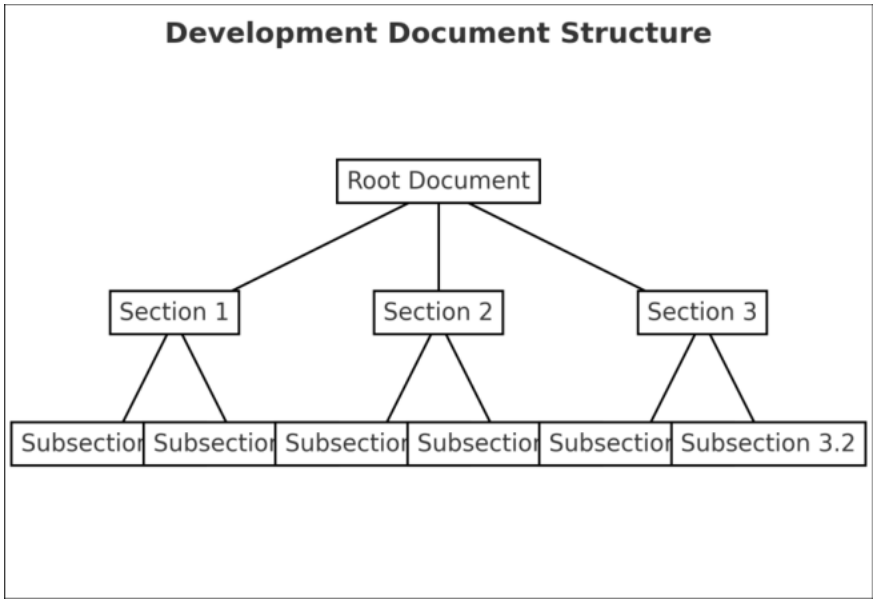


Figure 3-329 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-439 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

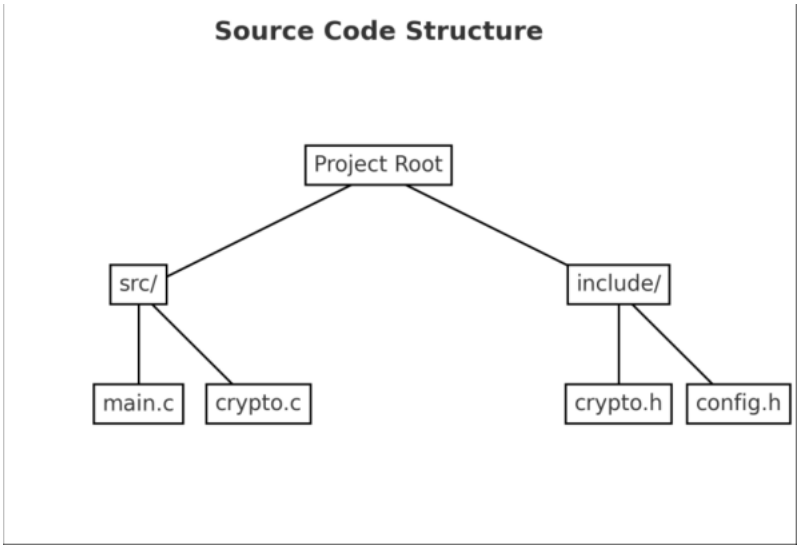


Figure 3-330 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-440 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

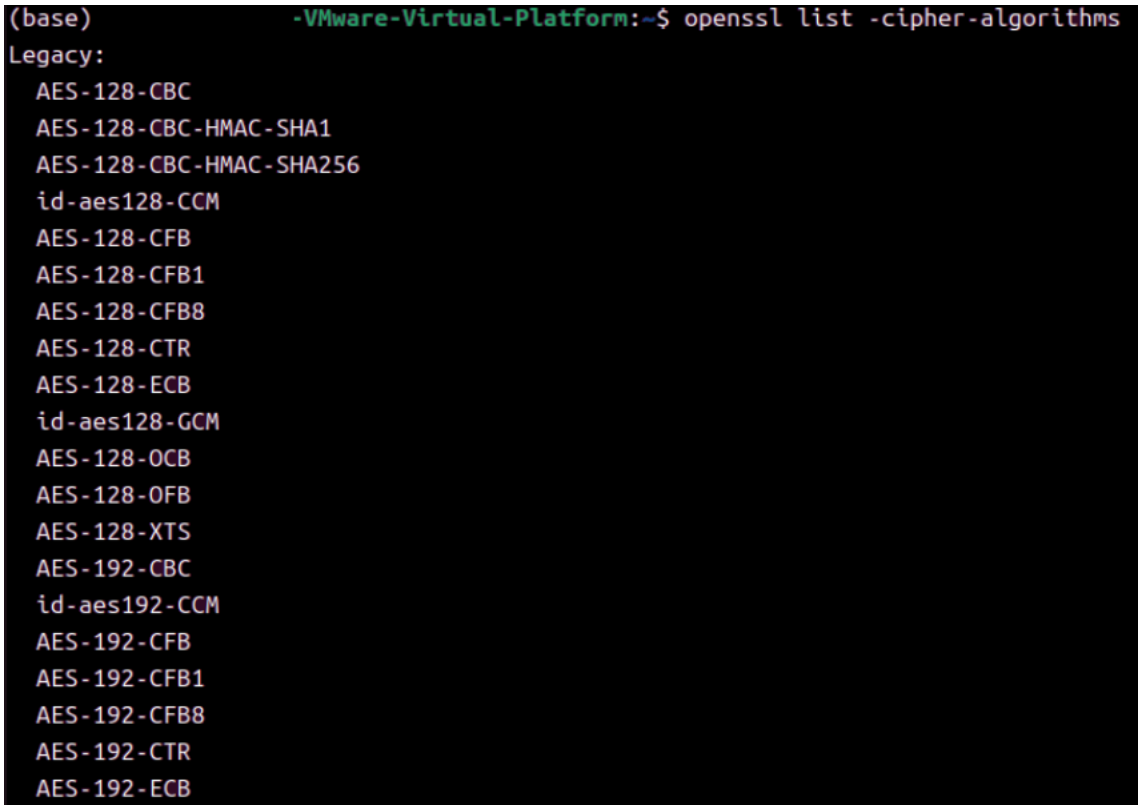


Figure 3-331 그림 제목

7.4.3 판정근거

Table 3-441 TE10.07.03 시험결과 판정근거

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

7.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.5 TE10.07.04

7.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.07.04	동작모드에 무관하게 모든 자가시험 수행	암호모듈 검사

7.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-442 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

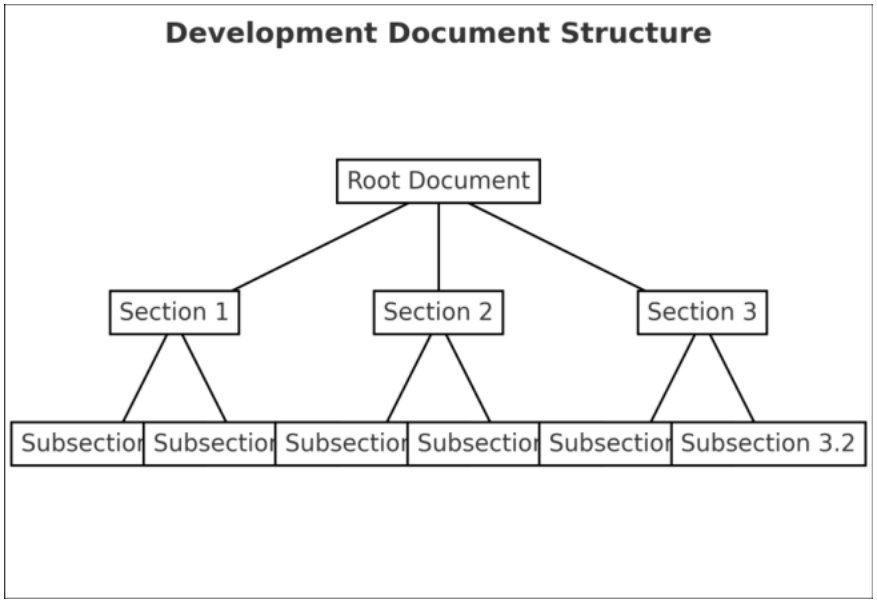


Figure 3-332 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-443 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

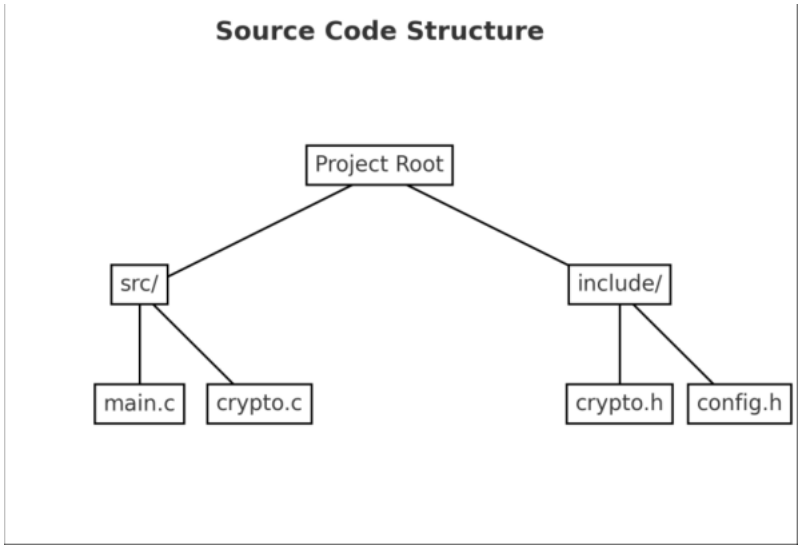


Figure 3-333 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-444 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

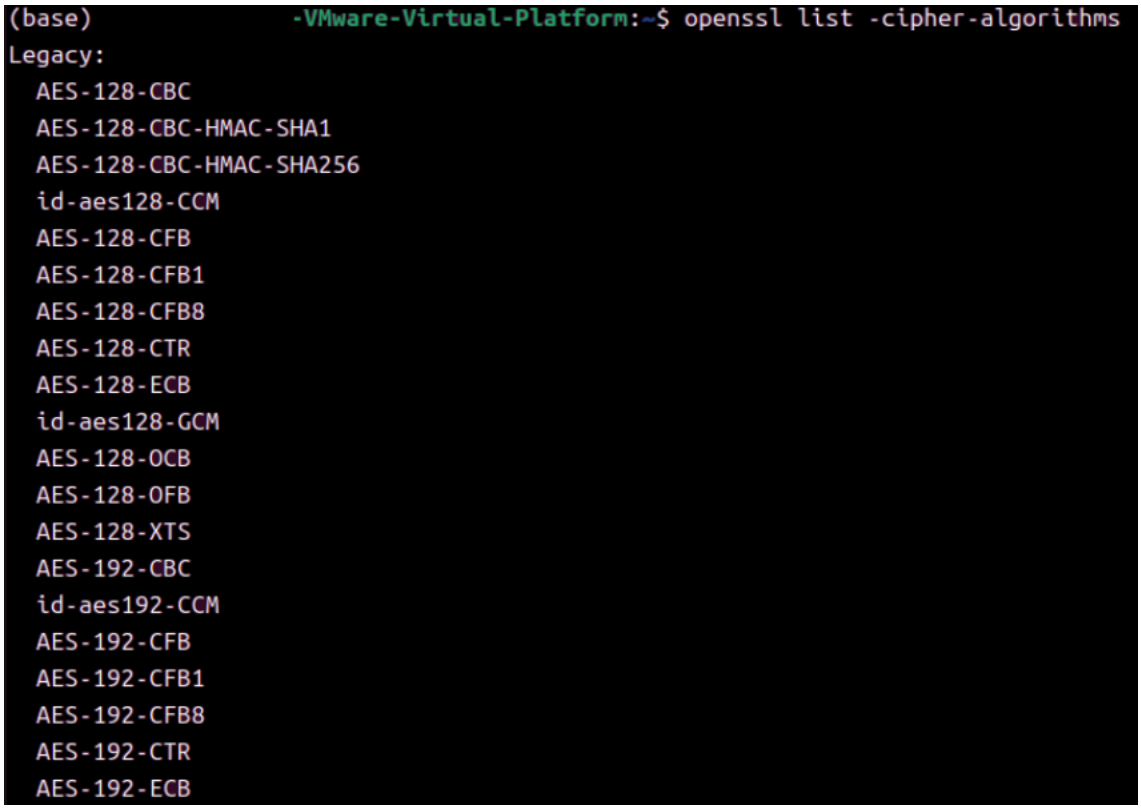


Figure 3-334 그림 제목

7.5.3 판정근거

Table 3-445 TE10.07.04 시험결과 판정근거

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

7.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.6 TE10.07.05

7.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.07.05	자가시험 성공 · 실패 판정이 암호모듈에 의해서만 결정	암호모듈 검사

7.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-446 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

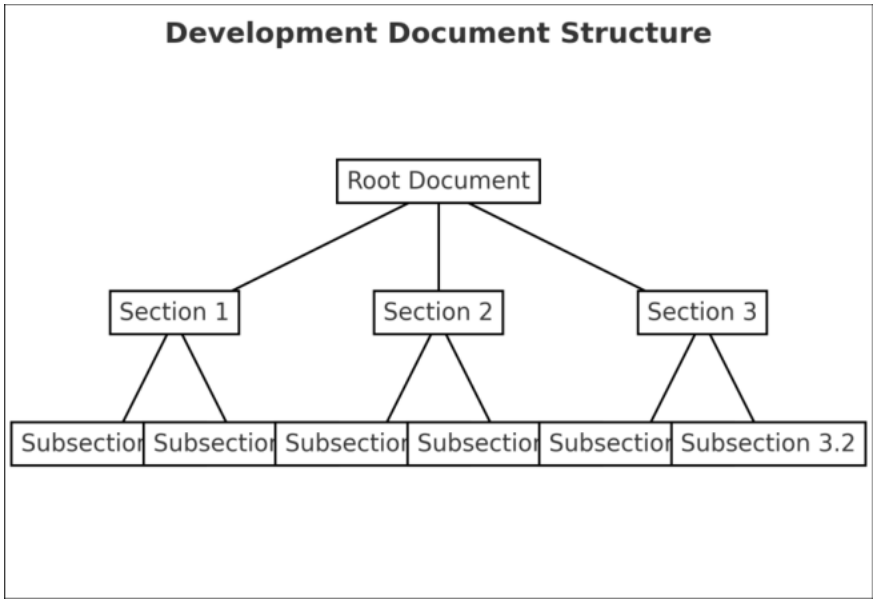


Figure 3-335 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-447 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

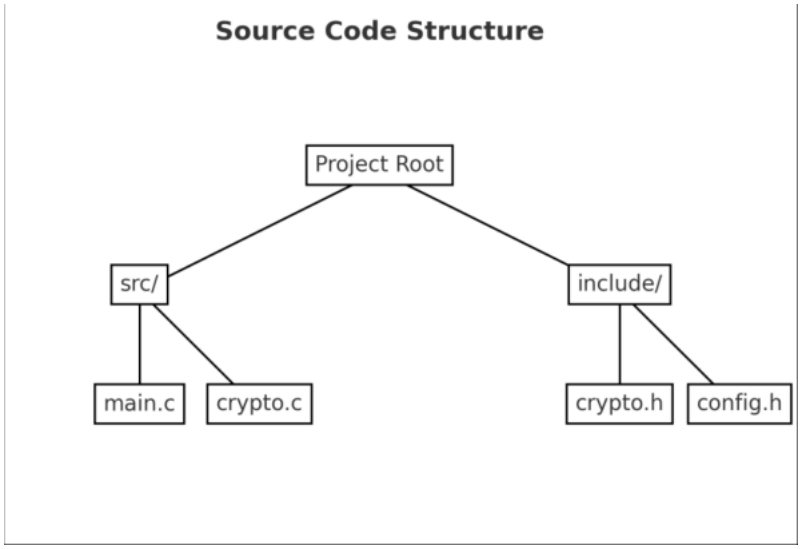


Figure 3-336 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-448 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

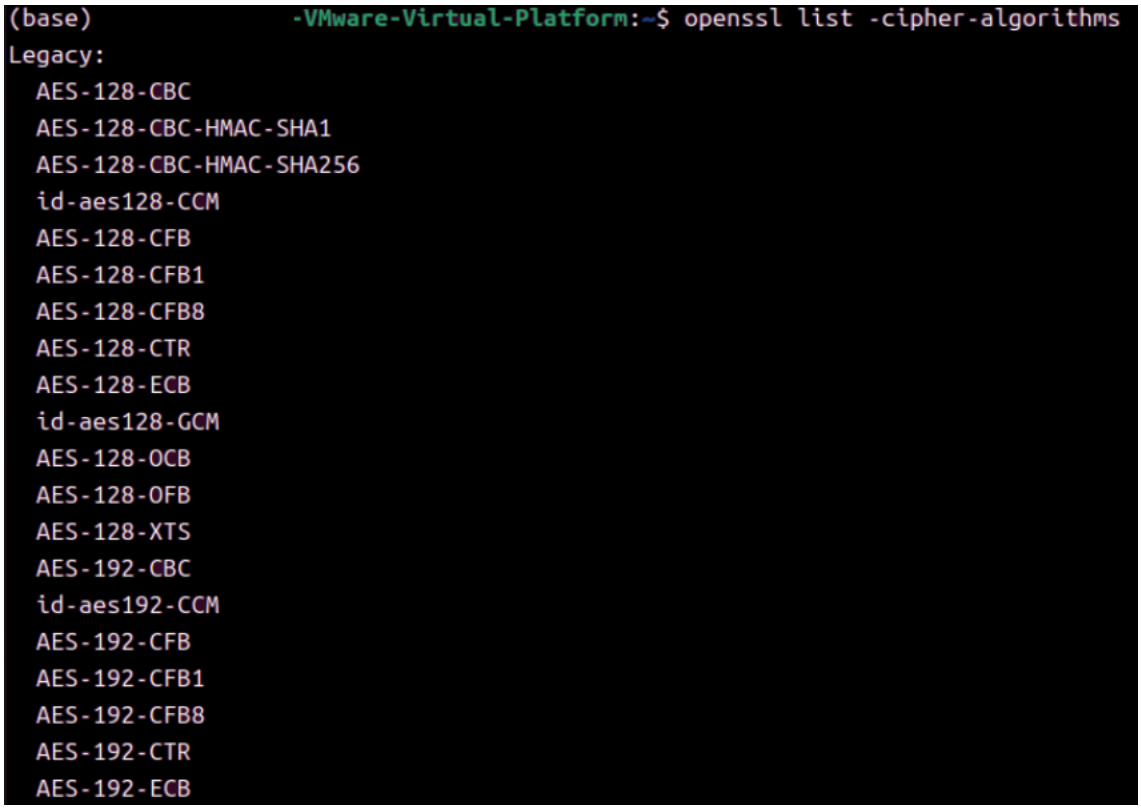


Figure 3-337 그림 제목

7.6.3 판정근거

Table 3-449 TE10.07.05 시험결과 판정근거

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

7.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.7 TE10.08.01

7.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.08.01	자가시험 실패 시 오류 상태 목록	개발문서 검토

7.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-450 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

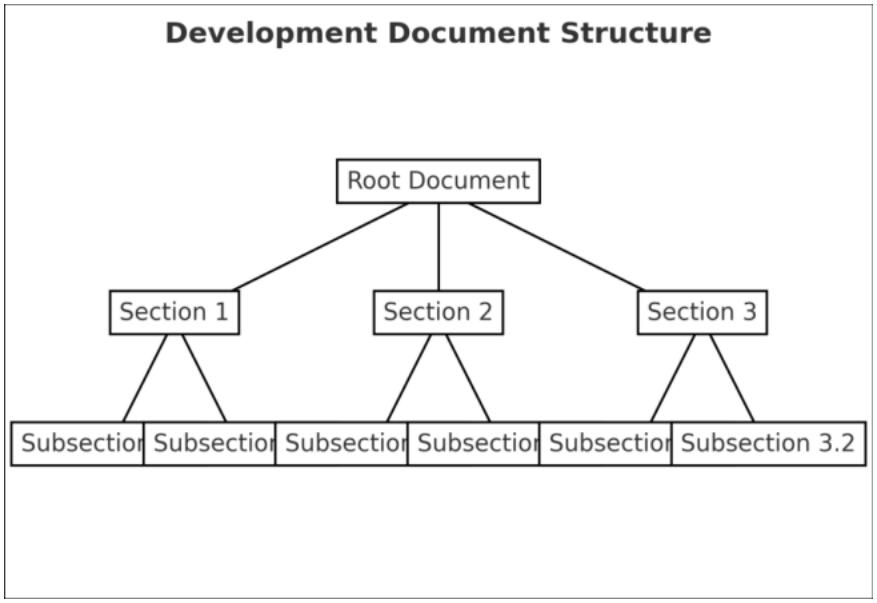


Figure 3-338 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-451 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

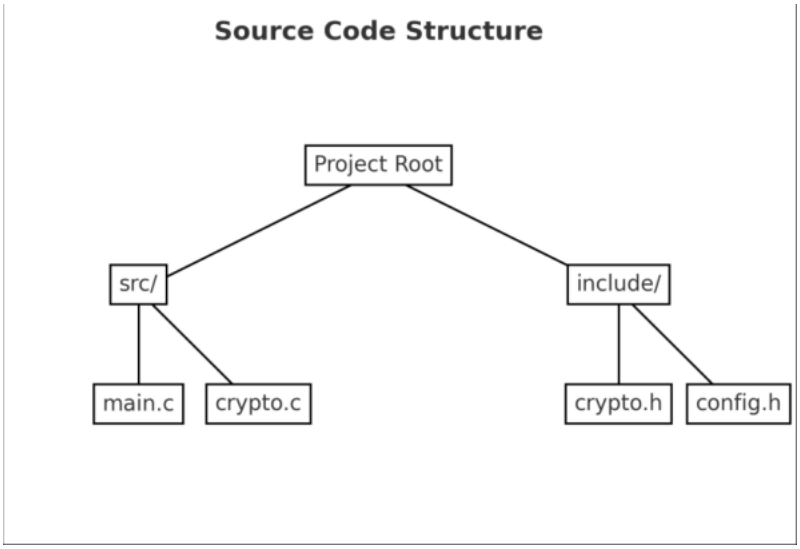


Figure 3-339 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-452 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

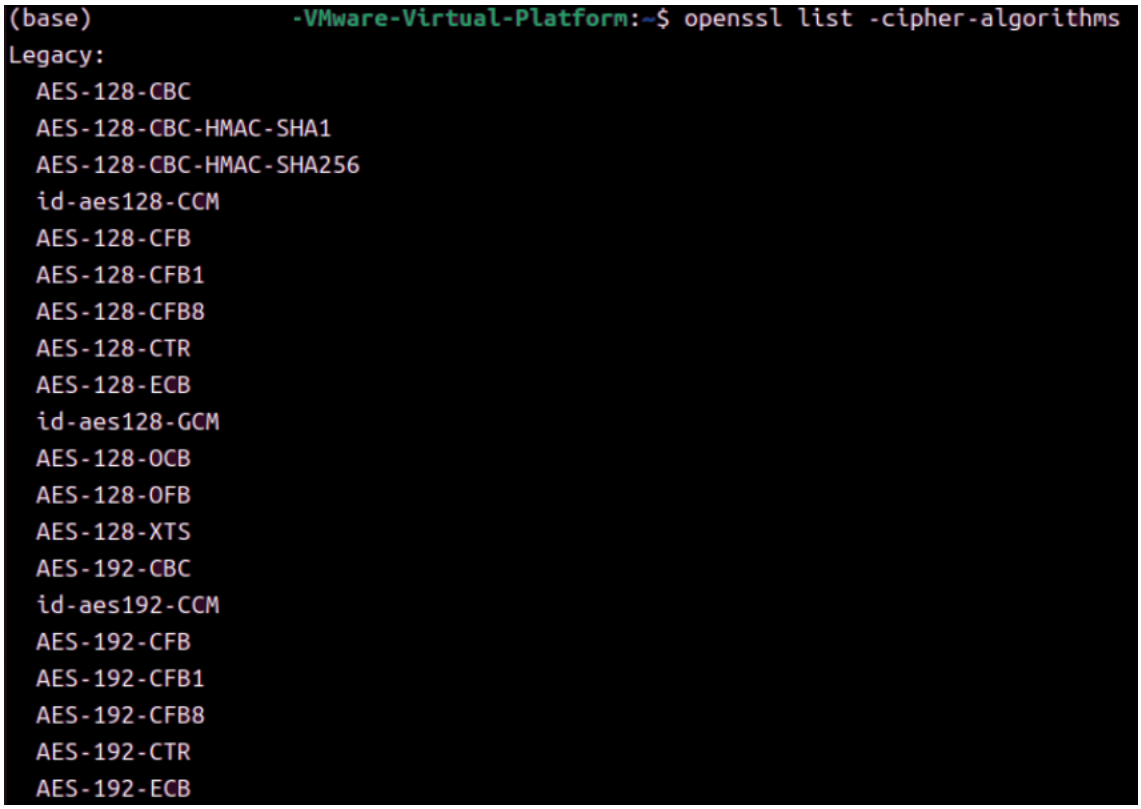


Figure 3-340 그림 제목

7.7.3 판정근거

Table 3-453 TE10.08.01 시험결과 판정근거

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

7.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.8 TE10.08.02

7.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.08.02	자가시험 실패 시 오류 상태 진입 및 오류 표시 출력	개발문서 검토

7.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-454 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

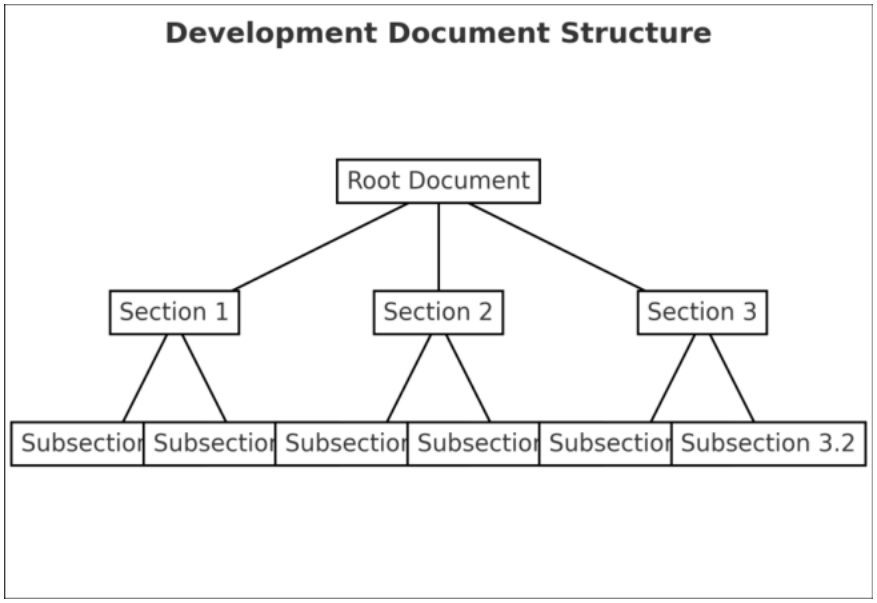


Figure 3-341 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-455 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

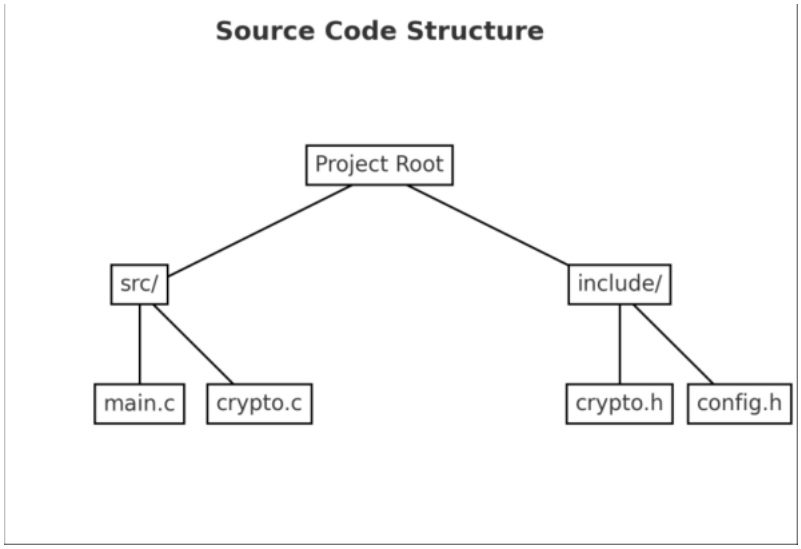


Figure 3-342 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-456 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

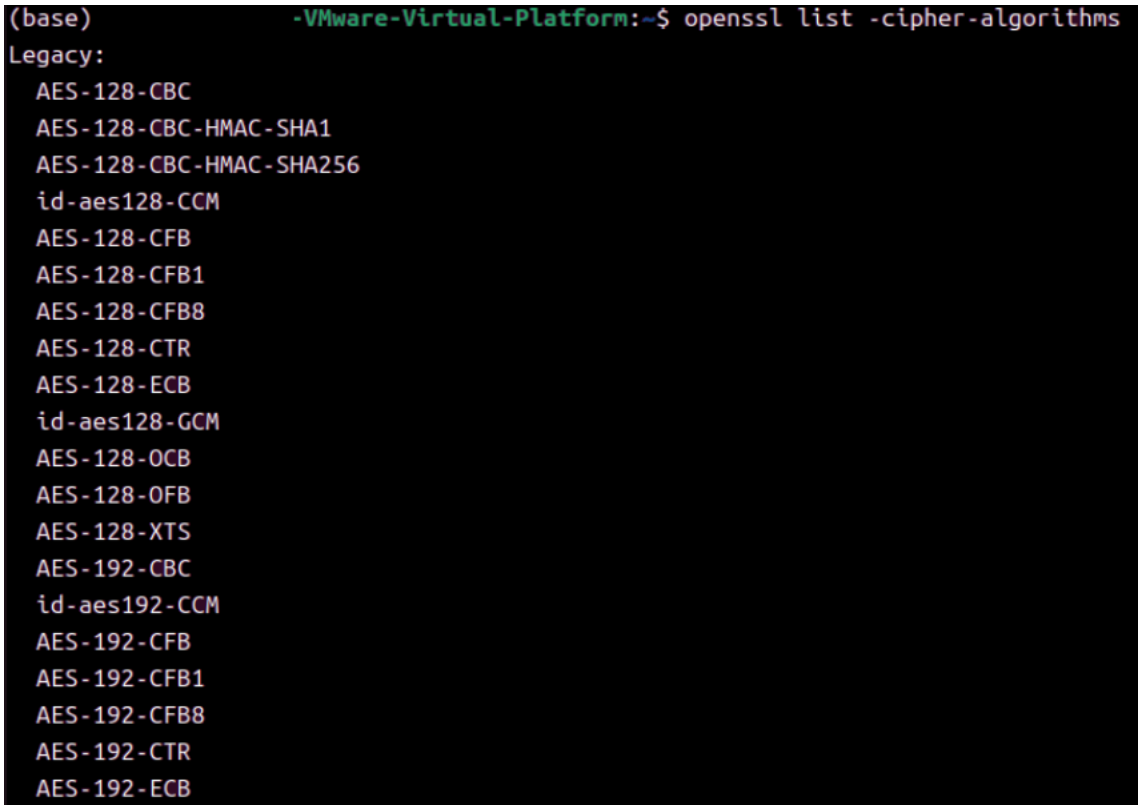


Figure 3-343 그림 제목

7.8.3 판정근거

Table 3-457 TE10.08.02 시험결과 판정근거

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

7.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.9 TE10.08.03

7.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.08.03	자가시험 오류 상태 시 오류 표시 명세와 일치 여부	암호모듈 검사

7.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-458 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

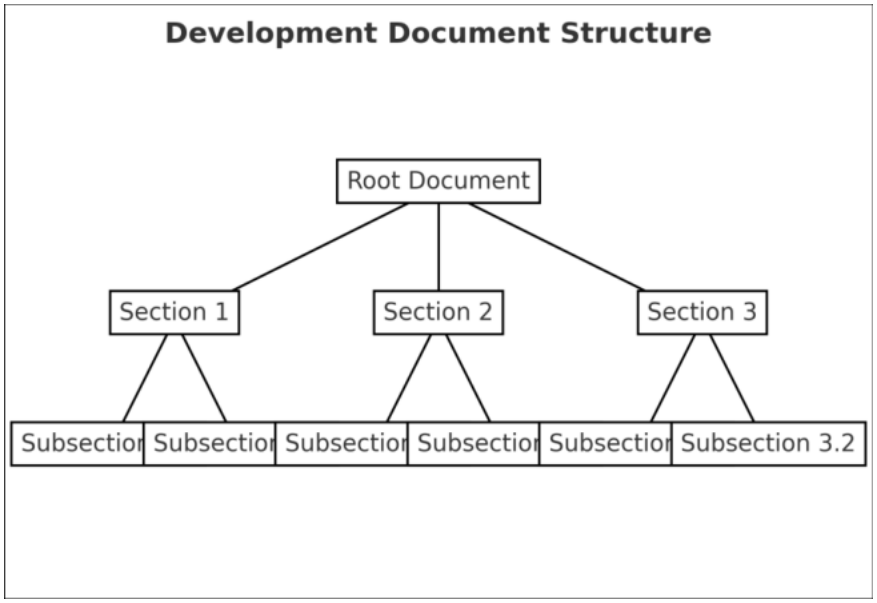


Figure 3-344 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-459 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

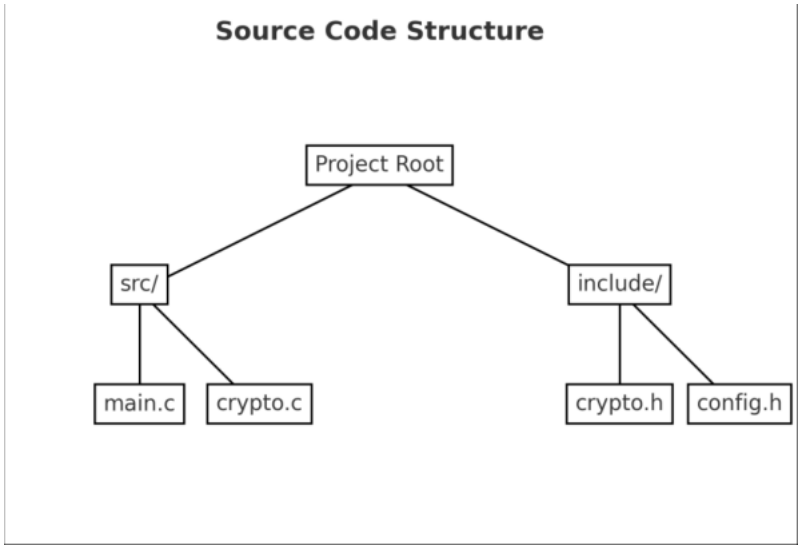


Figure 3-345 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-460 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

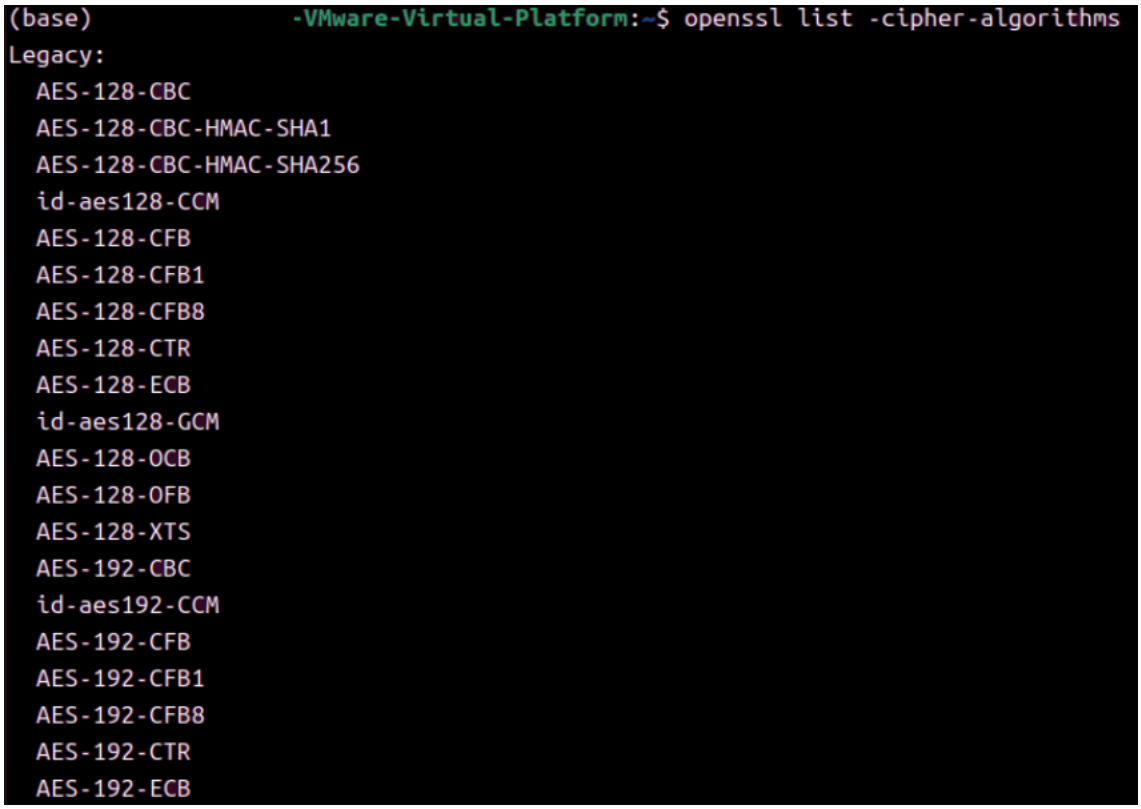


Figure 3-346 그림 제목

7.9.3 판정근거

Table 3-461 TE10.08.03 시험결과 판정근거

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

7.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.10 TE10.09.01

7.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.09.01	오류 상태에서 제어 및 데이터 출력 금지	암호모듈 검사

7.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-462 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

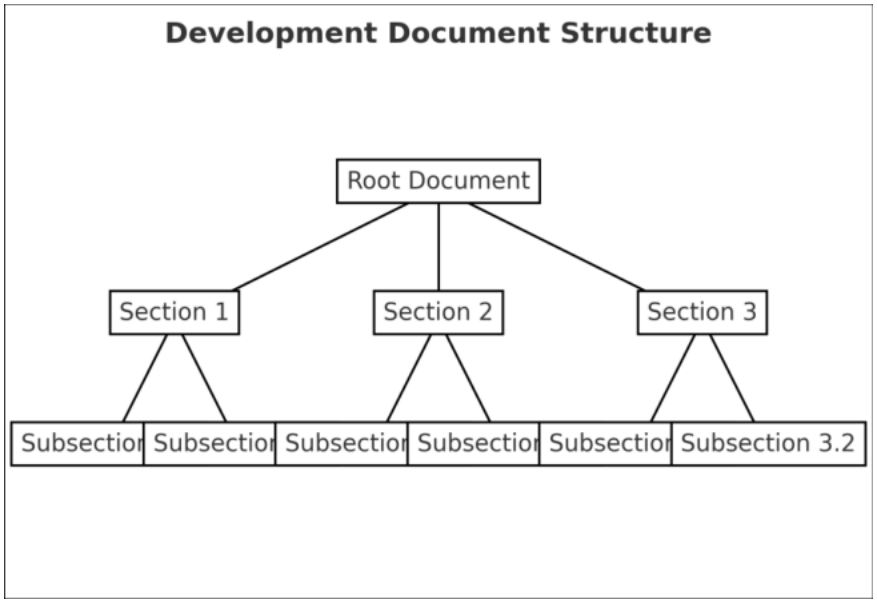


Figure 3-347 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-463 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

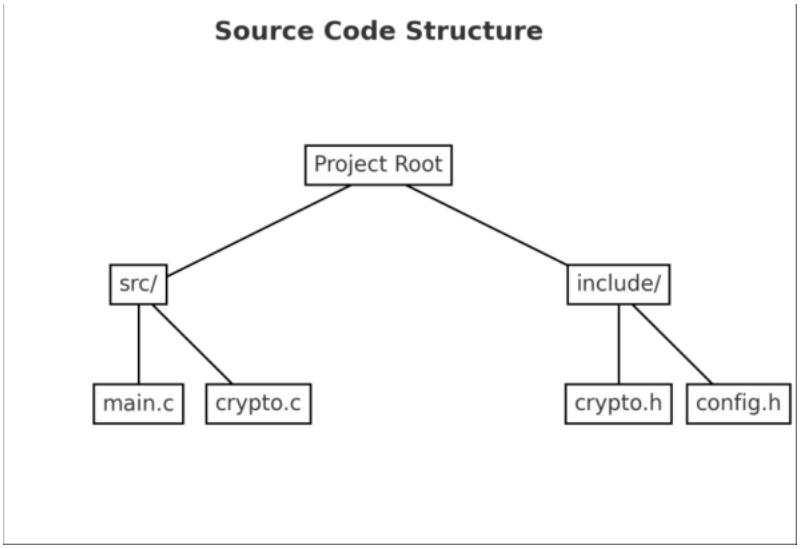


Figure 3-348 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-464 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

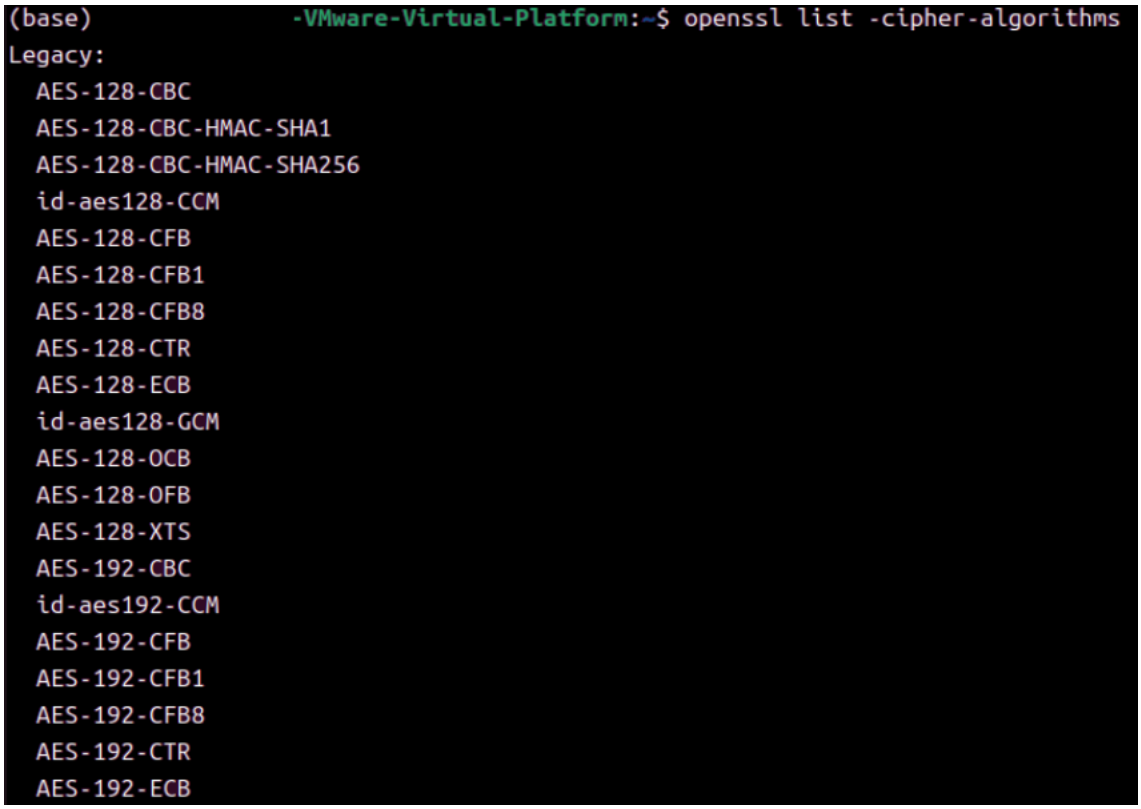


Figure 3-349 그림 제목

7.10.3 판정근거

Table 3-465 TE10.09.01 시험결과 판정근거

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

7.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.11 TE10.09.02

7.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.09.02	오류 상태에서 암호 기능 금지	개발문서 검토

7.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-466 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

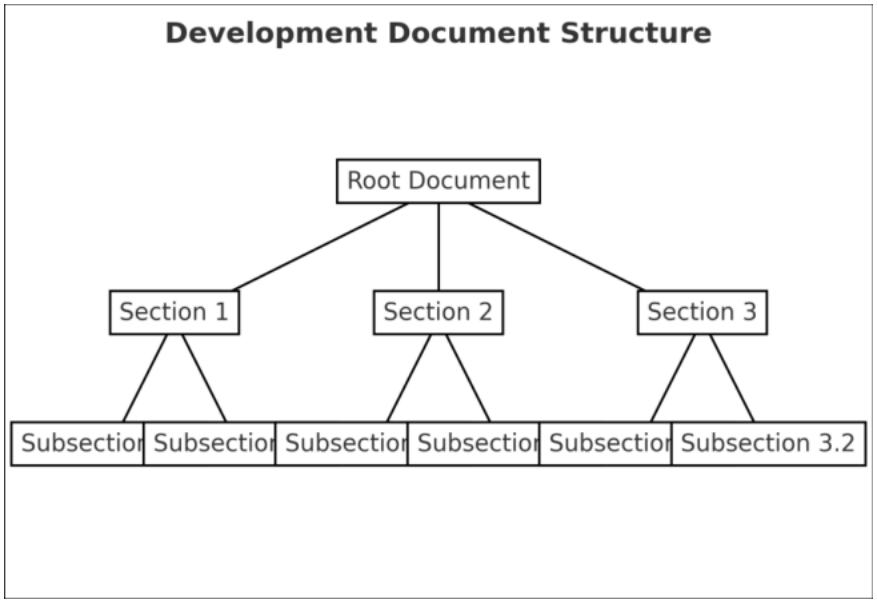


Figure 3-350 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-467 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

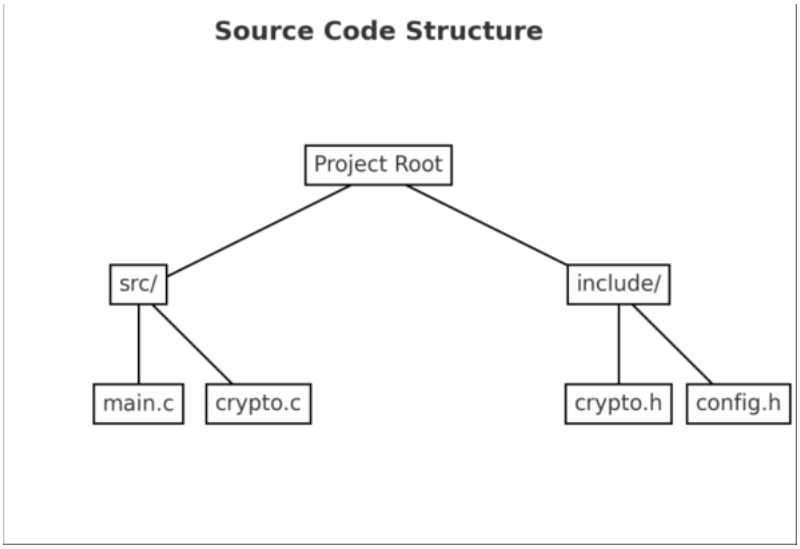


Figure 3-351 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-468 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

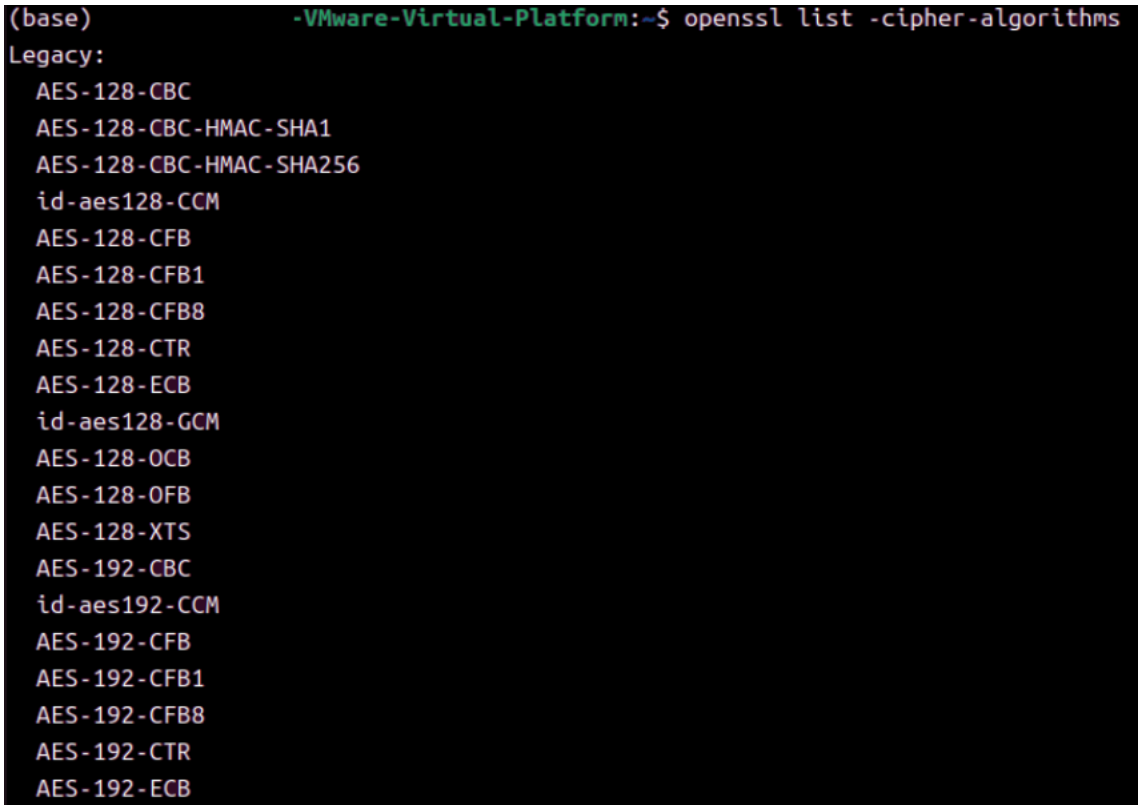


Figure 3-352 그림 제목

7.11.3 판정근거

Table 3-469 TE10.09.02 시험결과 판정근거

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

7.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.12 TE10.09.03

7.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.09.03	오류 상태 진입 및 암호 기능 수행 여부 확인	암호모듈 검사

7.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-470 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

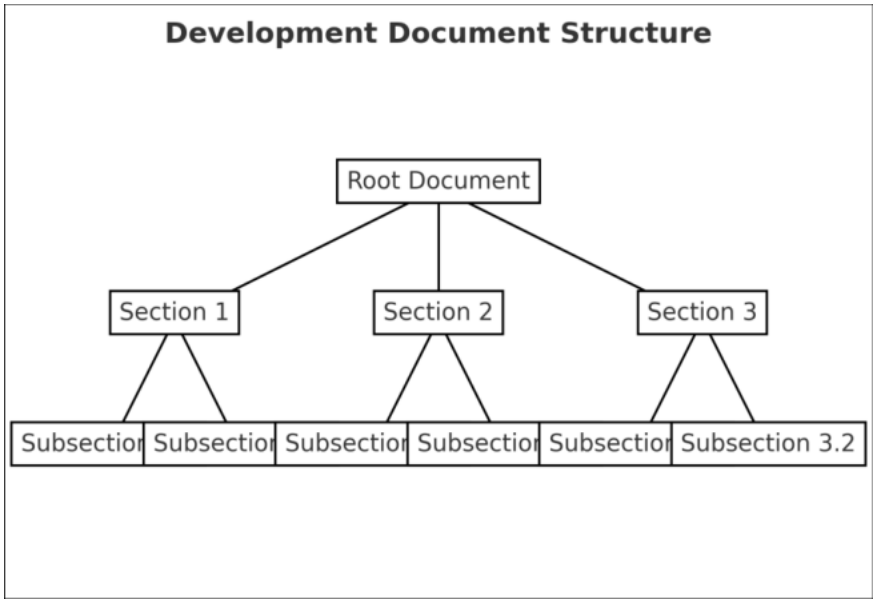


Figure 3-353 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-471 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

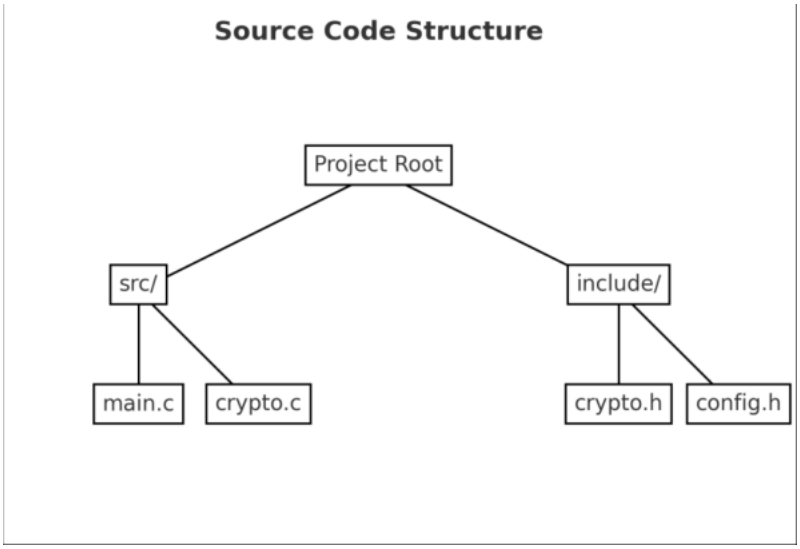


Figure 3-354 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-472 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

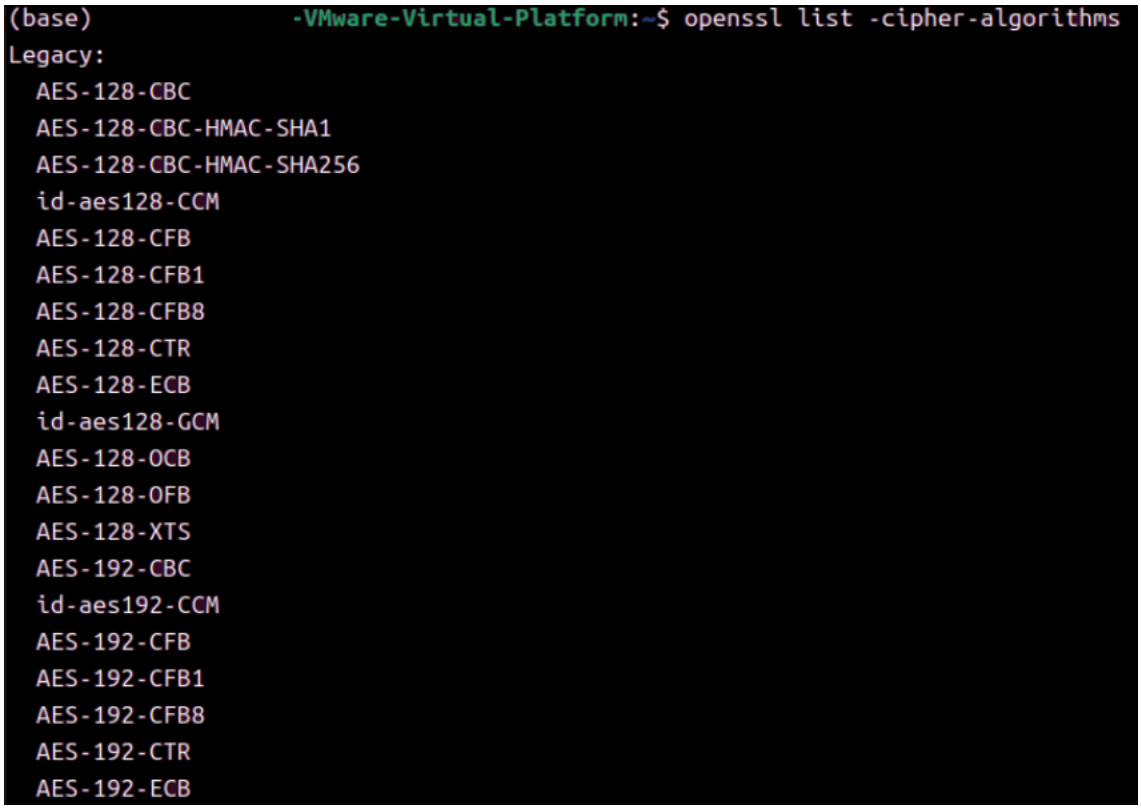


Figure 3-355 그림 제목

7.12.3 판정근거

Table 3-473 TE10.09.03 시험결과 판정근거

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

7.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.13 TE10.10.01

7.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.10.01	알고리즘 자가시험 실패 시 암호기능 수행 불가	암호모듈 검사

7.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-474 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

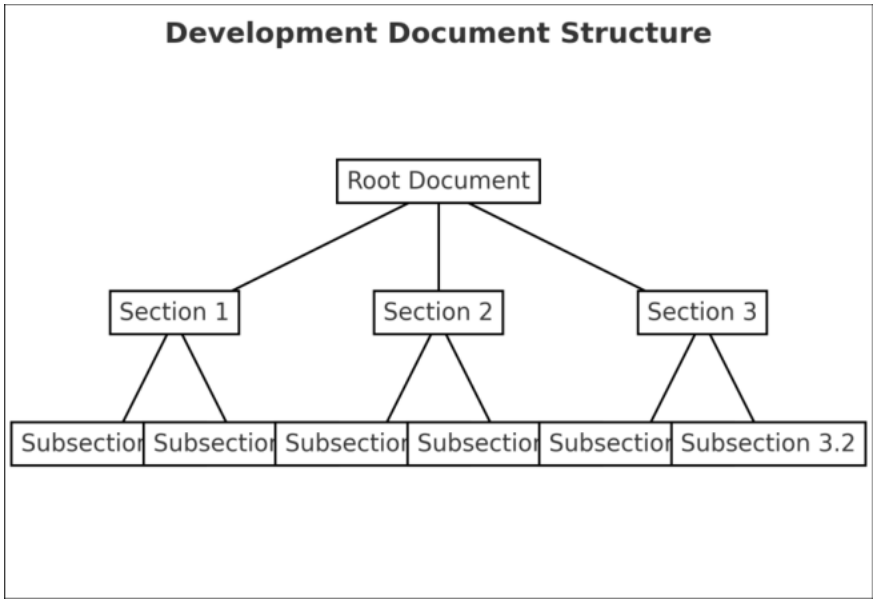


Figure 3-356 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-475 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

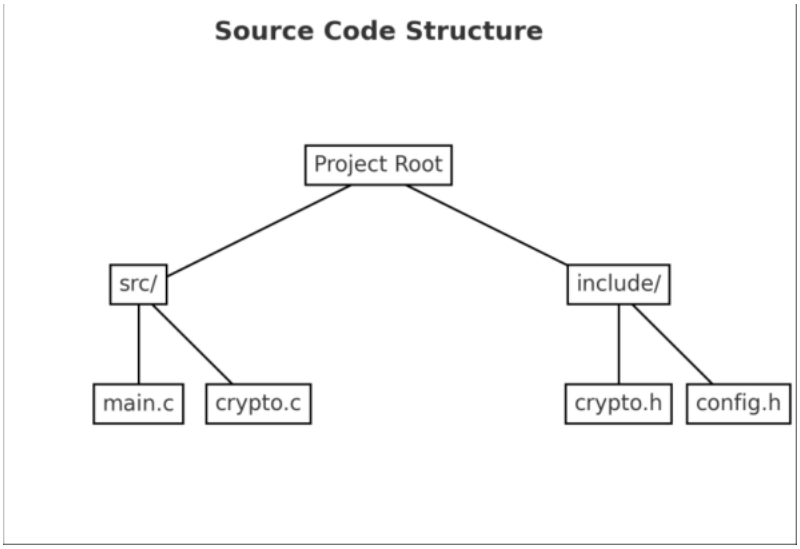


Figure 3-357 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-476 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

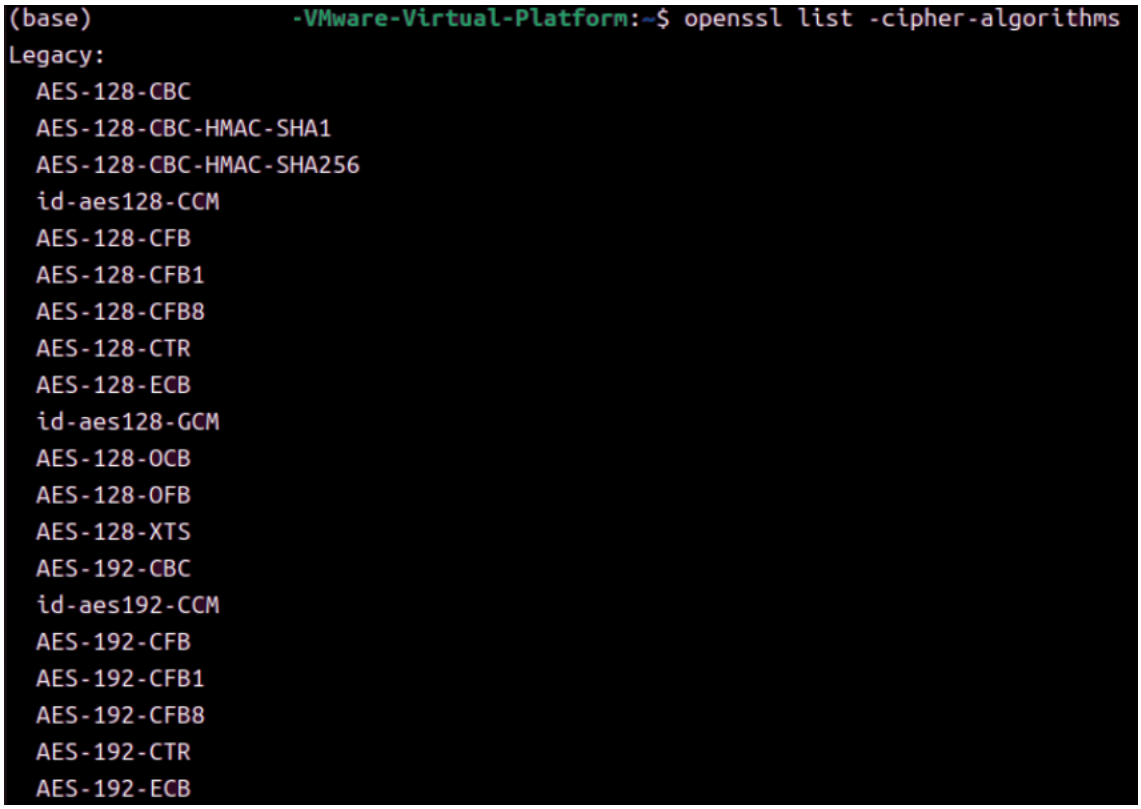


Figure 3-358 그림 제목

7.13.3 판정근거

Table 3-477 TE10.09.03 시험결과 판정근거

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

7.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.14 TE10.10.01

7.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.10.01	알고리즘 자가시험 실패 시 암호기능 수행 불가	암호모듈 검사

7.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-478 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

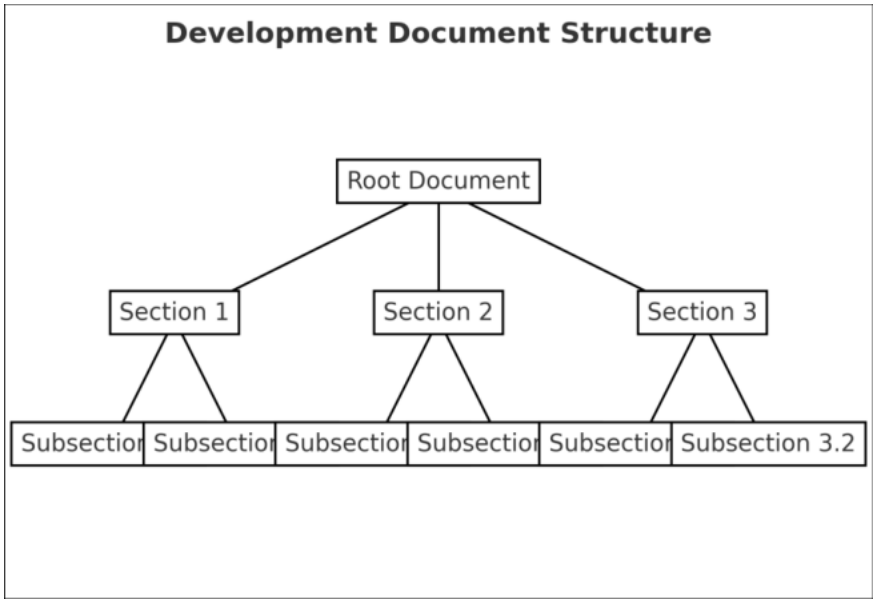


Figure 3-359 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-479 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

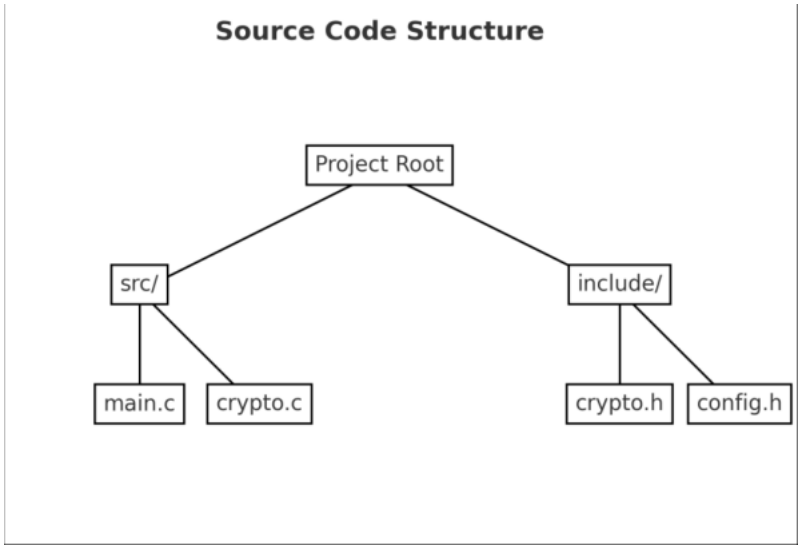


Figure 3-360 그림 제목

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-480 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

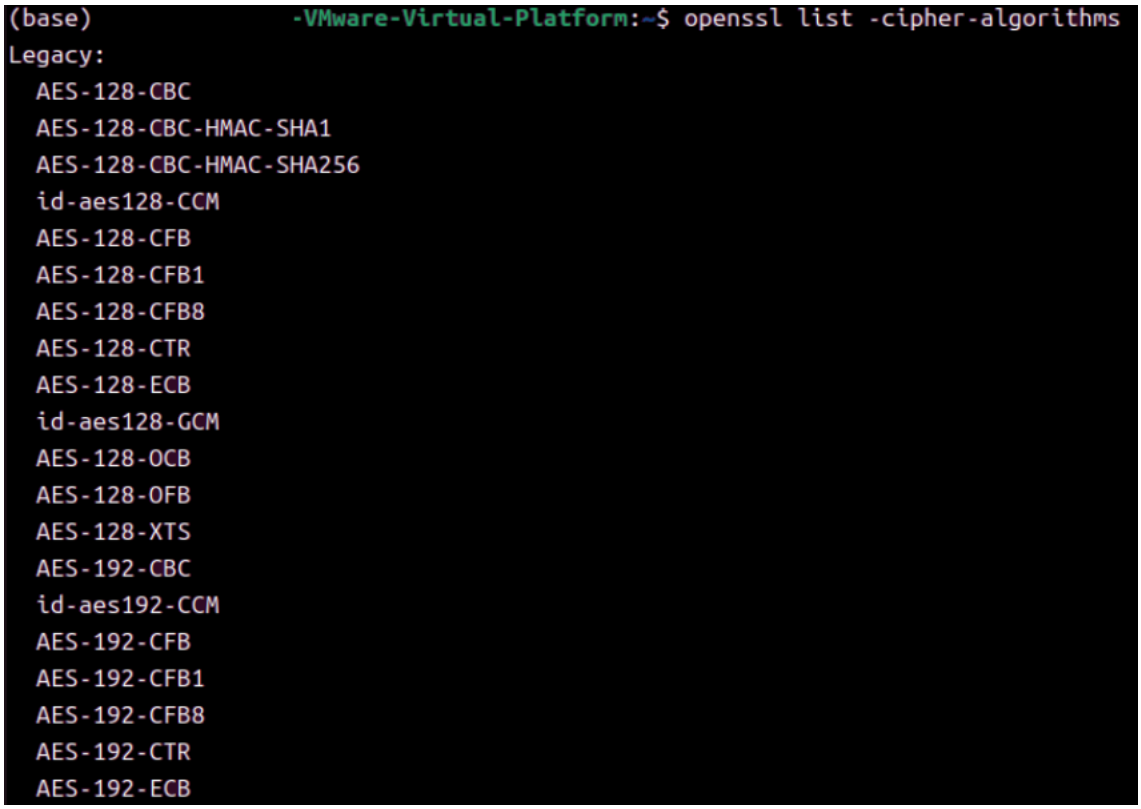


Figure 3-361 그림 제목

7.14.3 판정근거

Table 3-481 TE10.10.01 시험결과 판정근거

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

7.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.15 TE10.10.02

7.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.10.02	자가시험 반복하여 성공할 때까지 해당 알고리즘 암호기능 수행 불가	암호모듈 검사

7.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-482 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

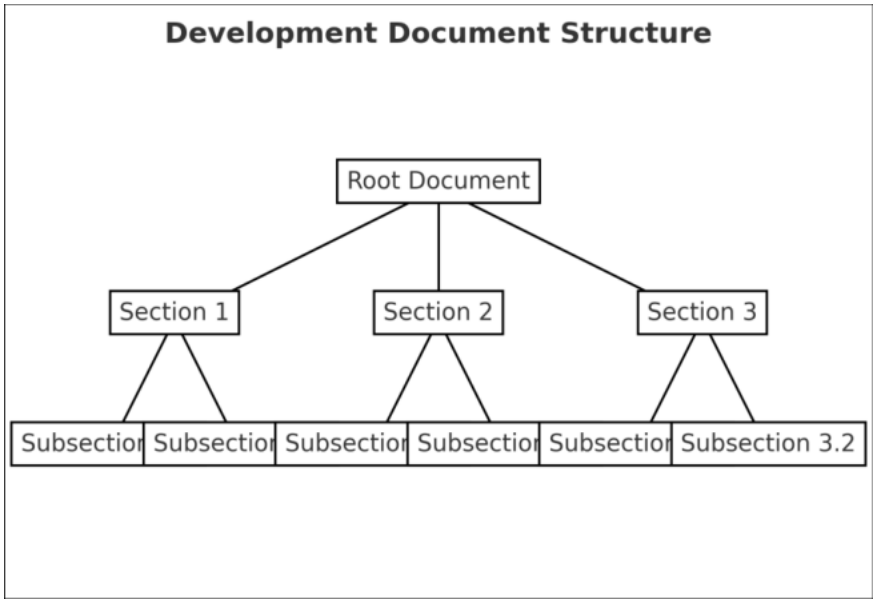


Figure 3-362 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-483 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

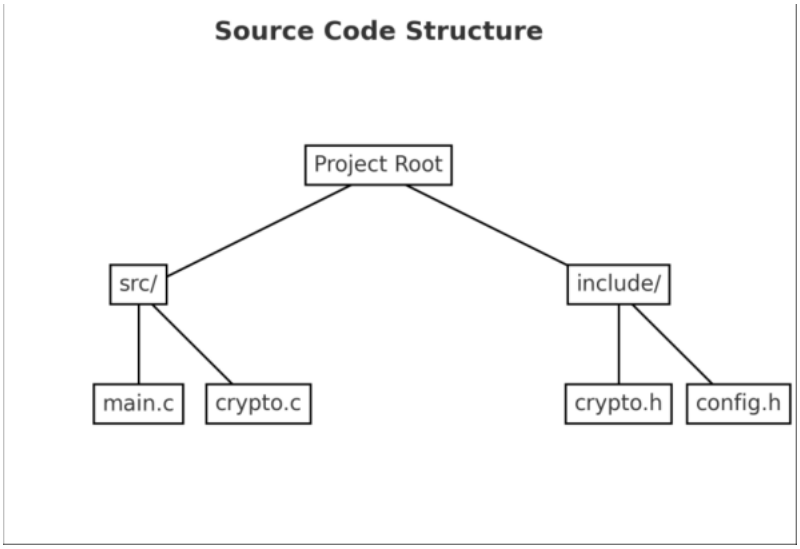


Figure 3-363 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-484 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

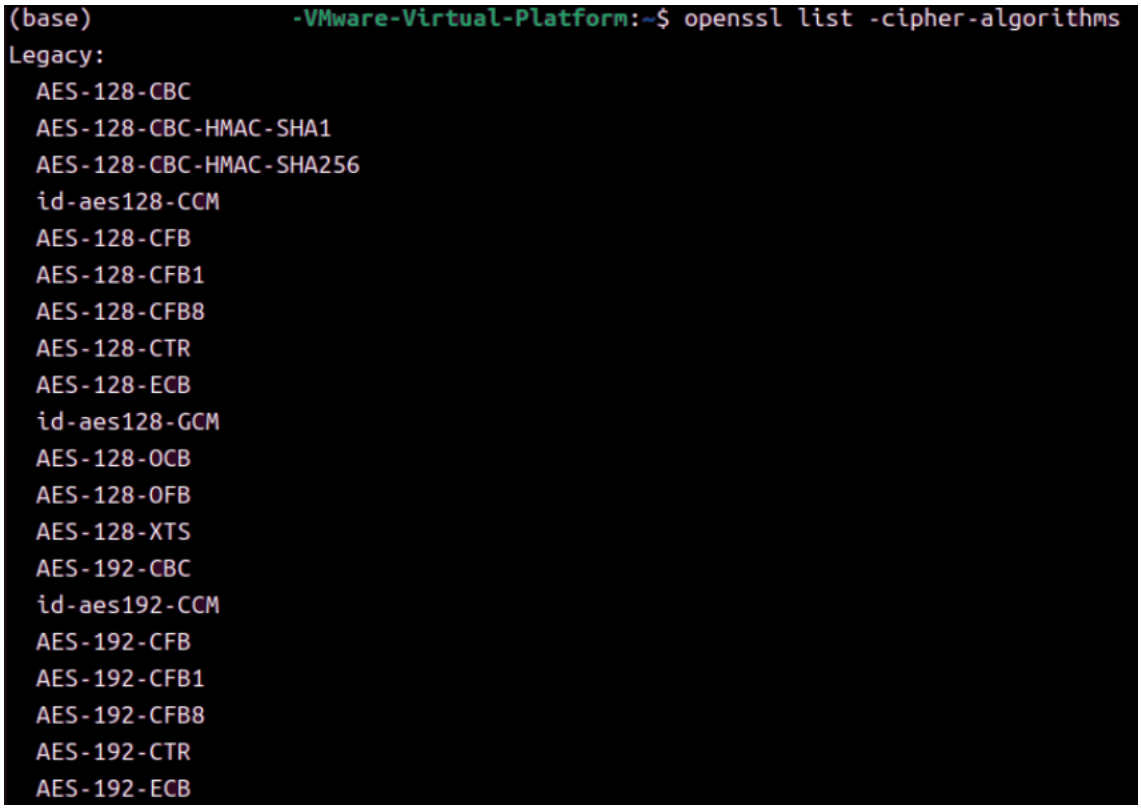


Figure 3-364 그림 제목

7.15.3 판정근거

Table 3-485 TE10.10.02 시험결과 판정근거

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

7.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.16 TE10.11.01

7.16.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.11.01	자가시험 실패 오류 상태 미출력 시 오류 상태 진입 여부를 결정하기 위한 절차 존재 확인	암호모듈 검사

7.16.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-486 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

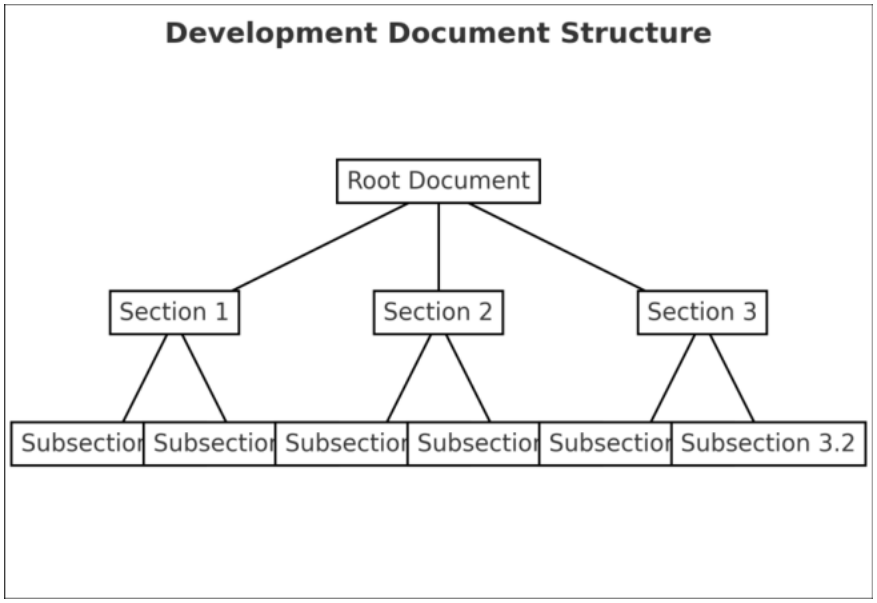


Figure 3-365 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-487 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

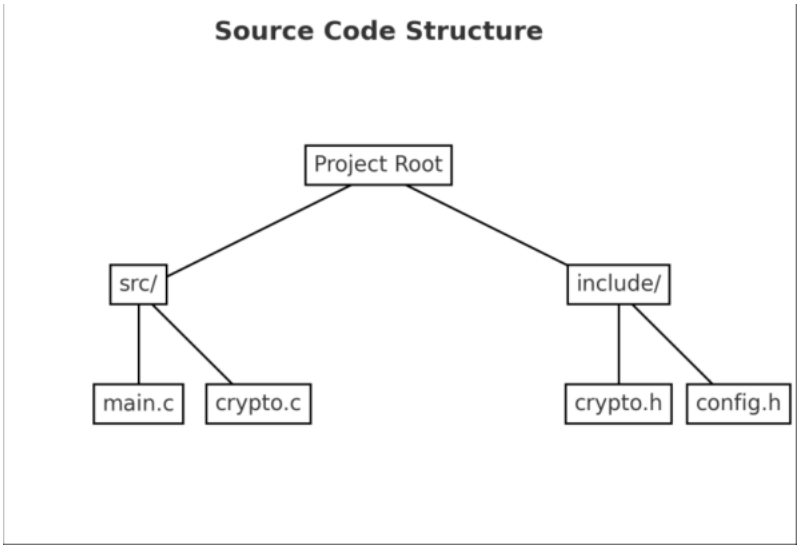


Figure 3-366 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-488 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

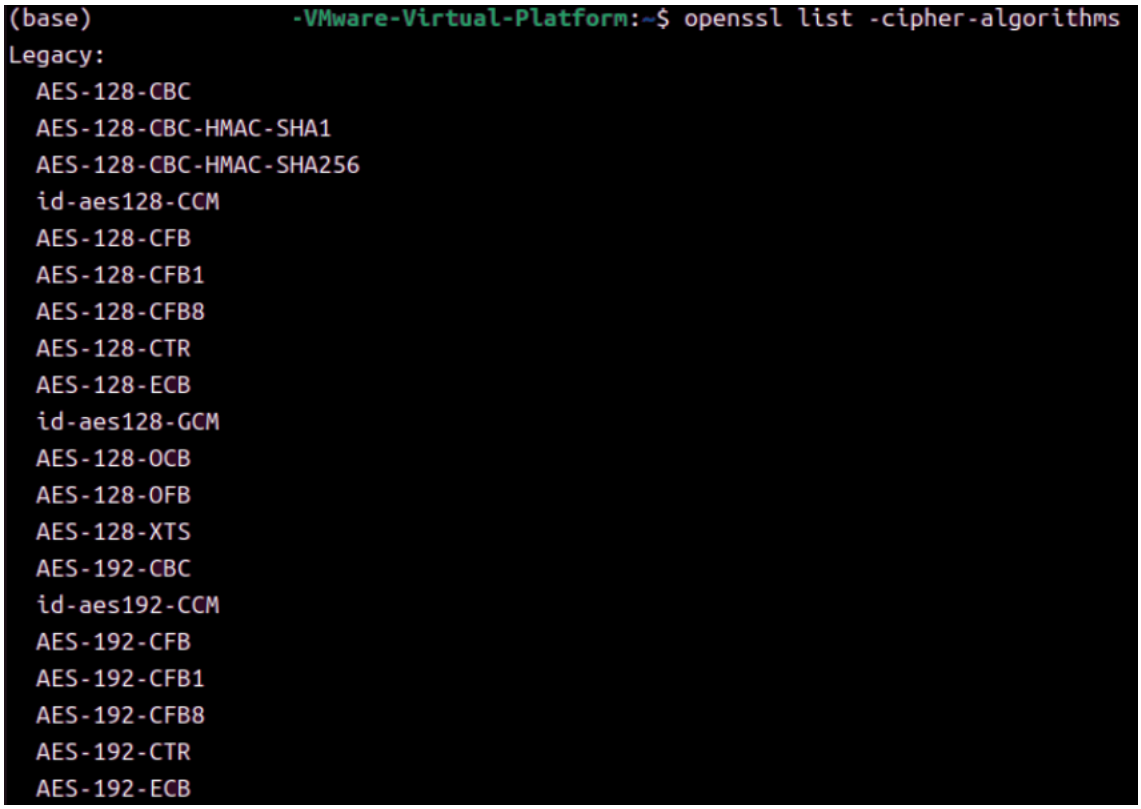


Figure 3-367 그림 제목

7.16.3 판정근거

Table 3-489 TE10.11.01 시험결과 판정근거

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

7.16.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.17 TE10.15.01

7.17.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.15.01	동작 전 자가시험 명세 여부	개발문서 검토

7.17.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-490 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

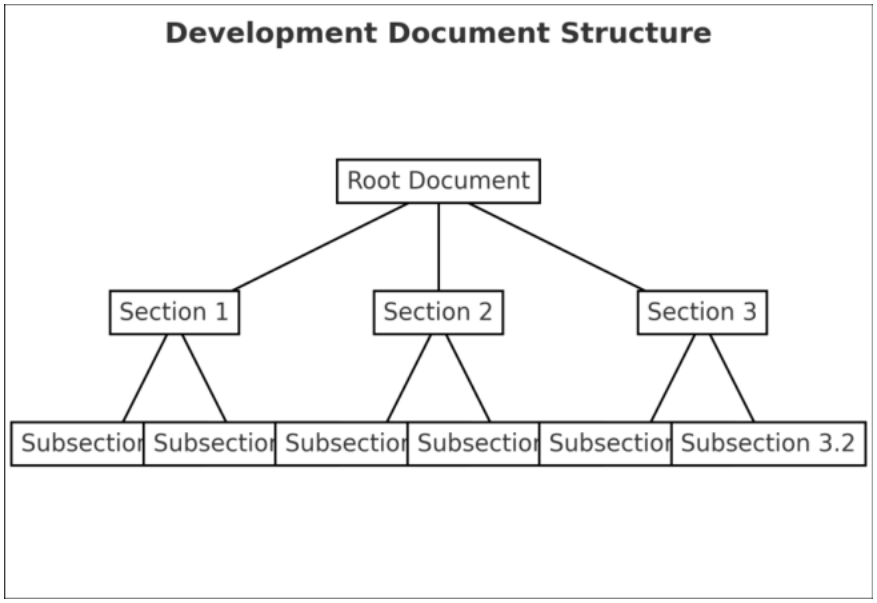


Figure 3-368 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-491 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

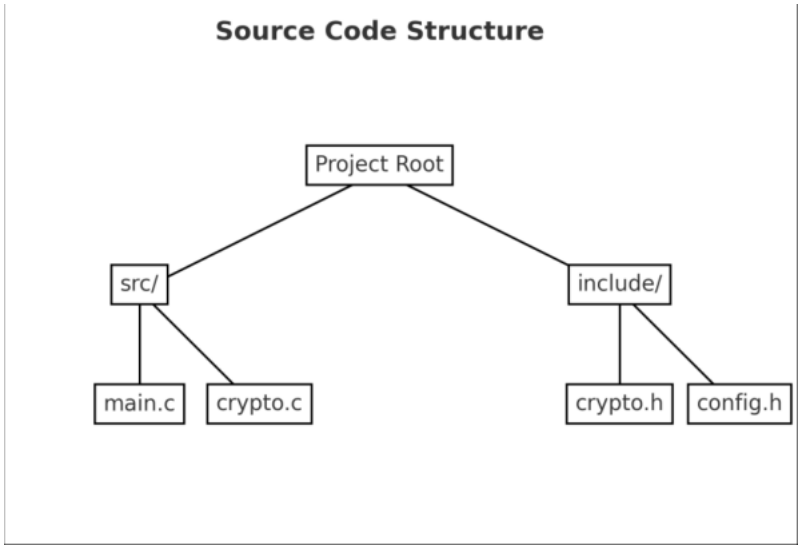


Figure 3-369 그림 제목

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-492 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

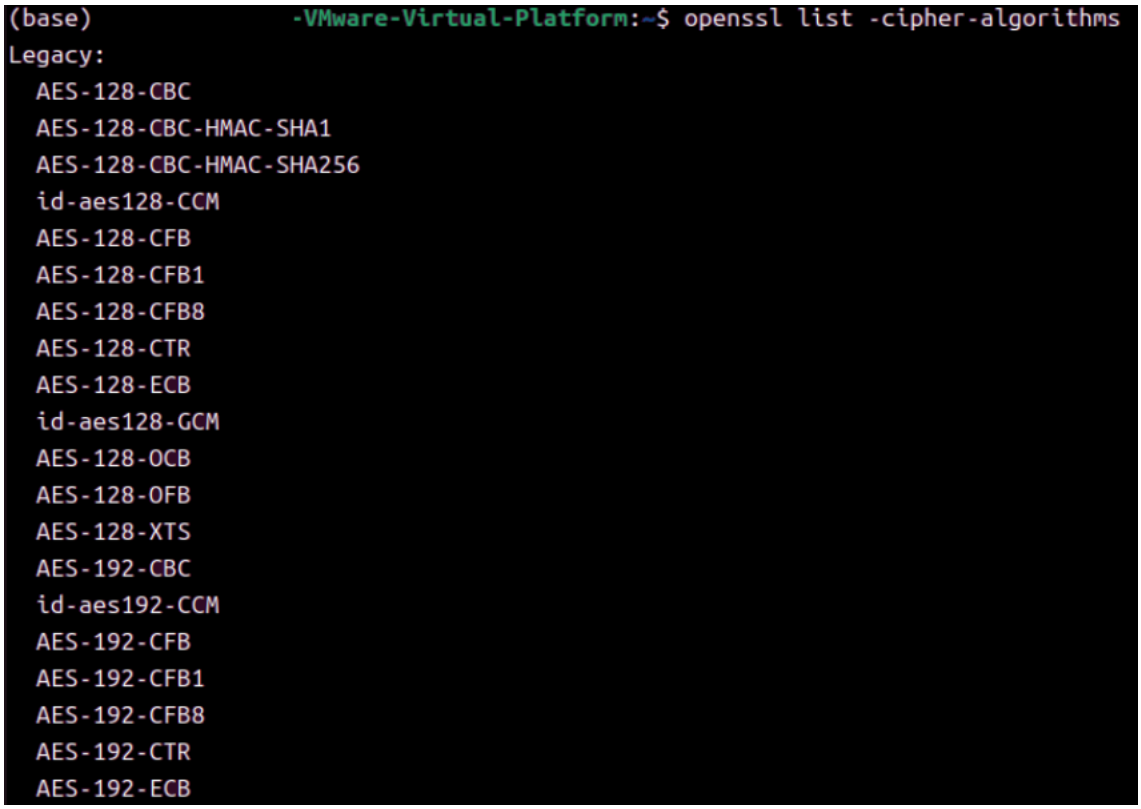


Figure 3-370 그림 제목

7.17.3 판정근거

Table 3-493 TE10.15.01 시험결과 판정근거

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

7.17.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.18 TE10.15.02

7.18.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.15.02	동작 전 자가시험이 전원인가 (또는 인스턴스화) 시점과 동작 상태로 전이되는 시점 사이에 수행 여부	암호모듈 검사

7.18.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-494 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

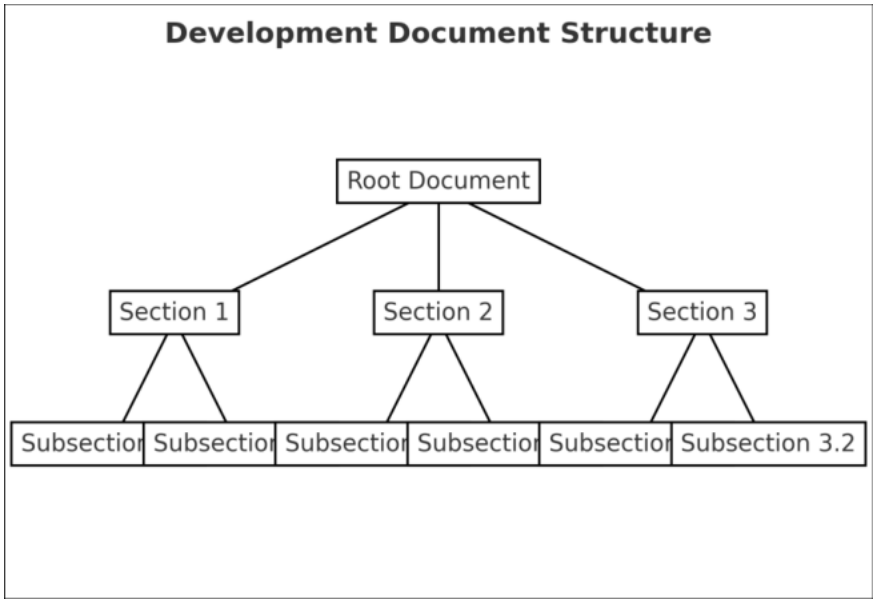


Figure 3-371 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-495 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

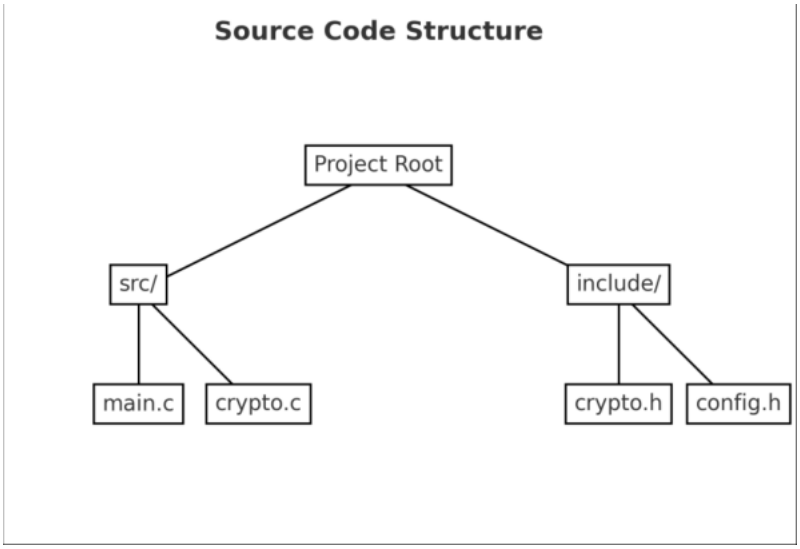


Figure 3-372 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-496 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

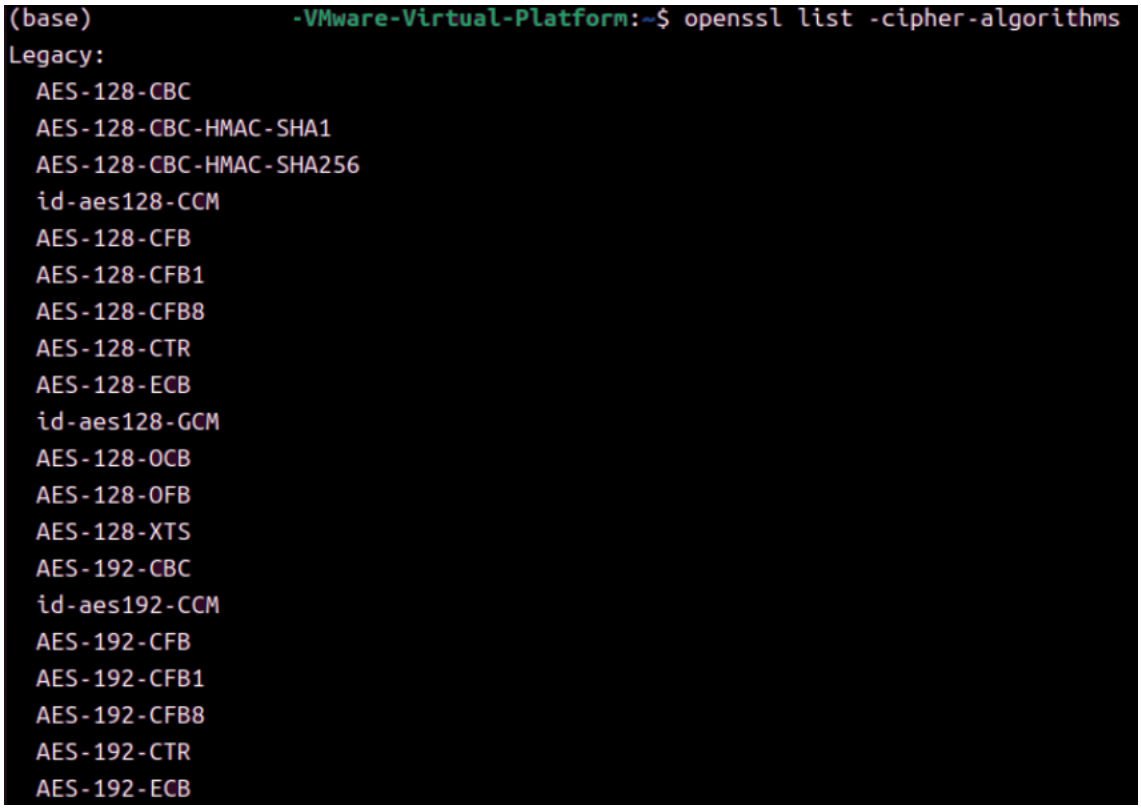


Figure 3-373 그림 제목

7.18.3 판정근거

Table 3-497 TE10.15.02 시험결과 판정근거

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

7.18.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.19 TE10.17.01

7.19.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.17.01	무결성 검증 기술의 구현적합성 검증 성공 여부	개발문서 검토

7.19.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-498 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

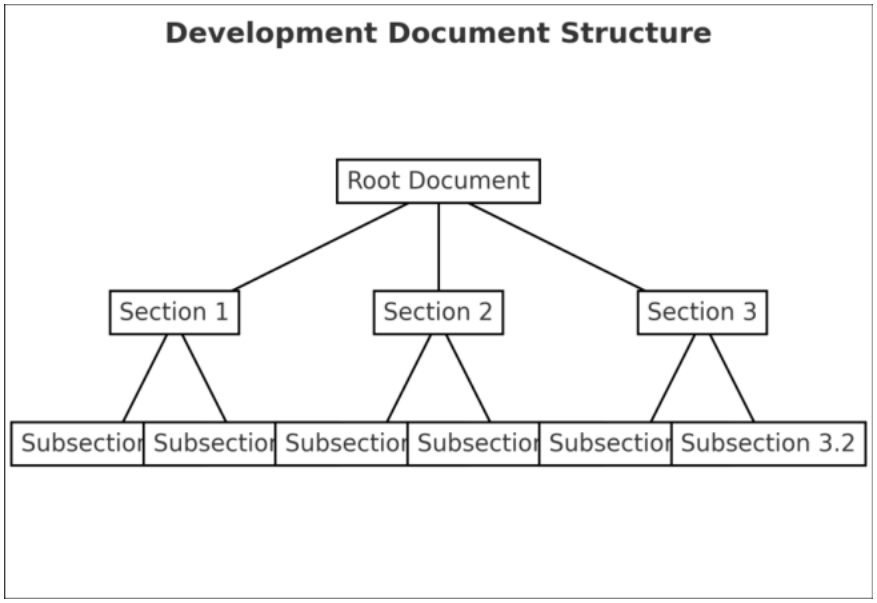


Figure 3-374 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-499 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

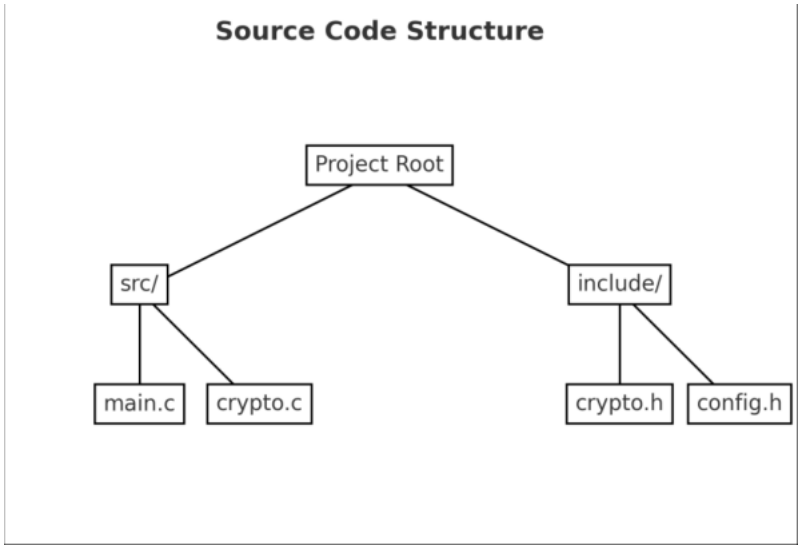


Figure 3-375 그림 제목

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-500 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

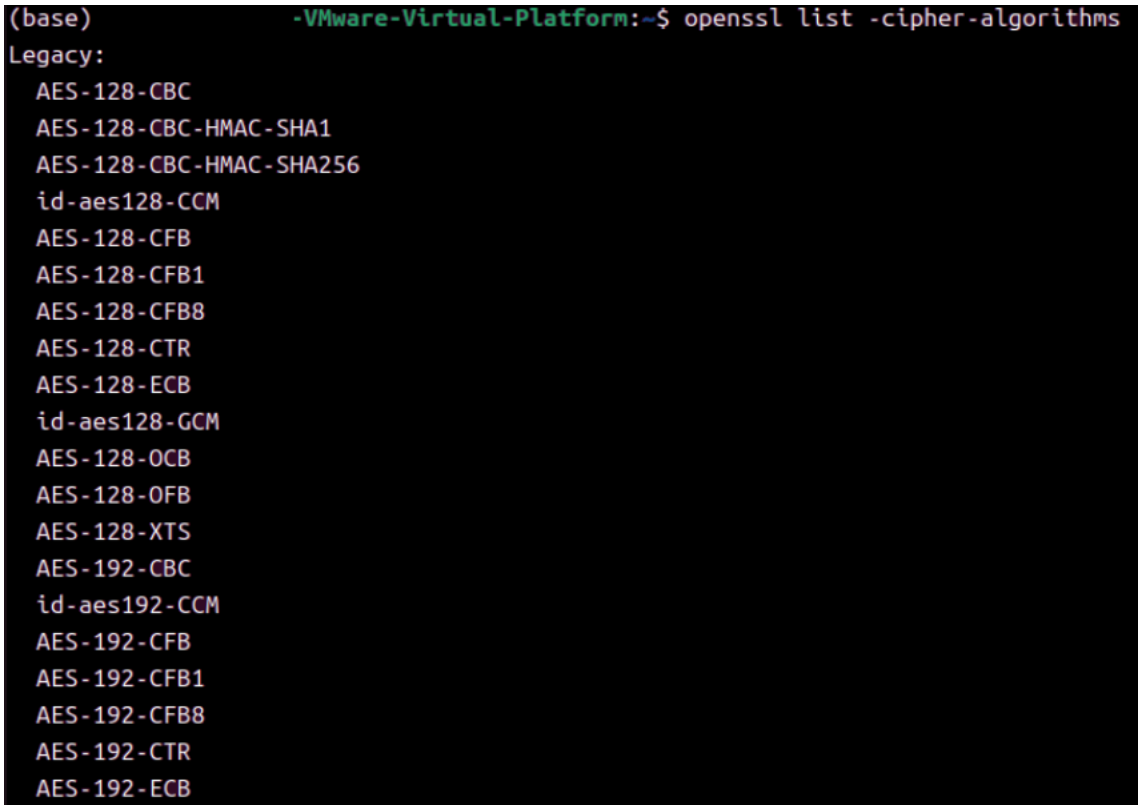


Figure 3-376 그림 제목

7.19.3 판정근거

Table 3-501 TE10.17.01 시험결과 판정근거

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

7.19.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.20 TE10.17.02

7.20.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.17.02	무결성 시험에 사용된 Hash 와 MAC 확인 과정 서술	개발문서 검토

7.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-502 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

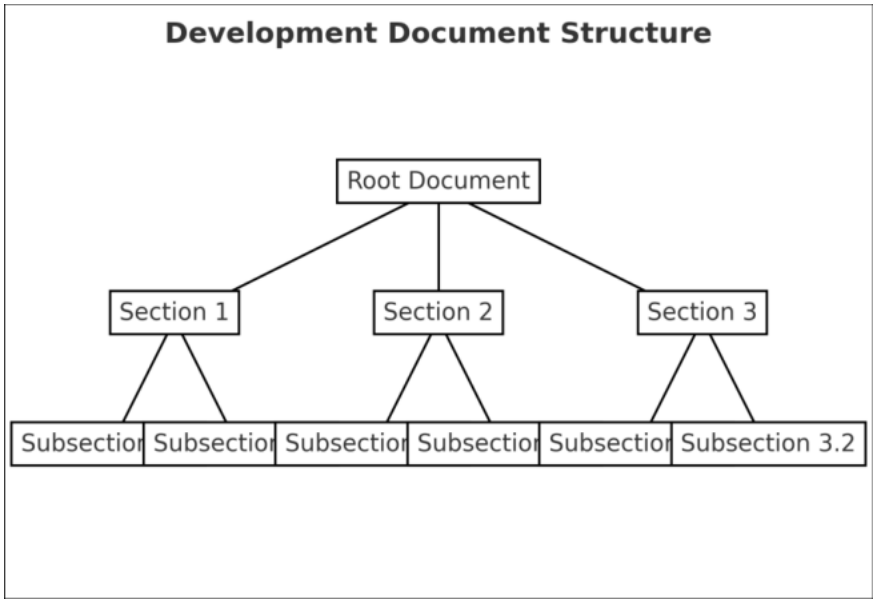


Figure 3-377 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-503 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

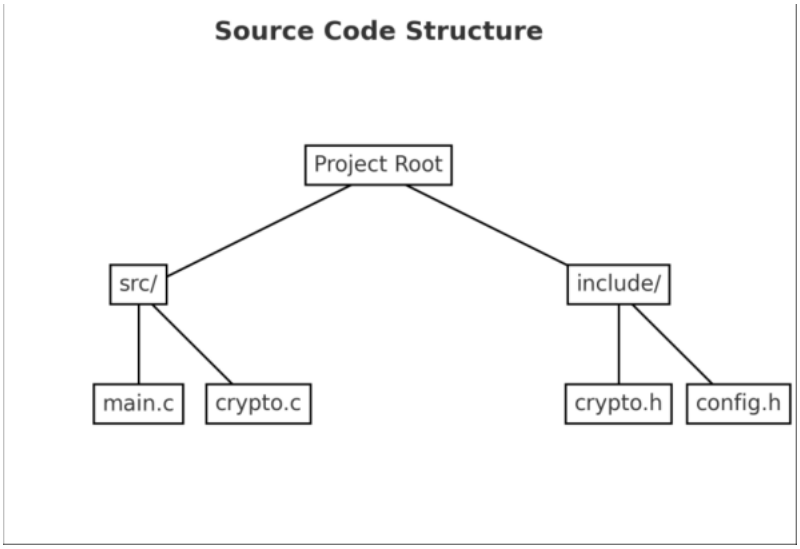


Figure 3-378 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-504 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

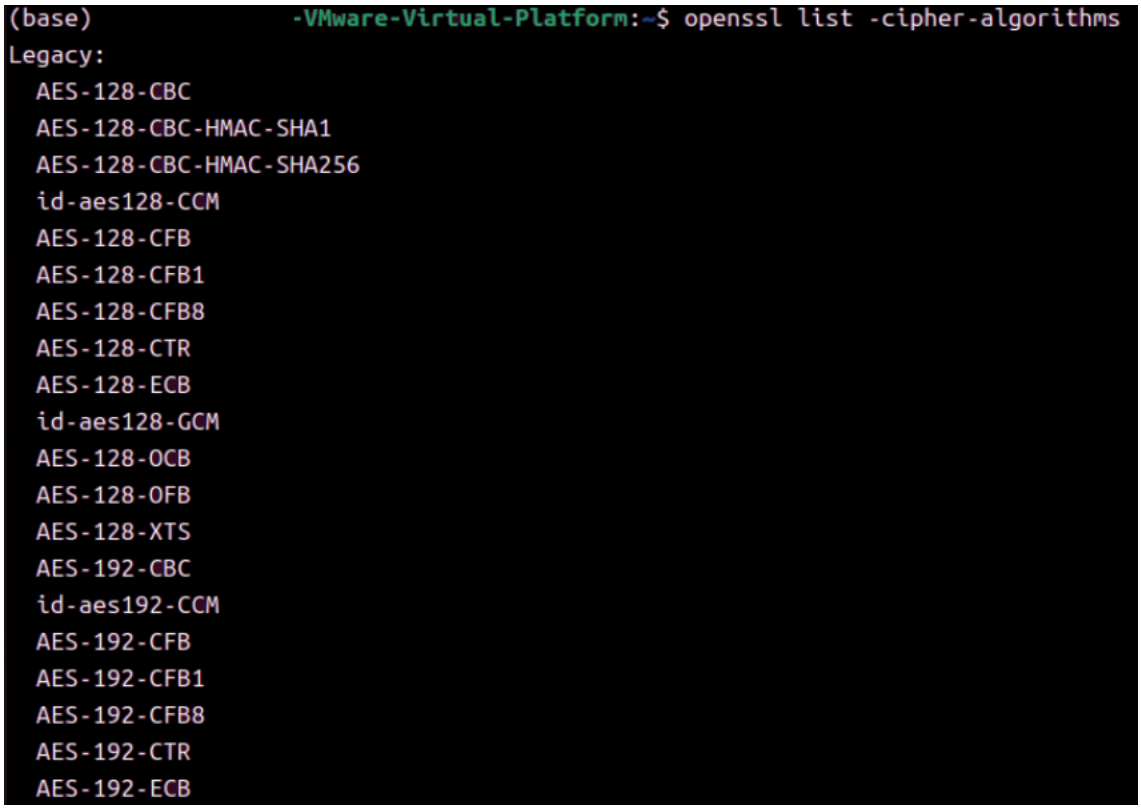


Figure 3-379 그림 제목

7.20.3 판정근거

Table 3-505 TE10.17.02 시험결과 판정근거

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

7.20.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.21 TE10.17.04

7.21.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.17.04	무결성 시험 개발문서 명세와 구현 일치	암호모듈 검사

7.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-506 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

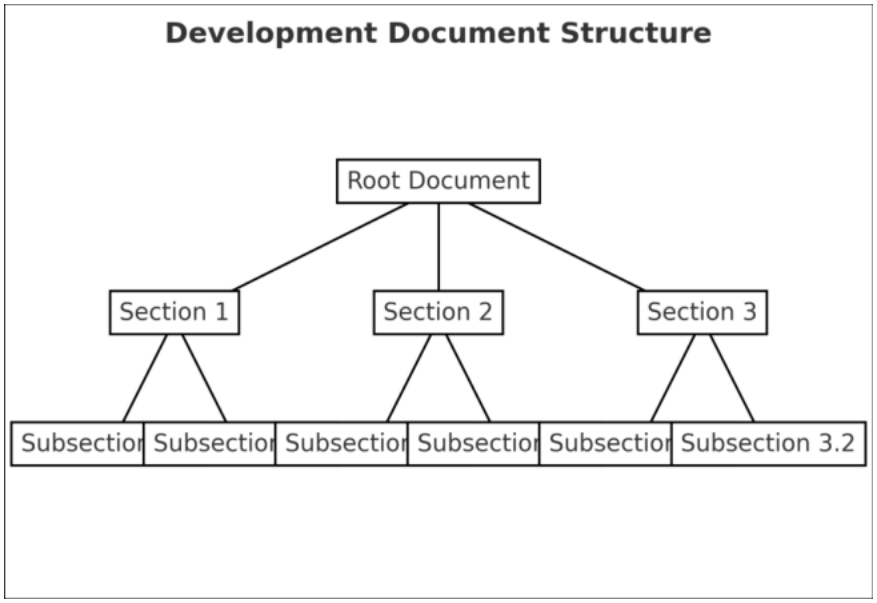


Figure 3-380 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-507 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

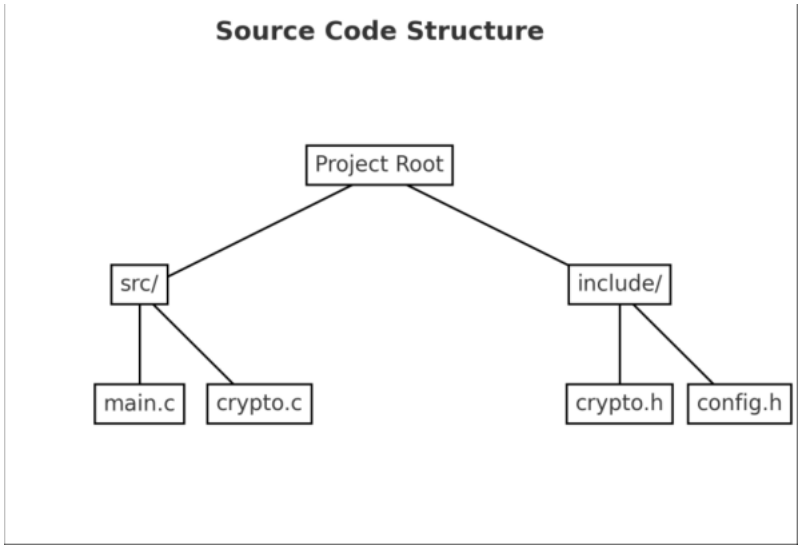


Figure 3-381 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-508 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

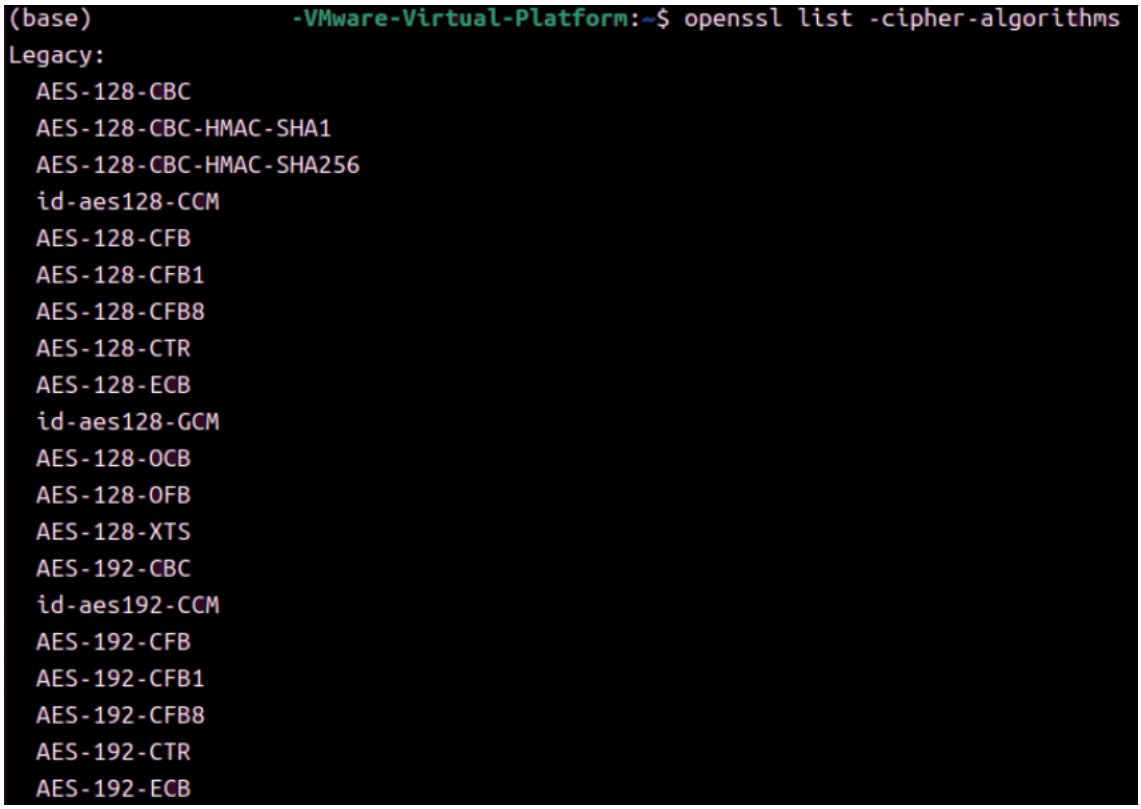


Figure 3-382 그림 제목

7.21.3 판정근거

Table 3-509 TE10.17.04 시험결과 판정근거

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

7.21.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.22 TE10.17.06

7.22.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.17.06	암호모듈 변조하여 무결성 탐지 여부 확인	암호모듈 검사

7.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-510 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

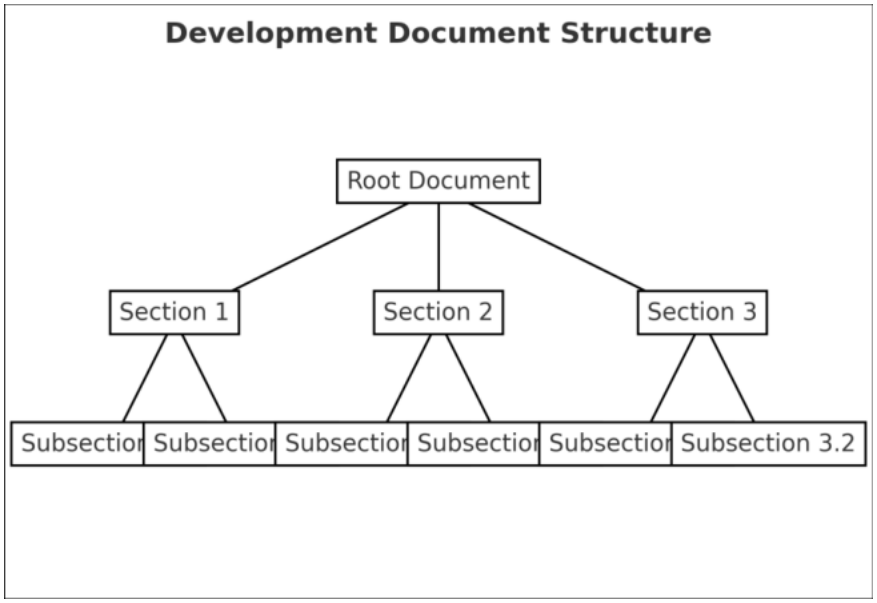


Figure 3-383 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-511 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

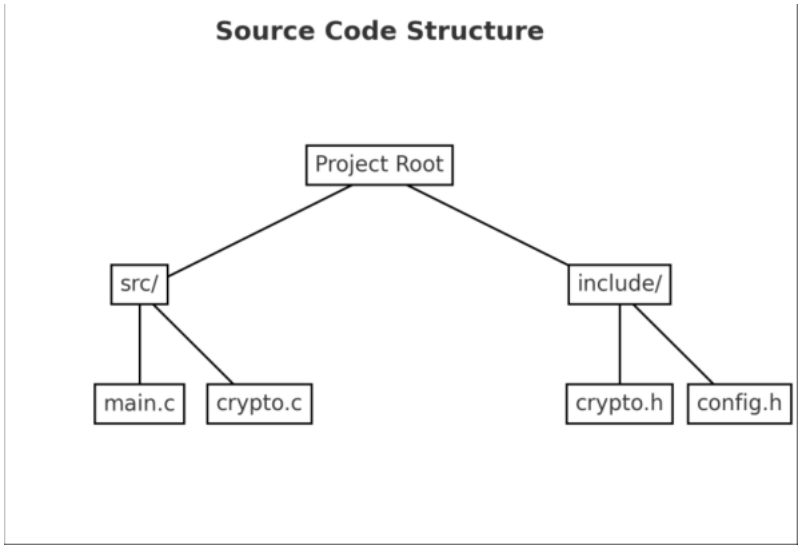


Figure 3-384 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-512 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

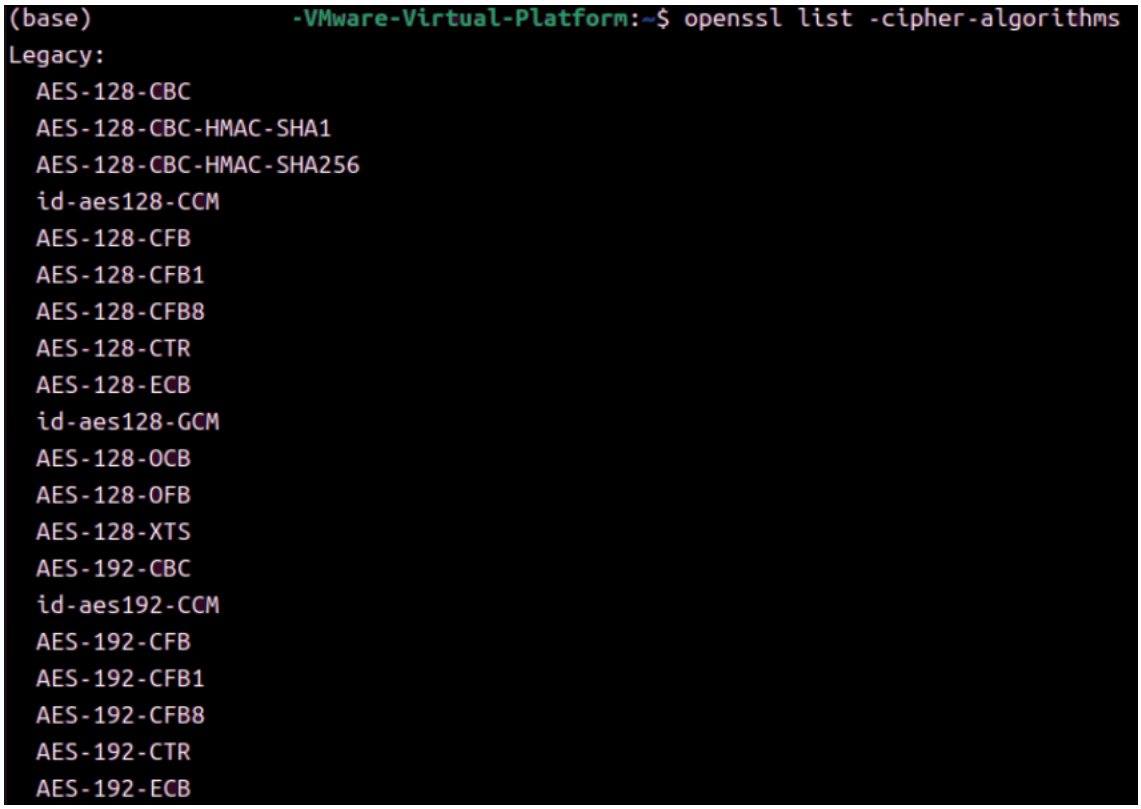


Figure 3-385 그림 제목

7.22.3 판정근거

Table 3-513 TE10.17.06 시험결과 판정근거

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

7.22.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.23 TE10.20.01

7.23.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.20.01	무결성 시험 전 무결성 기술 암호알고리즘 시험 통과	암호모듈 검사

7.23.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-514 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

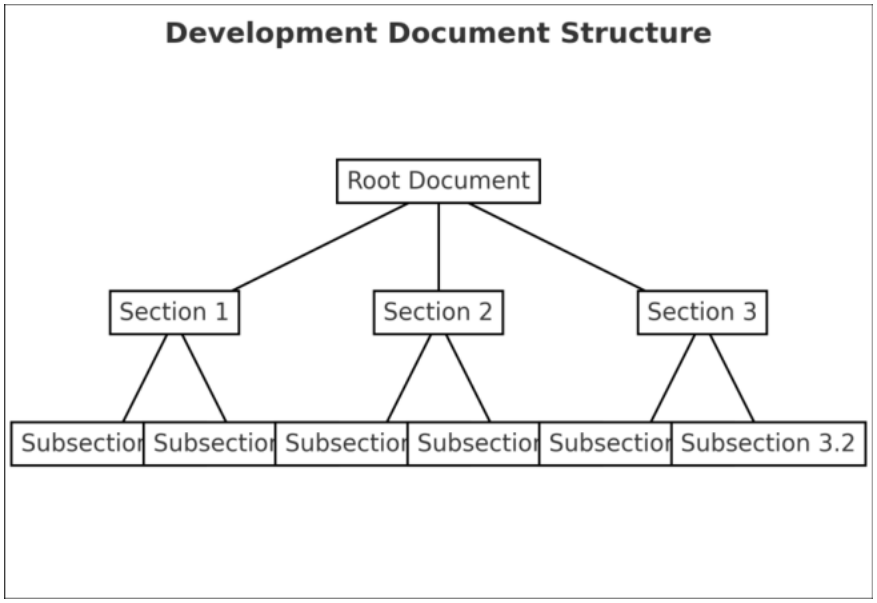


Figure 3-386 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-515 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

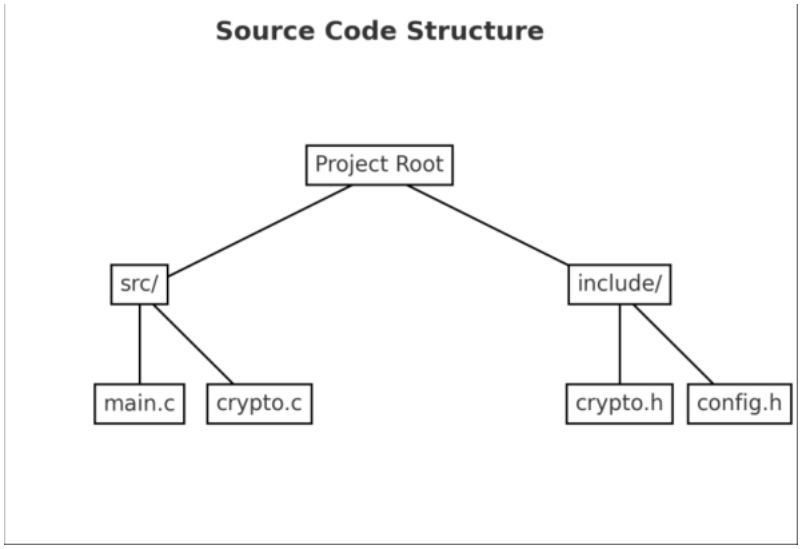


Figure 3-387 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-516 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

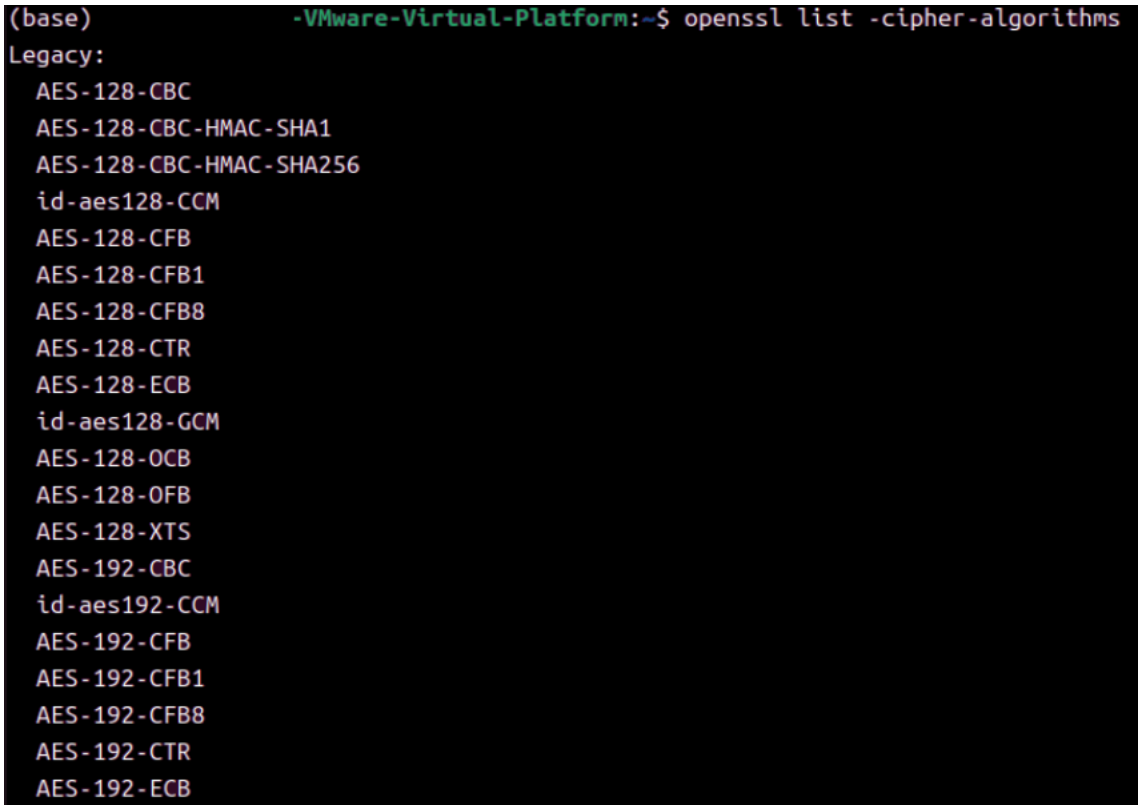


Figure 3-388 그림 제목

7.23.3 판정근거

Table 3-517 TE10.20.01 시험결과 판정근거

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

7.23.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.24 TE10.24.01

7.24.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.24.01	핵심기능 자가시험 명세	개발문서 검토

7.24.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-518 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

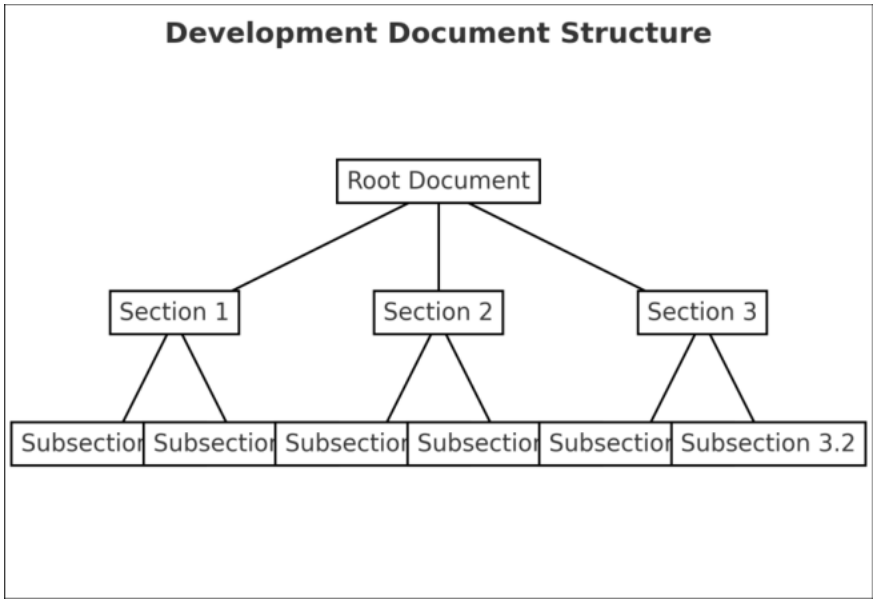


Figure 3-389 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

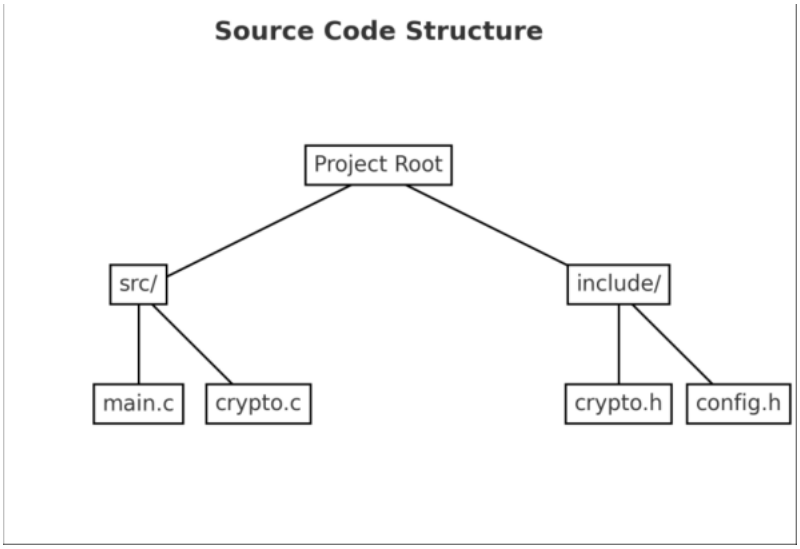
☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-519 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			



3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-520 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

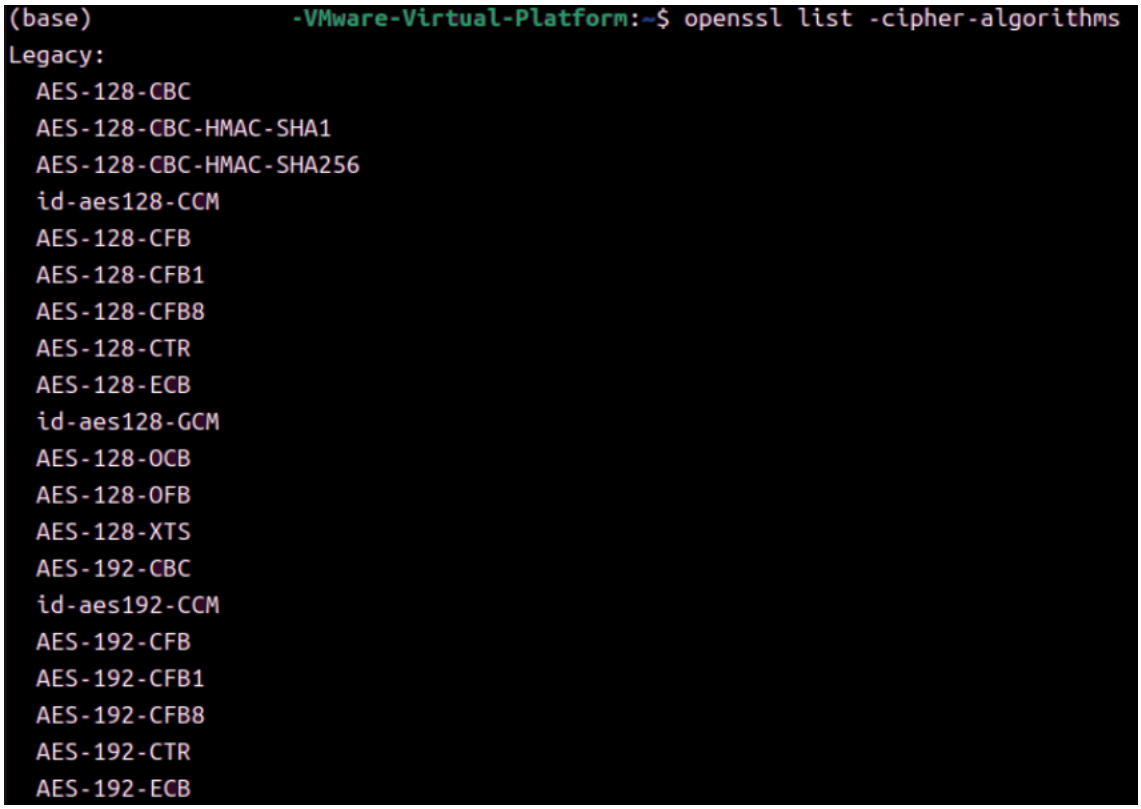


Figure 3-390 그림 제목

7.24.3 판정근거

Table 3-521 TE10.24.01 시험결과 판정근거

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

7.24.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.25 TE10.24.02

7.25.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.24.02	핵심기능 자가시험 수행	암호모듈 검사

7.25.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-522 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

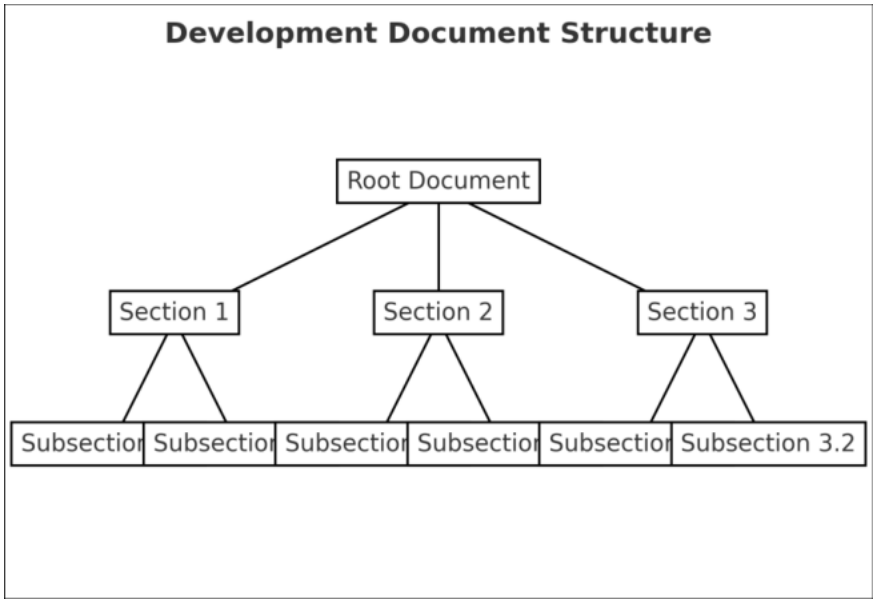


Figure 3-391 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-523 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

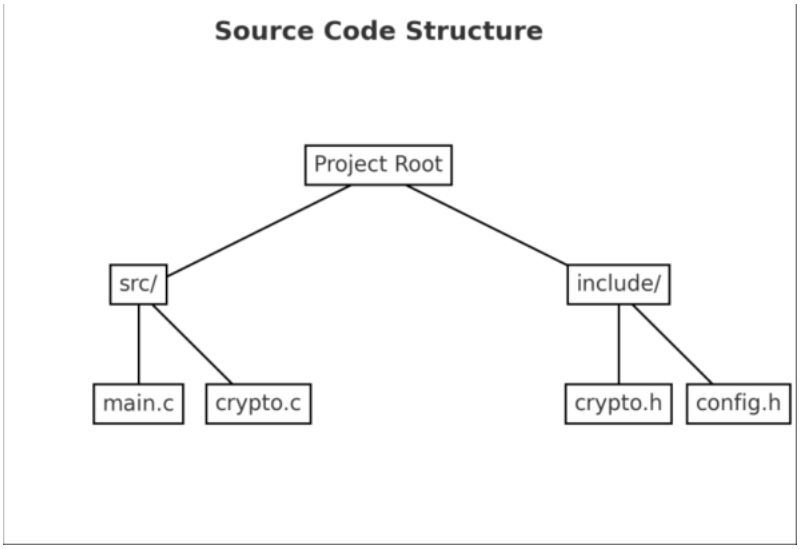


Figure 3-392 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-524 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

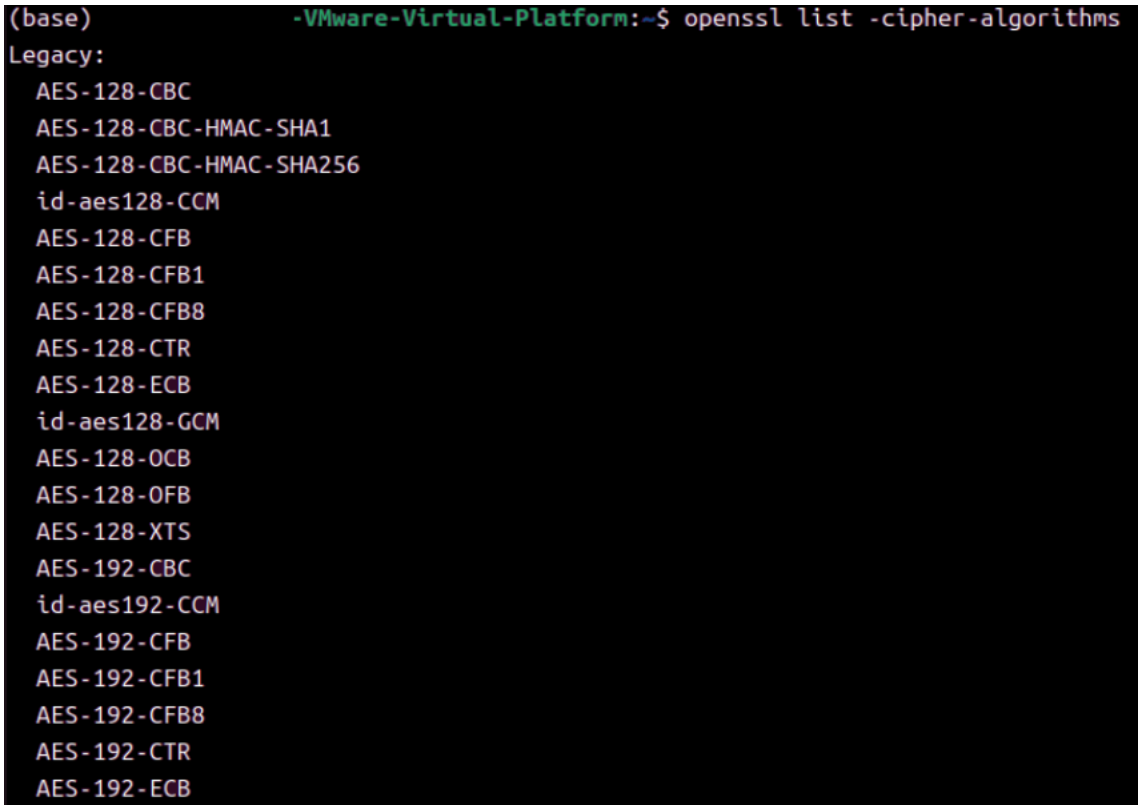


Figure 3-393 그림 제목

7.25.3 판정근거

Table 3-525 TE10.24.02 시험결과 판정근거

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

7.25.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.26 TE10.25.01

7.26.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.25.01	조건부 자사시험 명세	개발문서 검토

7.26.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-526 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

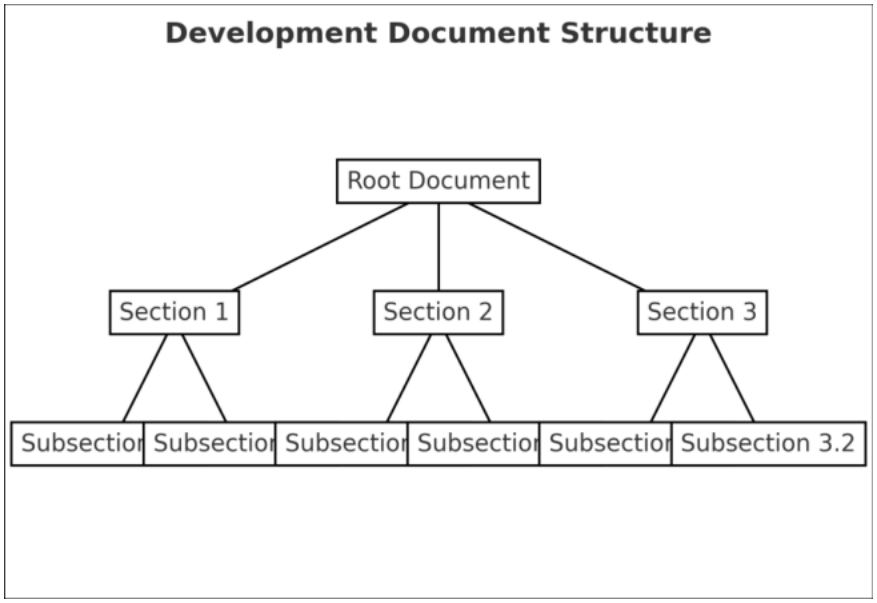


Figure 3-394 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-527 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

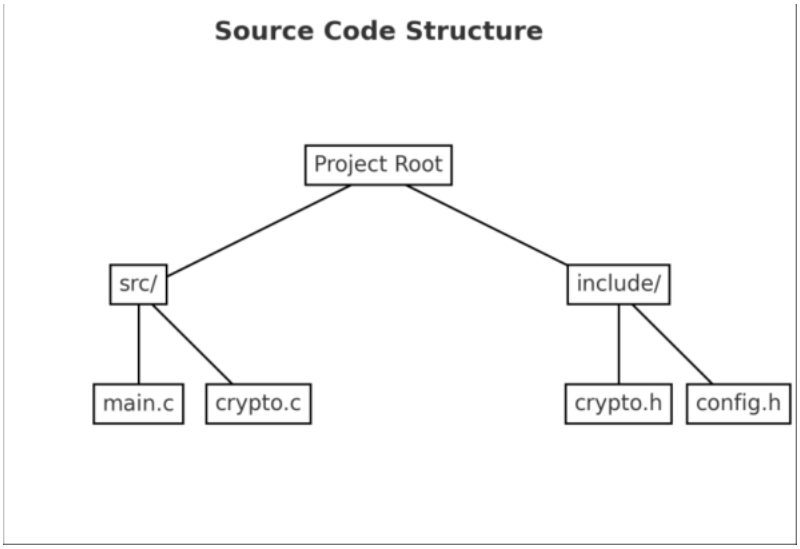


Figure 3-395 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-528 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

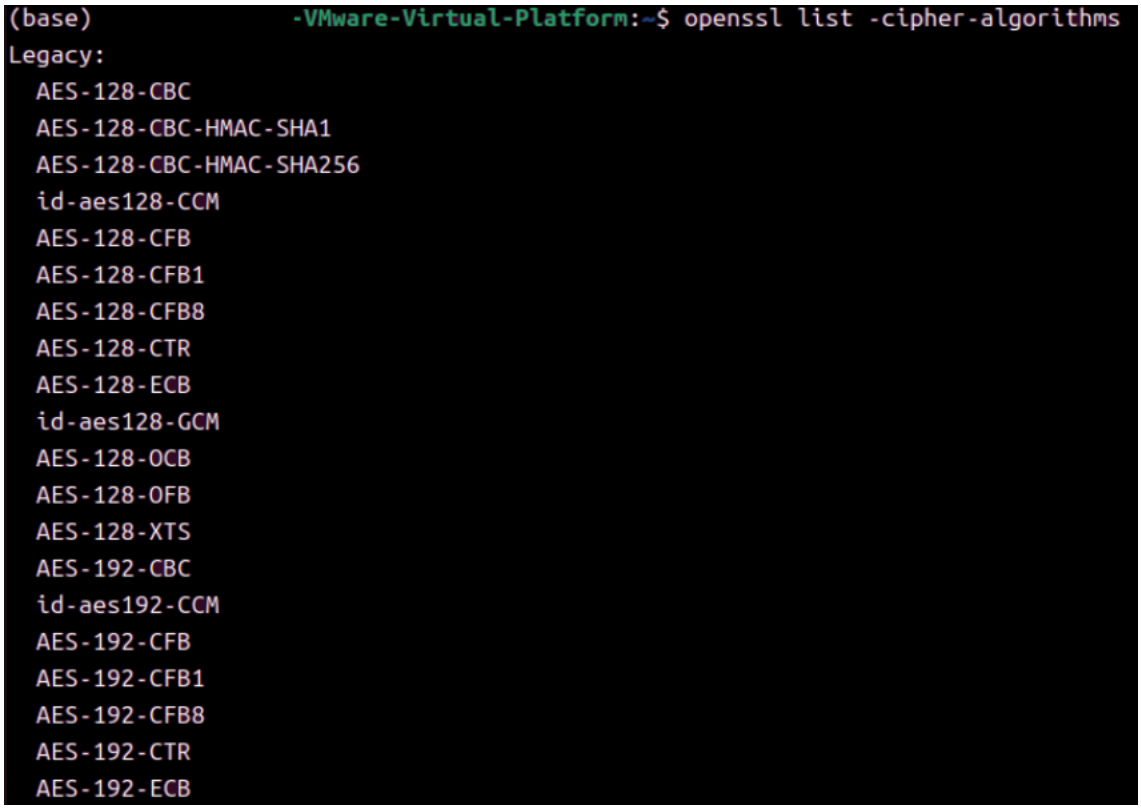


Figure 3-396 그림 제목

7.26.3 판정근거

Table 3-529 TE10.25.01 시험결과 판정근거

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

7.26.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.27 TE10.25.02

7.27.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.25.02	조건부 자가시험 수행	암호모듈 검사

7.27.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-530 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

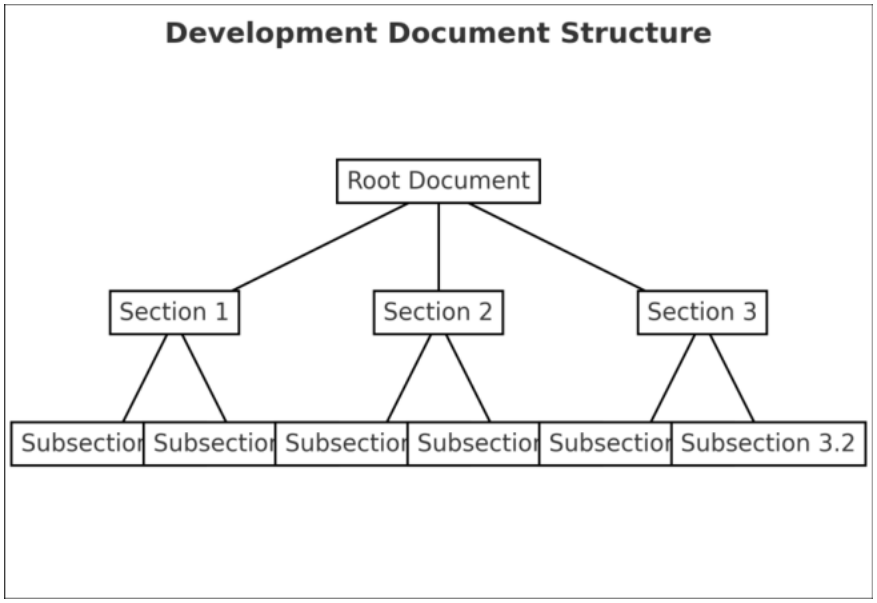


Figure 3-397 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-531 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

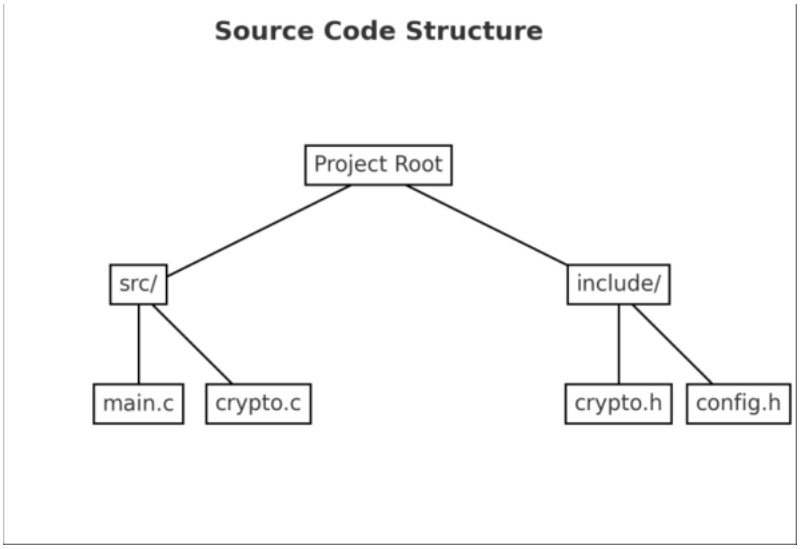


Figure 3-398 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-532 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

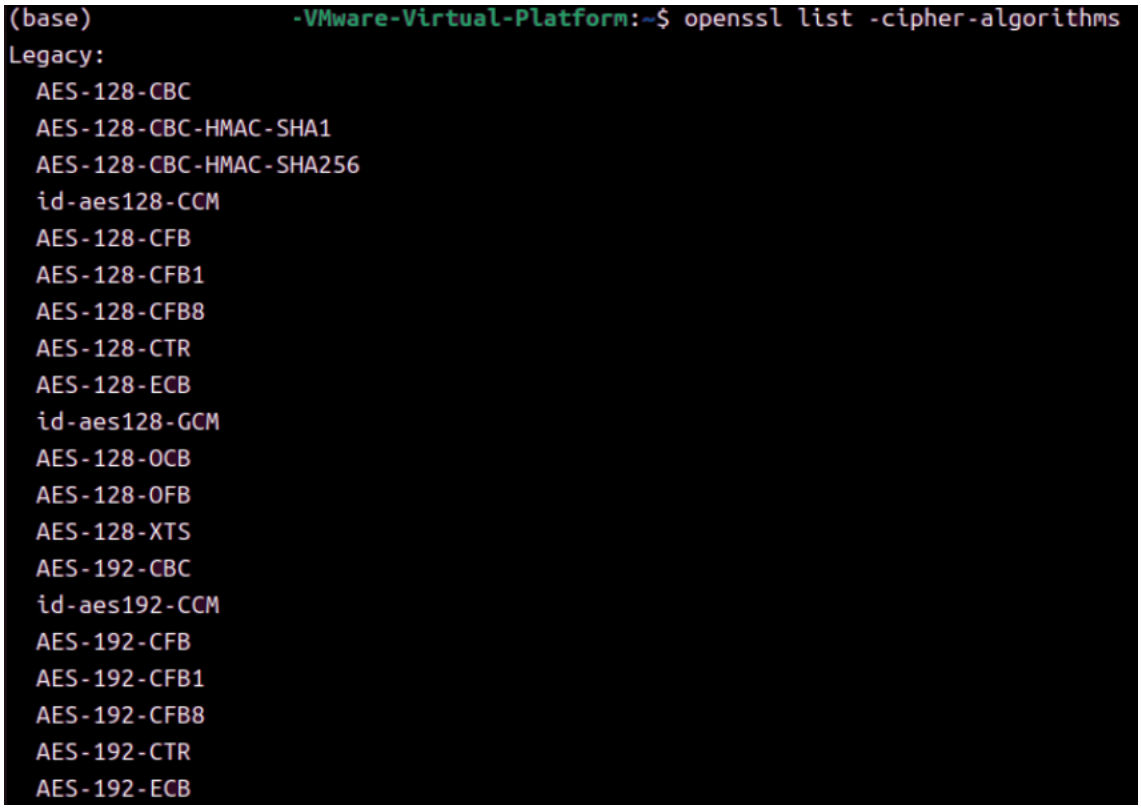


Figure 3-399 그림 제목

7.27.3 판정근거

Table 3-533 TE10.25.02 시험결과 판정근거

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

7.27.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.28 TE10.27.01

7.28.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.27.01	암호알고리즘 최초 사용 전 조건부 자가시험 수행	암호모듈 검사

7.28.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-534 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

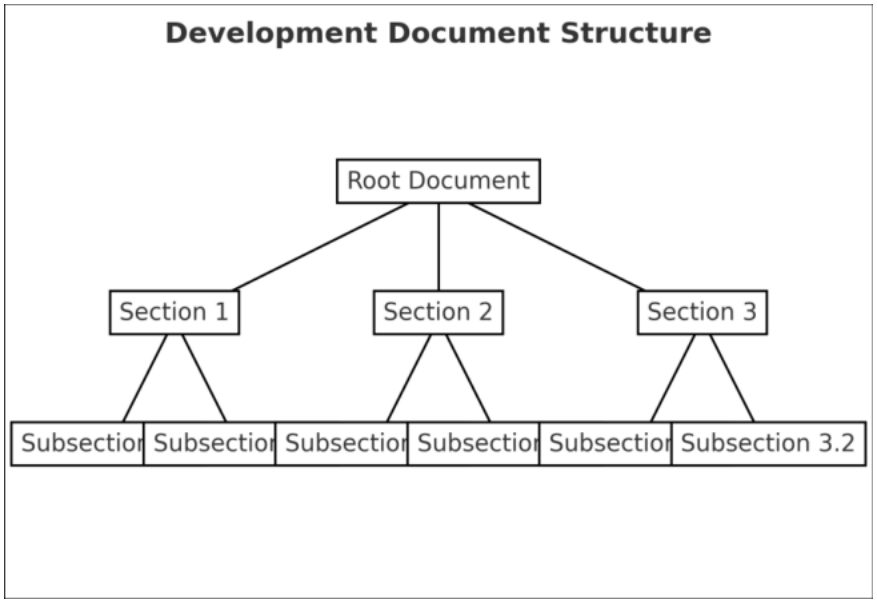


Figure 3-400 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-535 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

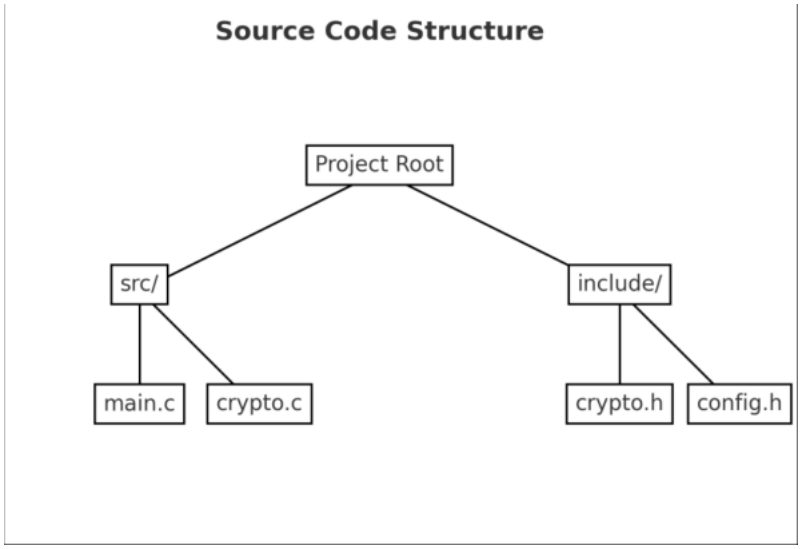


Figure 3-401 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-536 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

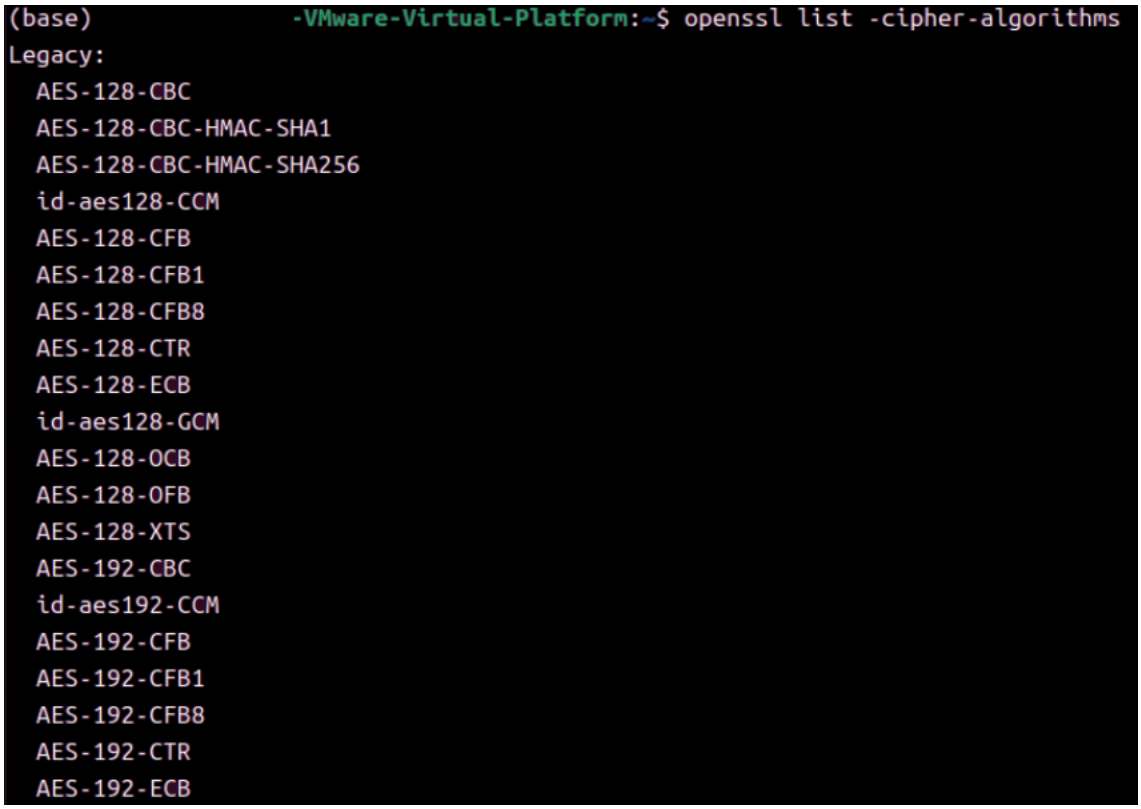


Figure 3-402 그림 제목

7.28.3 판정근거

Table 3-537 TE10.27.01 시험결과 판정근거

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

7.28.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.29 TE10.28.01

7.29.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.28.01	암호알고리즘 기지 답안 시험 수행록	암호모듈 검사

7.29.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-538 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

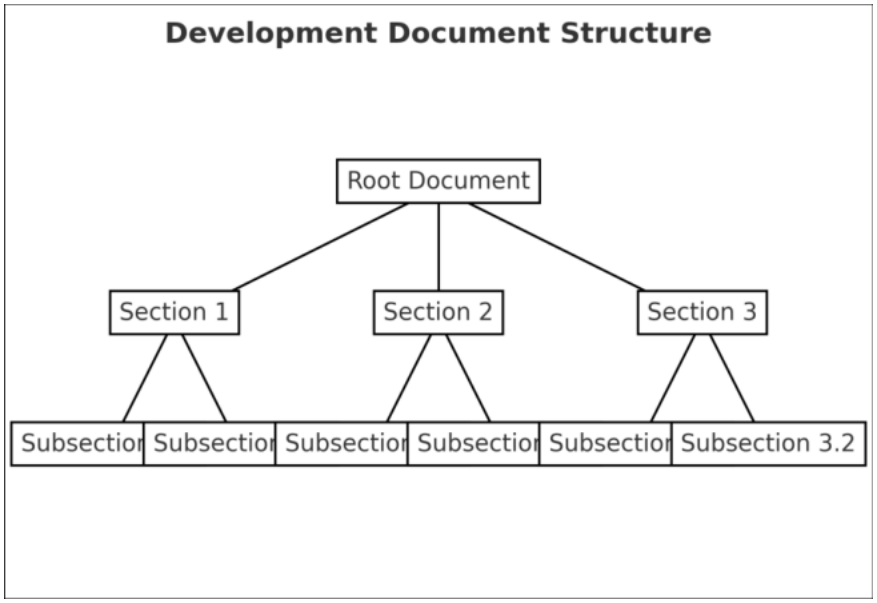


Figure 3-403 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-539 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

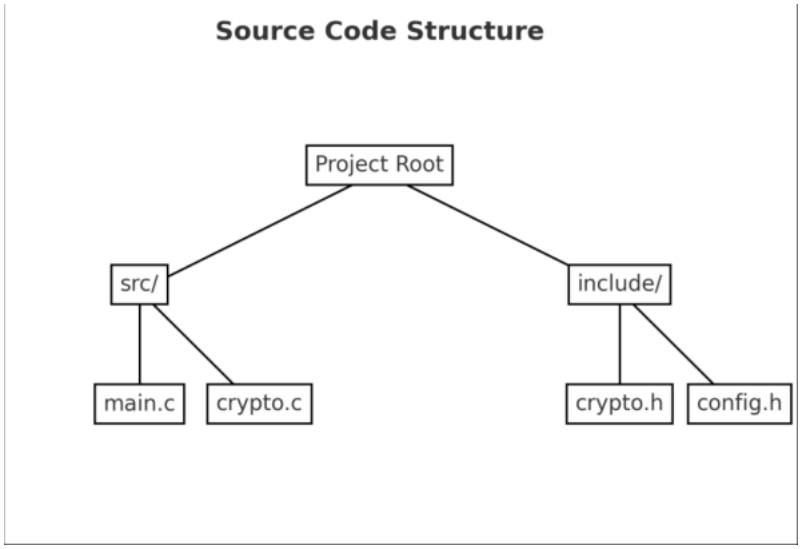


Figure 3-404 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-540 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

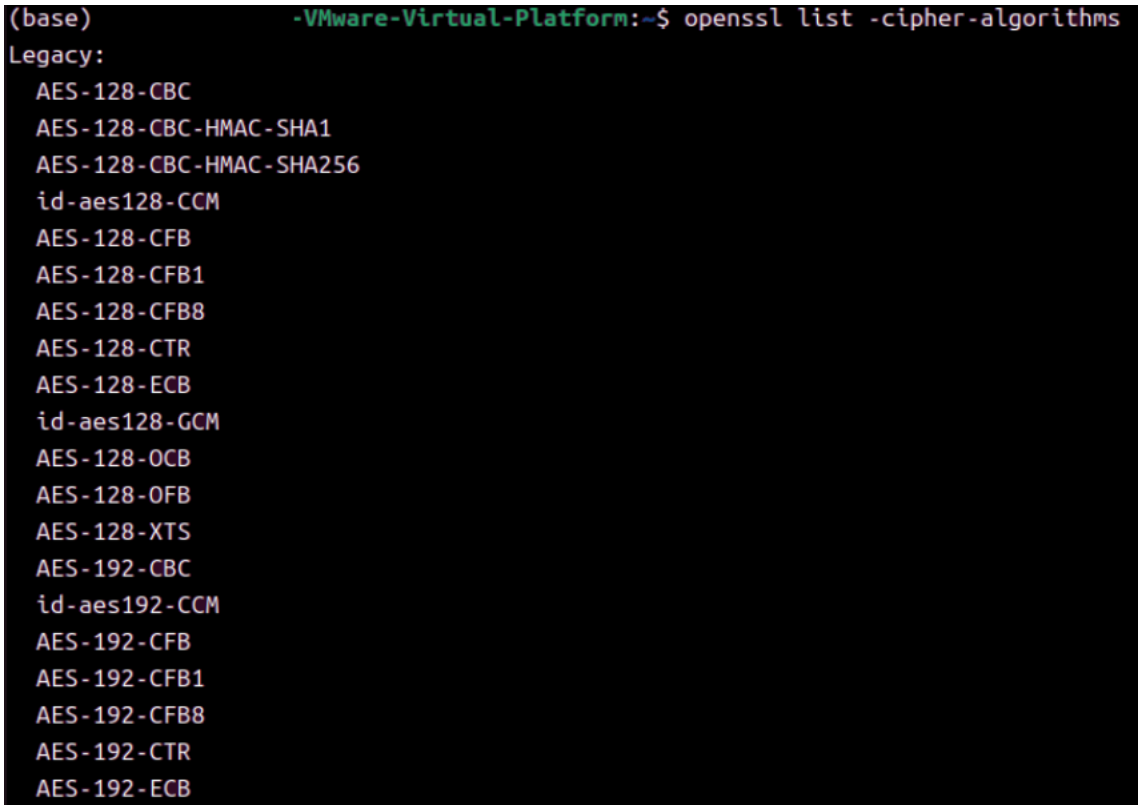


Figure 3-405 그림 제목

7.29.3 판정근거

Table 3-541 TE10.28.01 시험결과 판정근거

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

7.29.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.30 TE10.29.01

7.30.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.29.01	키길이 , 모듈 크기 등은 가장 작은 파라미터 자가시험 수행 , 운영모드 중 최소 한 개 이상 자가시험 수행	암호모듈 검사

7.30.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-542 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

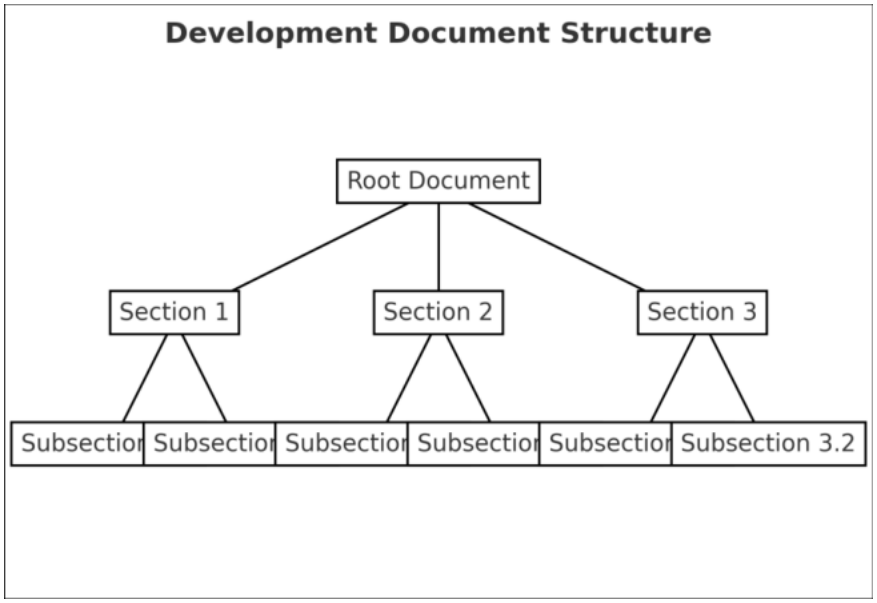


Figure 3-406 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-543 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

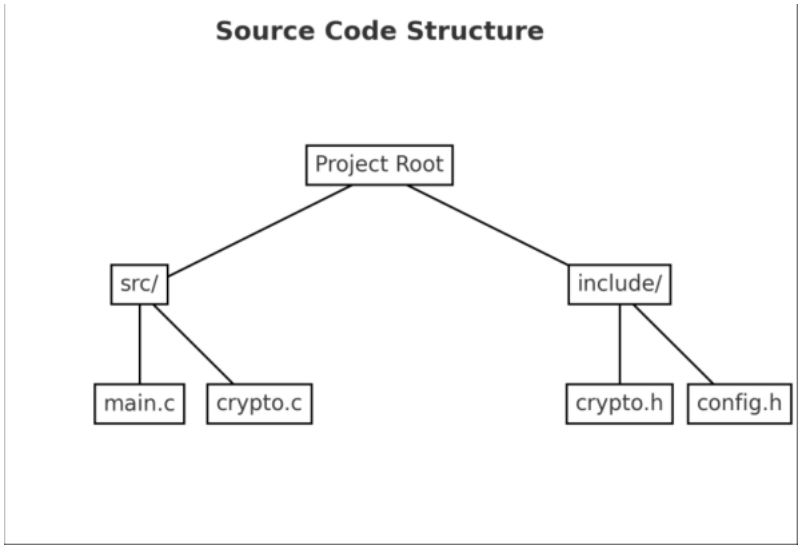


Figure 3-407 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-544 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

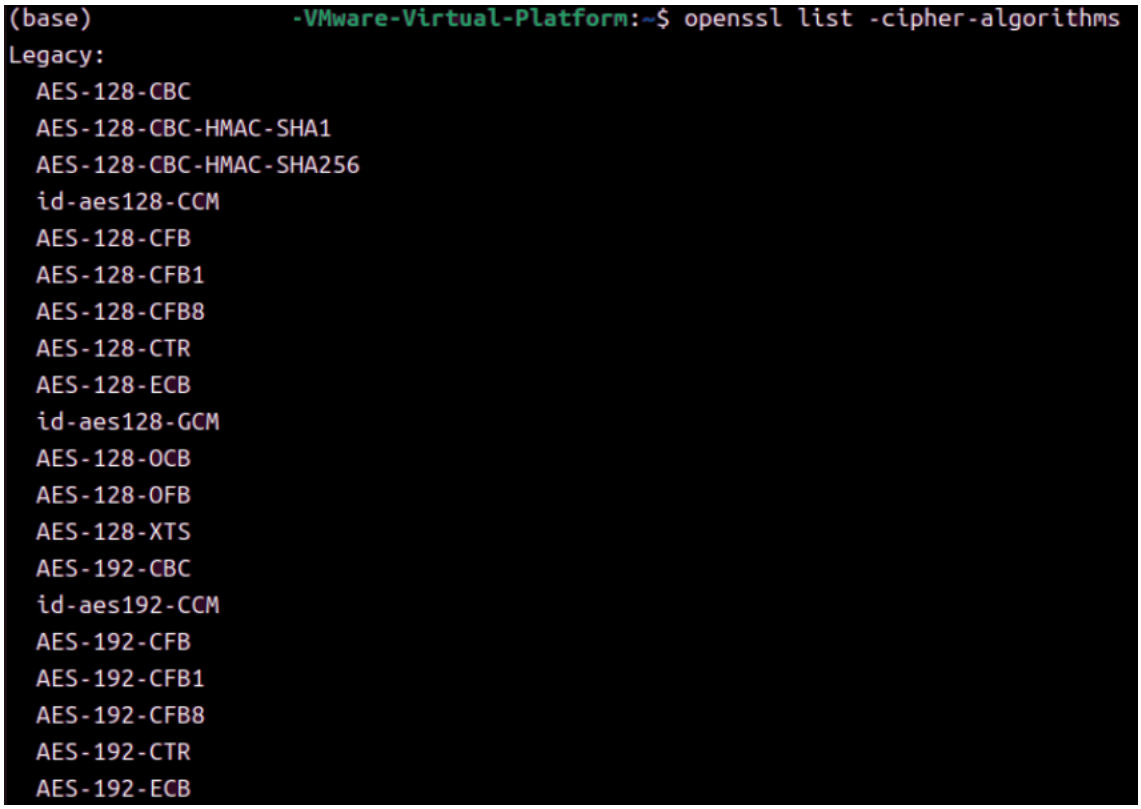


Figure 3-408 그림 제목

7.30.3 판정근거

Table 3-545 TE10.29.01 시험결과 판정근거

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

7.30.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.31 TE10.33.01

7.31.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.33.01	비교 시험 명세 포함록	개발문서 검토

7.31.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-546 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

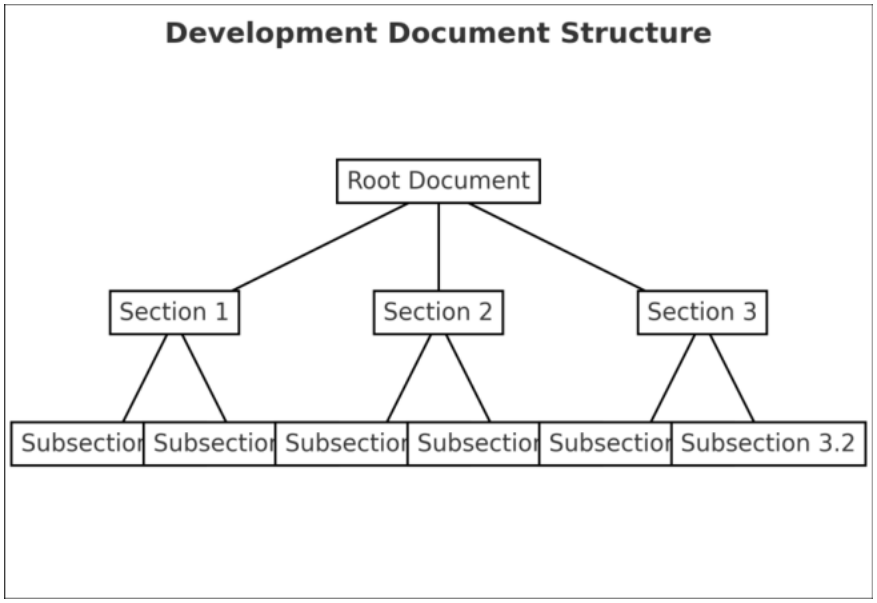


Figure 3-409 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-547 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

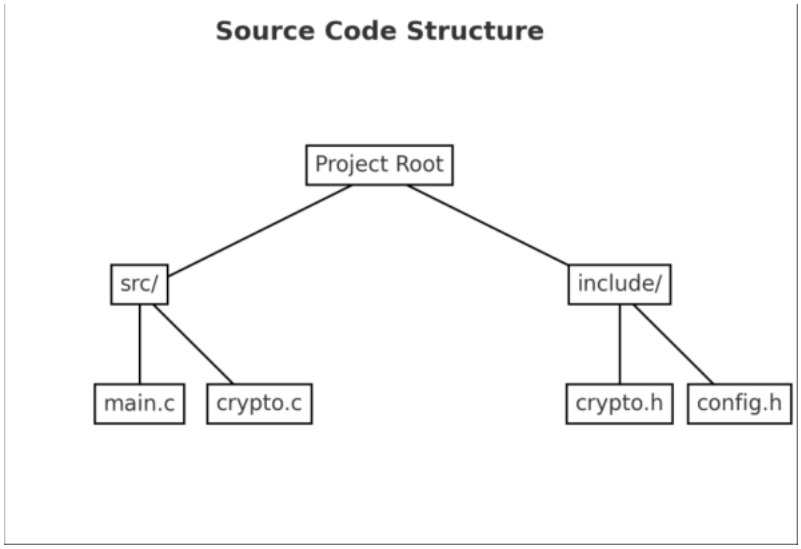


Figure 3-410 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-548 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

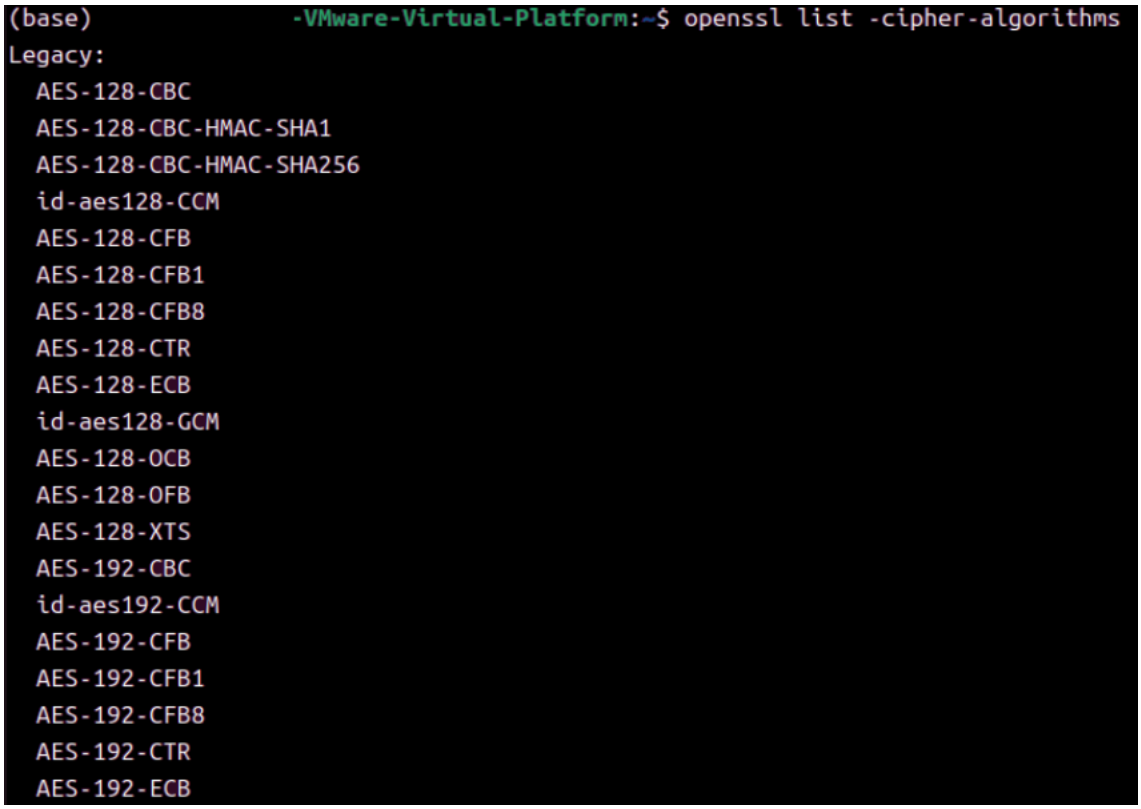


Figure 3-411 그림 제목

7.31.3 판정근거

Table 3-549 TE10.33.01 시험결과 판정근거

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

7.31.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.32 TE10.33.02

7.32.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.33.02	명세된 비교 시험 수행	암호모듈 검사

7.32.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-550 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

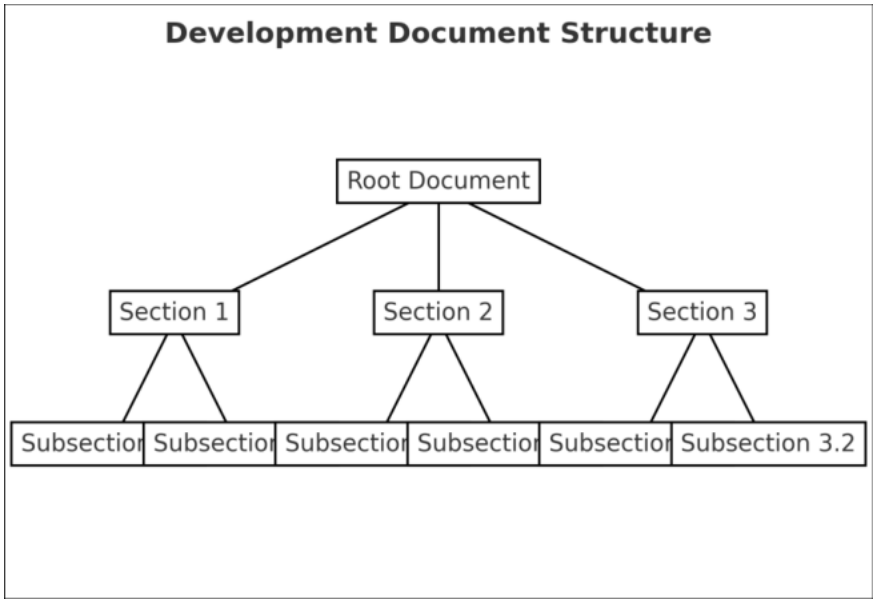


Figure 3-412 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-551 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

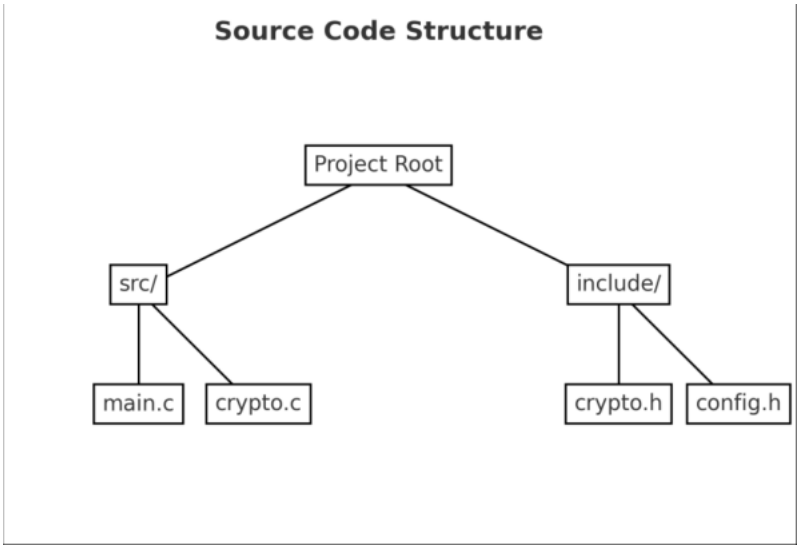


Figure 3-413 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-552 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

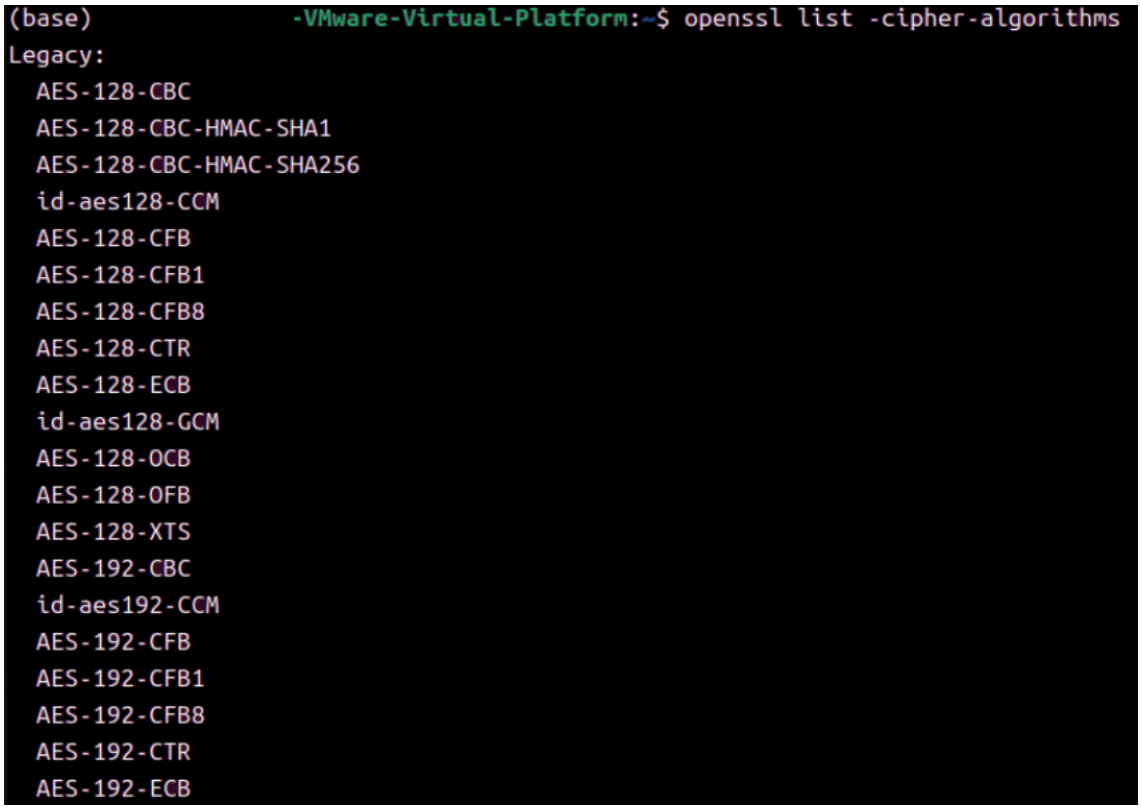


Figure 3-414 그림 제목

7.32.3 판정근거

Table 3-553 TE10.07.01 시험결과 판정근거

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

7.32.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.33 TE10.34.01

7.33.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.34.01	기지답안 및 비교 시험 보완을 위한 오류 탐지 시험 명세	개발문서 검토

7.33.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-554 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

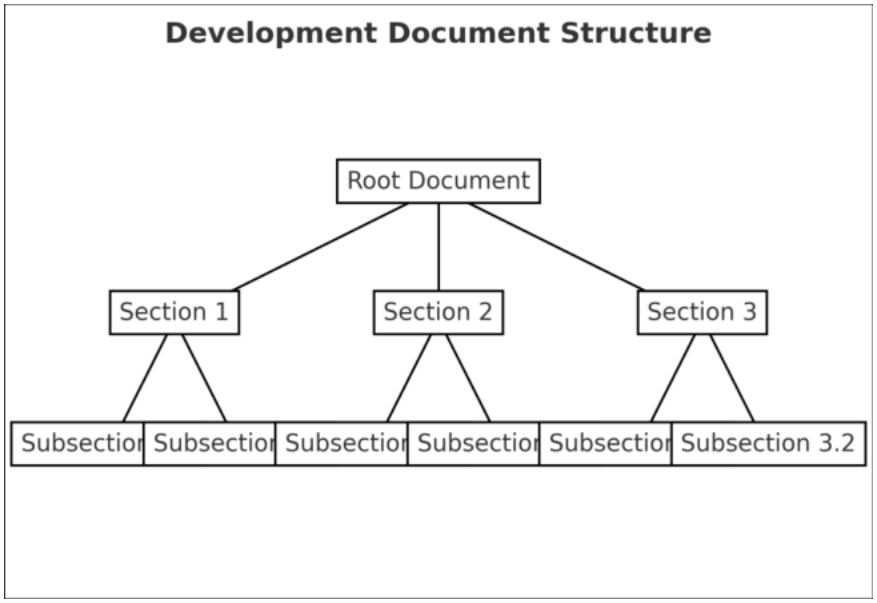


Figure 3-415 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-555 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

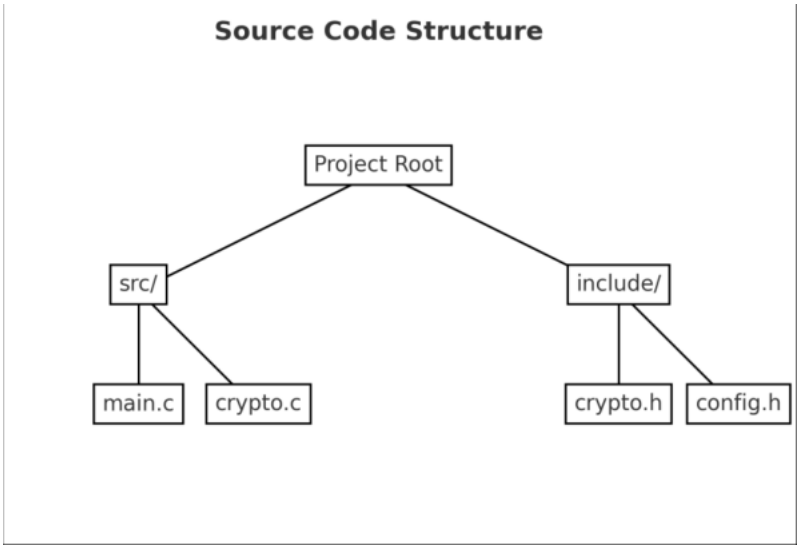


Figure 3-416 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-556 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

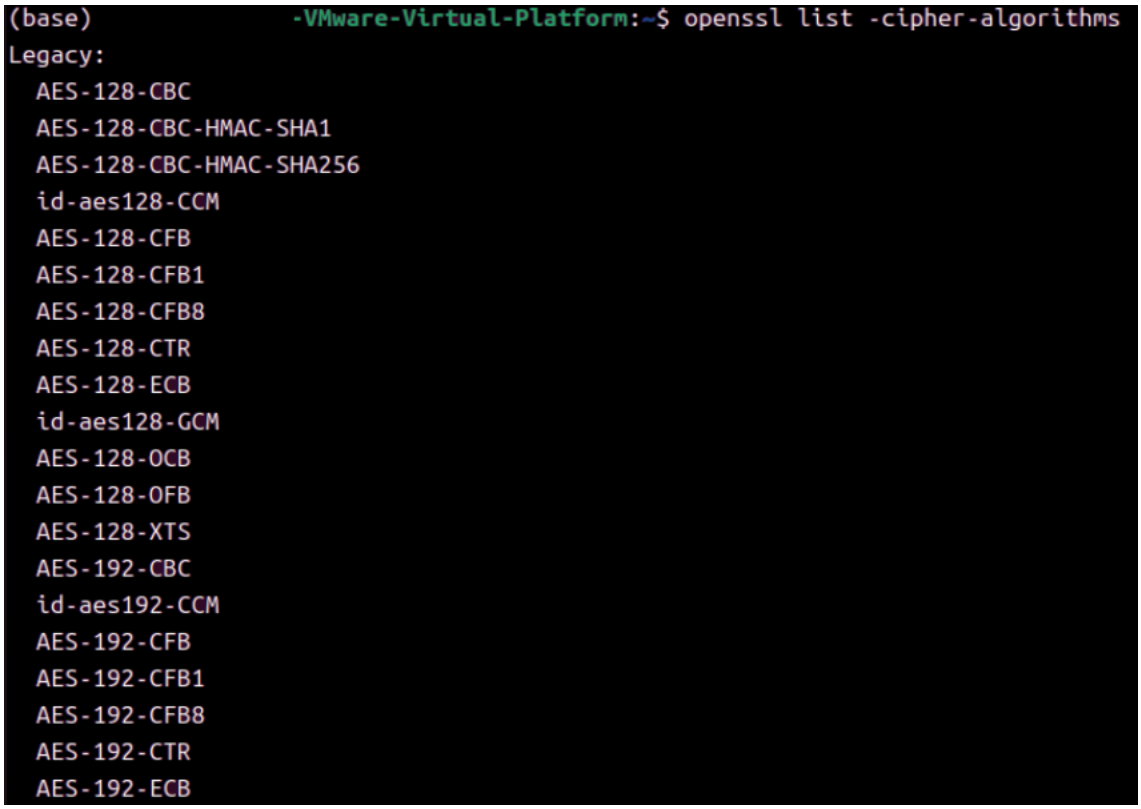


Figure 3-417 그림 제목

7.33.3 판정근거

Table 3-557 TE10.34.01 시험결과 판정근거

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

7.33.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.34 TE10.34.02

7.34.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.34.02	명세된 오류 탐지 시험 수행	암호모듈 검사

7.34.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-558 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

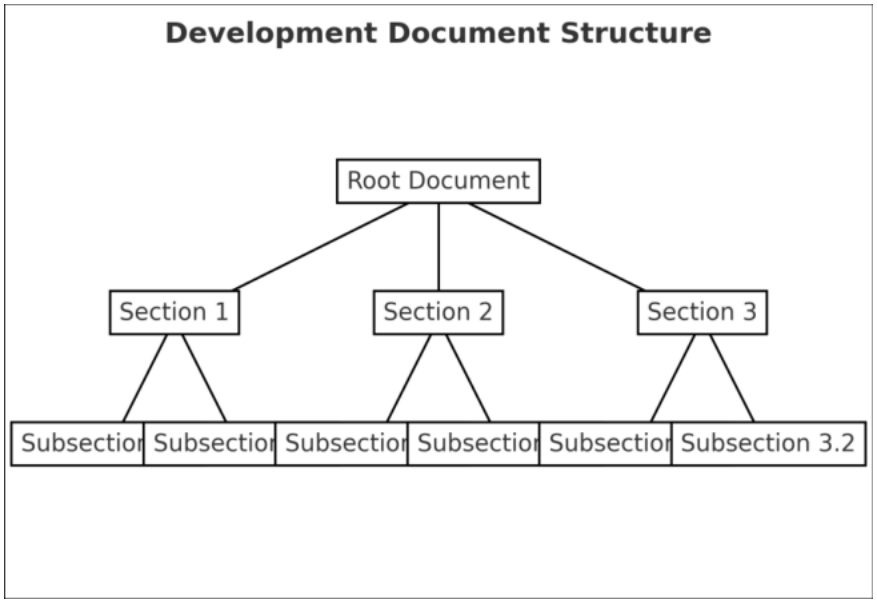


Figure 3-418 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-559 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

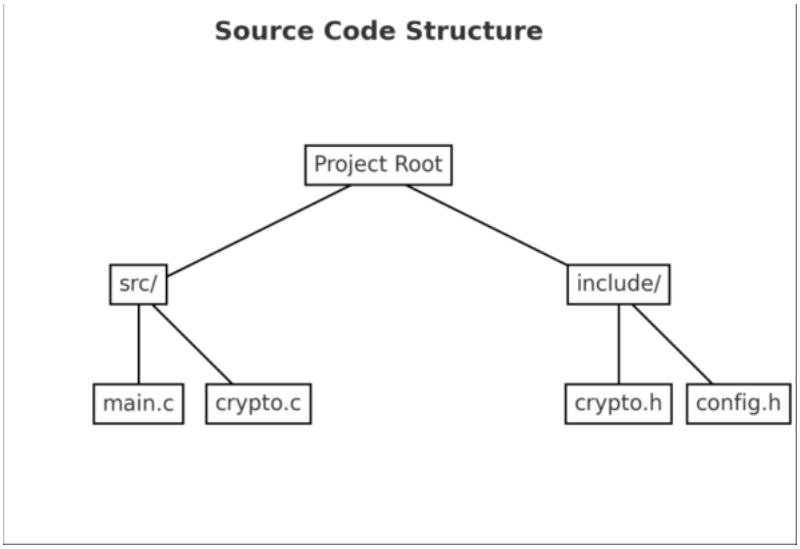


Figure 3-419 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-560 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

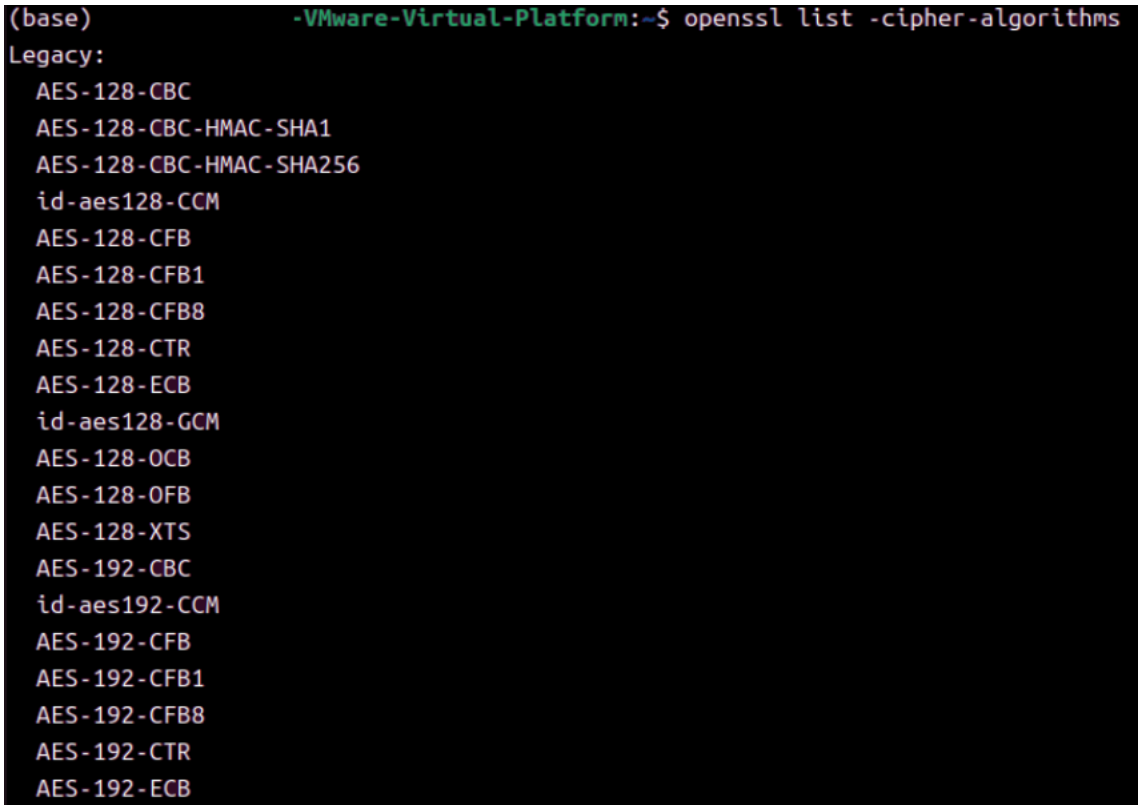


Figure 3-420 그림 제목

7.34.3 판정근거

Table 3-561 TE10.34.02 시험결과 판정근거

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

7.34.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.35 TE10.53.01

7.35.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.53.01	요청에 의한 동작 전 자기시험 명세	개발문서 검토

7.35.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-562 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

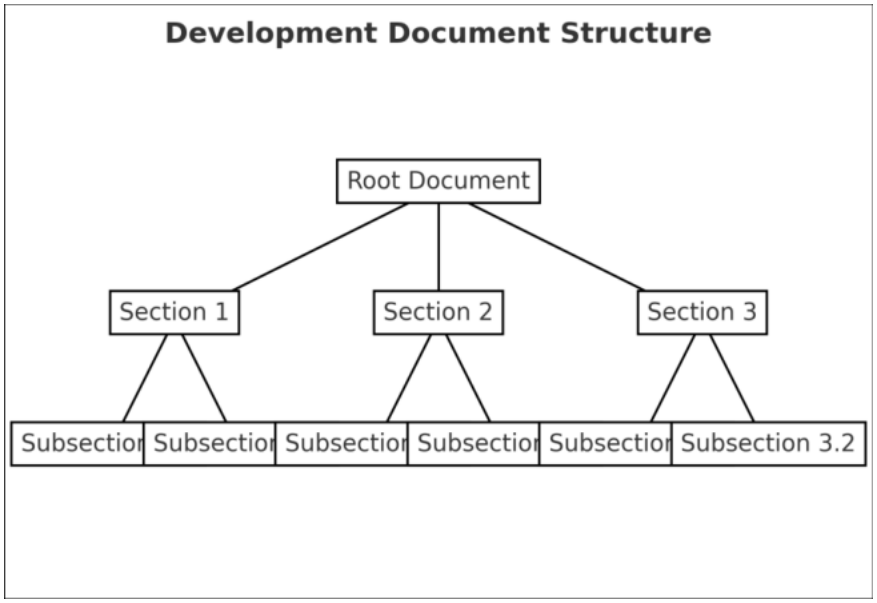


Figure 3-421 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-563 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

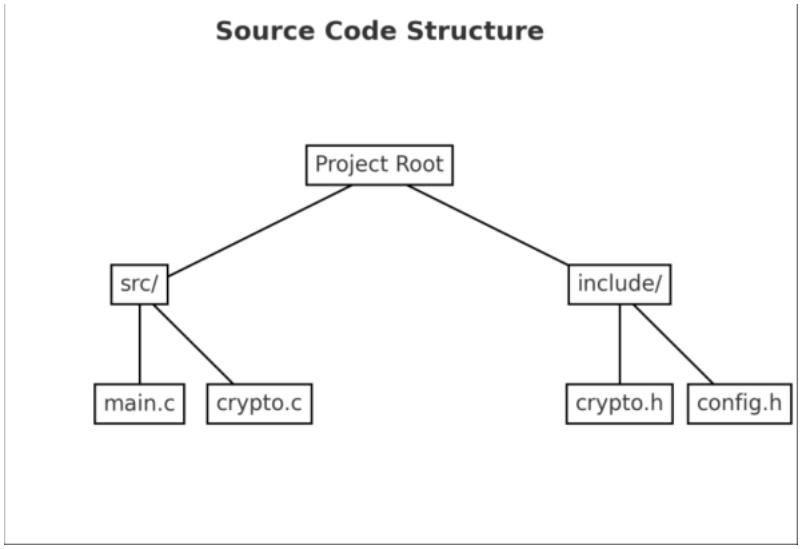


Figure 3-422 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-564 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

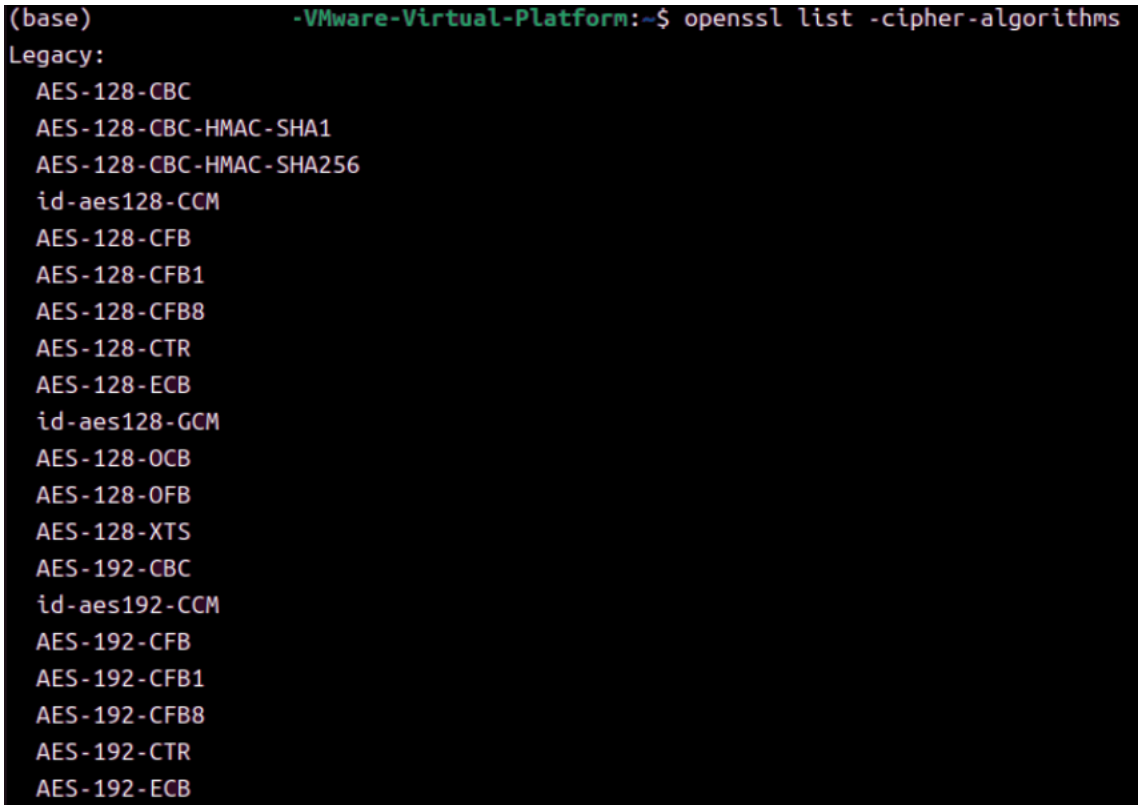


Figure 3-423 그림 제목

7.35.3 판정근거

Table 3-565 TE10.53.01 시험결과 판정근거

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

7.35.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.36 TE10.53.02

7.36.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.53.02	요청에 의한 동작 전 자가시험 명세와 구현 일치	소스코드 검토

7.36.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-566 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

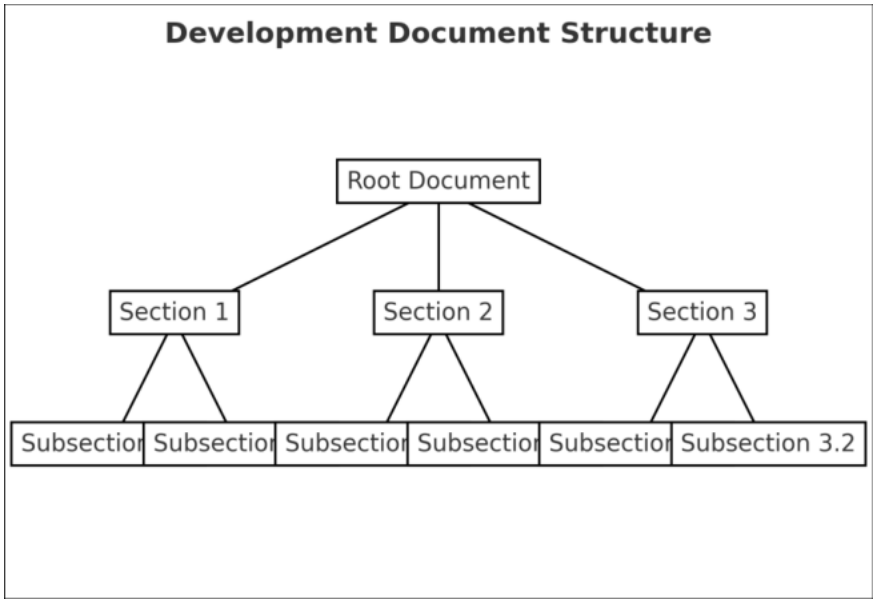


Figure 3-424 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-567 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

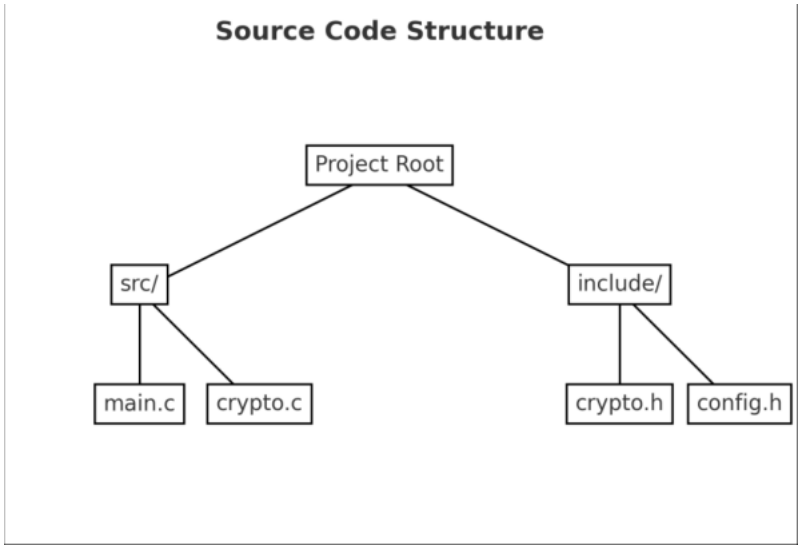


Figure 3-425 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-568 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

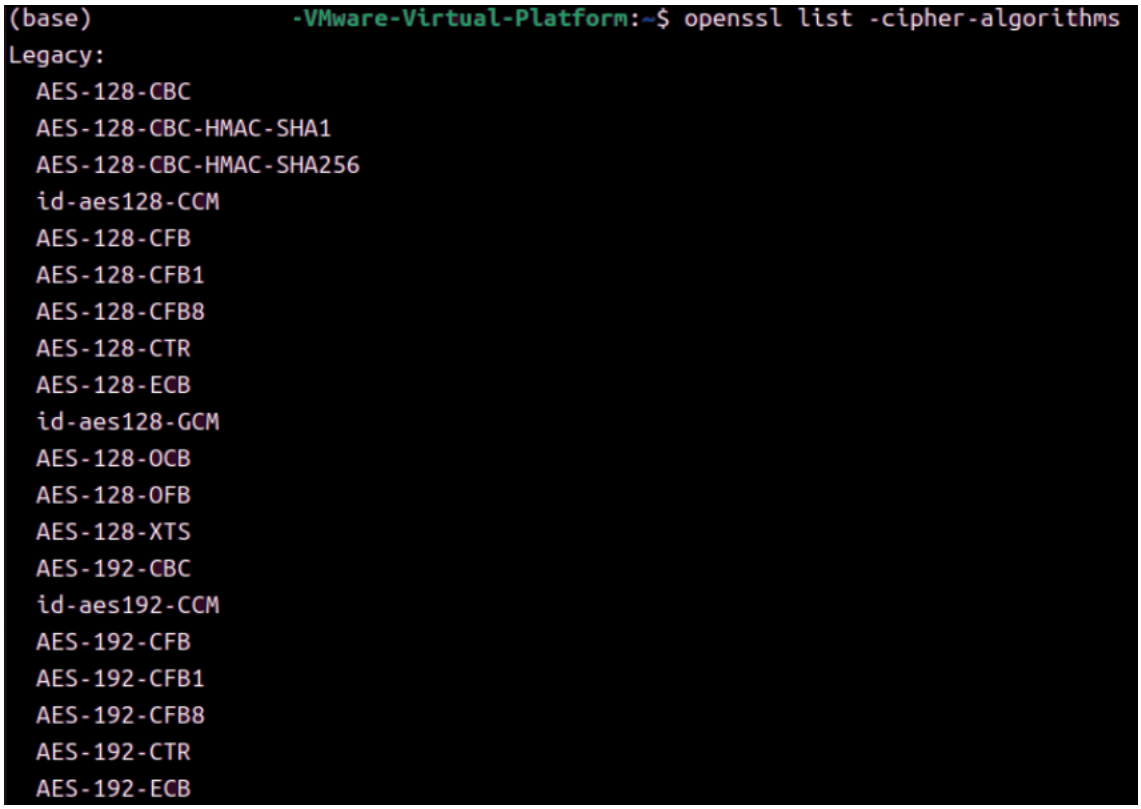


Figure 3-426 그림 제목

7.36.3 판정근거

Table 3-569 TE10.53.02 시험결과 판정근거

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

7.36.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

7.37 TE10.53.03

7.37.1 시험 요구사항

TE	주요 확인사항	확인방법
TE10.53.03	요청에 의한 조건부 자가시험 명세와 구현 일치	소스코드 검토

7.37.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-570 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

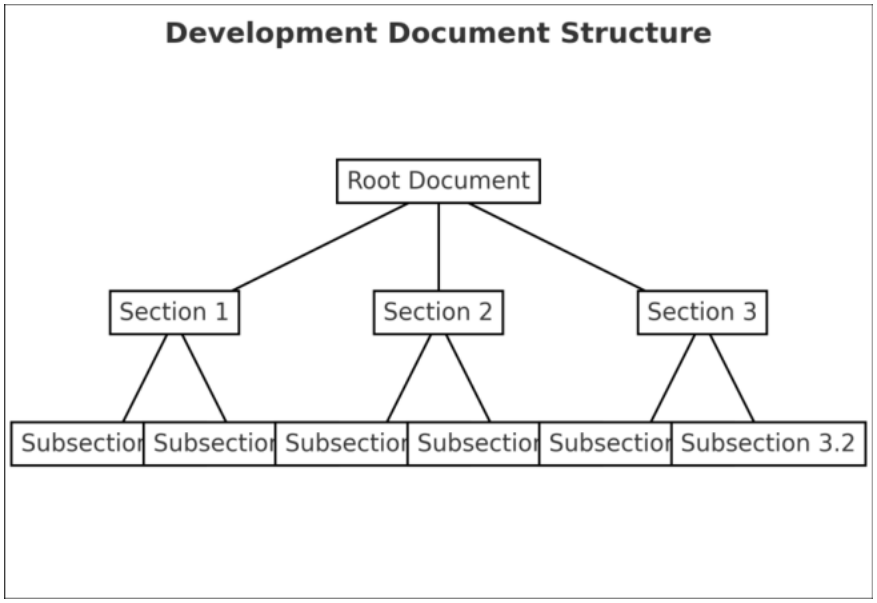


Figure 3-427 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-571 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

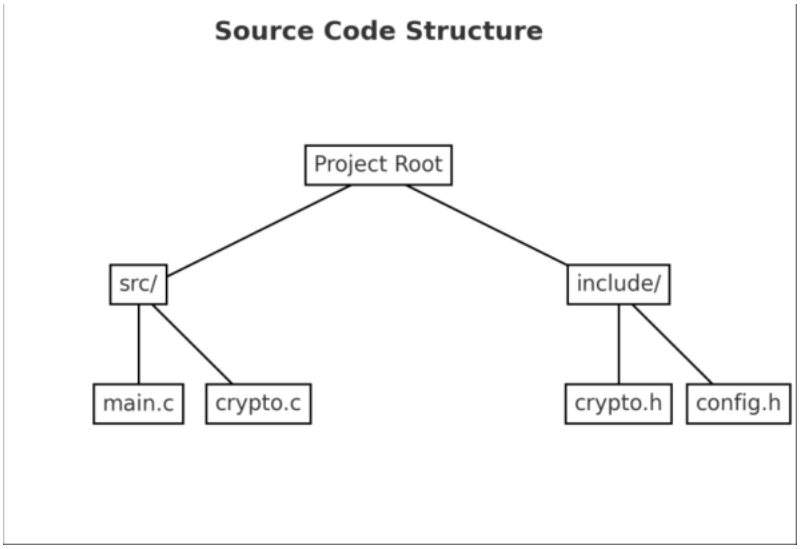


Figure 3-428 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-572 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

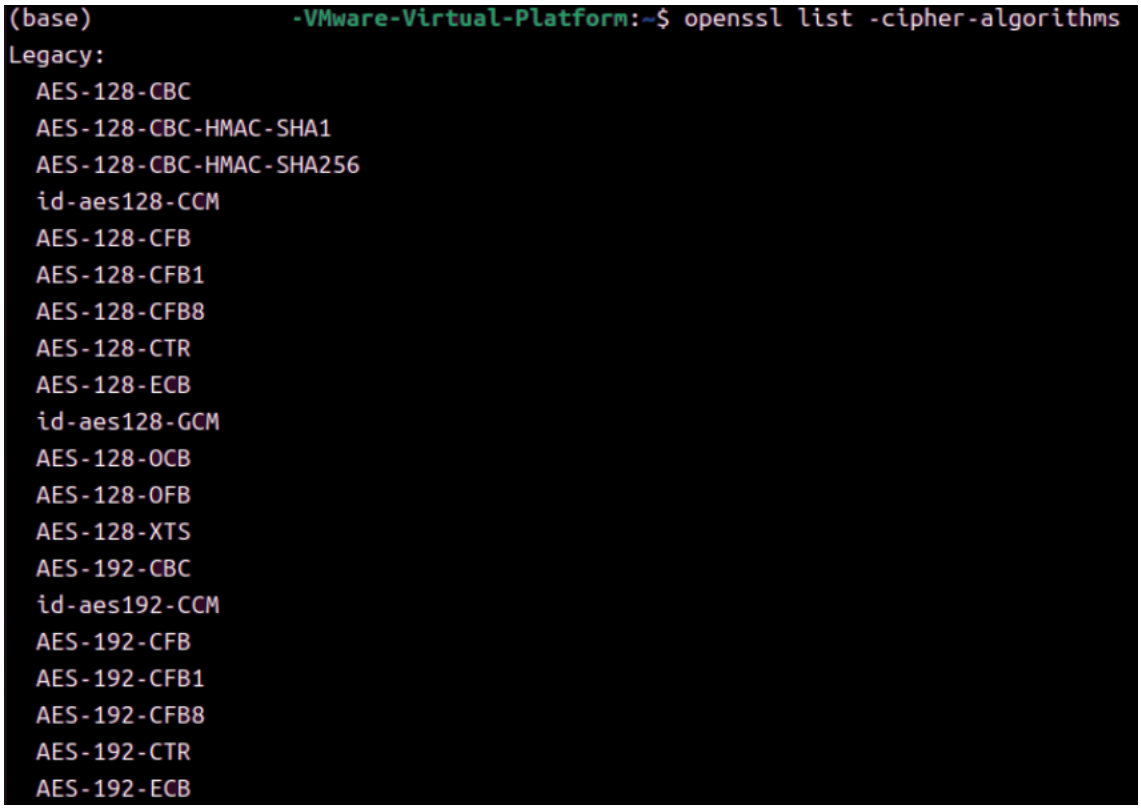


Figure 3-429 그림 제목

7.37.3 판정근거

Table 3-573 TE10.53.03 시험결과 판정근거

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

7.37.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8. 생명주기 보증 (AS11)

□ 암호모듈 제출물에 대한 객관성 및 타당성 확보를 위한 근거자료를 생명주기 보증 요구사항에서 다룬다 .

□ 생명주기 보증은 형상관리 , 설계 , 유한상태모델 , 개발 , 벤더시험 , 배포 및 운영 , 수명의 종료 , 그리고 안내서로 구분된다 .

8.1 AS11 시험항목

AS	TE	확인사항
AS11.01	1	개발문서의 최소 문서 요구사항 만족 여부
AS11.03	1	형상관리시스템
AS11.04	1~4	암호모듈 및 제출물에 대한 유일한 식별자 할당
AS11.05	1	승인된 형상 변경 방법 적용
AS11.08	1~12	상태 천이도 , 상태 천이표와 상태 설명
AS11.11	1	단순 오류에 대한 복구 가능
AS11.13	1	암호관리자 상태 변경
AS11.15	1, 2	암호모듈 개발환경 명세 (컴파일러 , 옵션 등)
AS11.16	1	소스코드 주석 처리
AS11.19	1	무결성 결과 코드 탑재
AS11.21	1	개발도구 (컴파일러)
AS11.29	1	벤더시험 (시험서)
AS11.30	1	자동화 보안 진단 도구 사용
AS11.32	1, 2	안전한 설치 , 초기화 및 시동을 위한 절차
AS11.36	1	안전한 파기 절차
AS11.38	1	관리자 안내서
AS11.39	1	비관리자 (사용자) 안내서

8.2 TE11.01.01

8.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.01.01	생명주기 보증 관련 문서	개발문서 검토

8.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-574 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

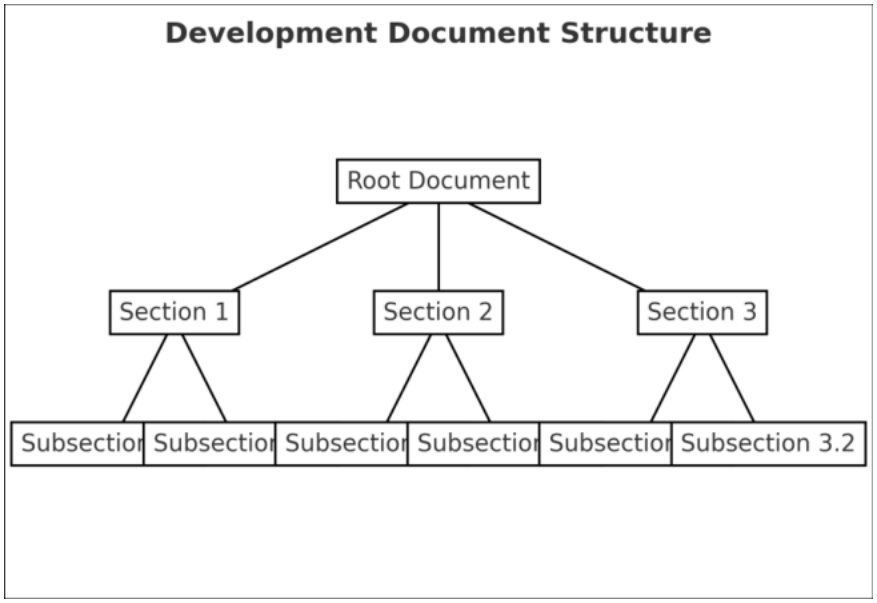


Figure 3-430 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-575 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

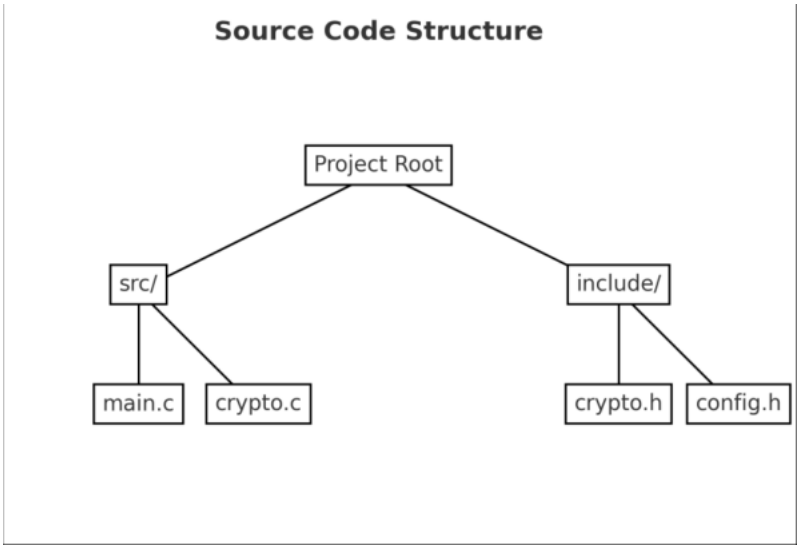


Figure 3-431 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-576 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

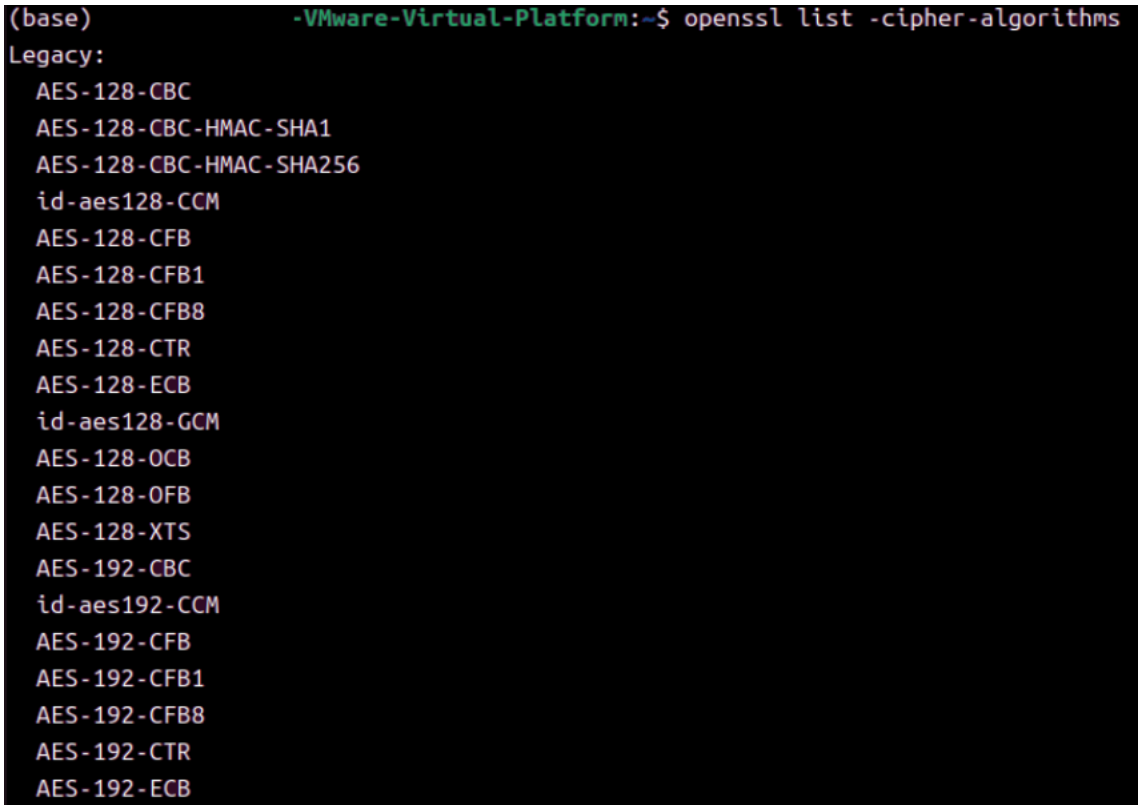


Figure 3-432 그림 제목

8.2.3 판정근거

Table 3-577 TE11.01.01 시험결과 판정근거

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

8.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.3 TE11.03.01

8.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.03.01	형상관리 시스템의 구현 관련 개발문서 검증	개발문서 검토

8.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-578 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

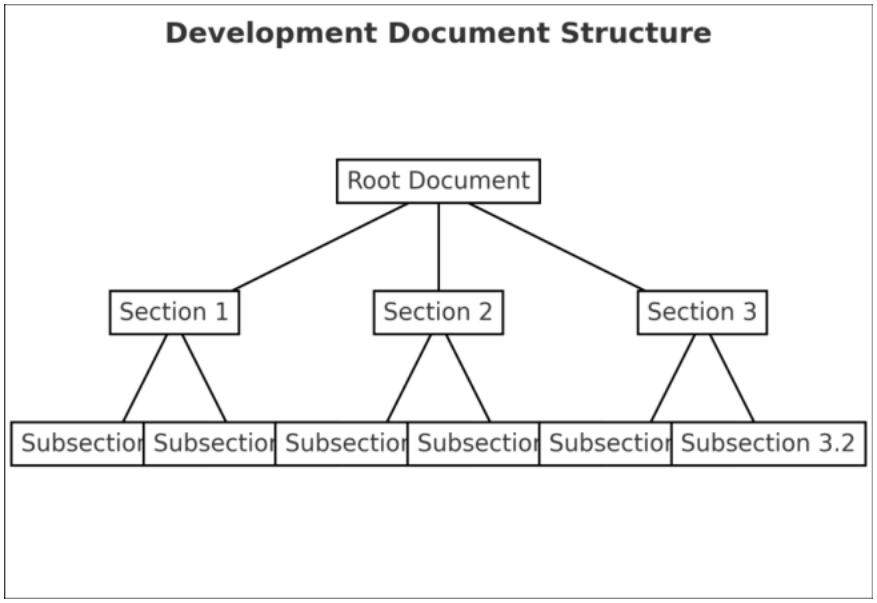


Figure 3-433 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-579 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

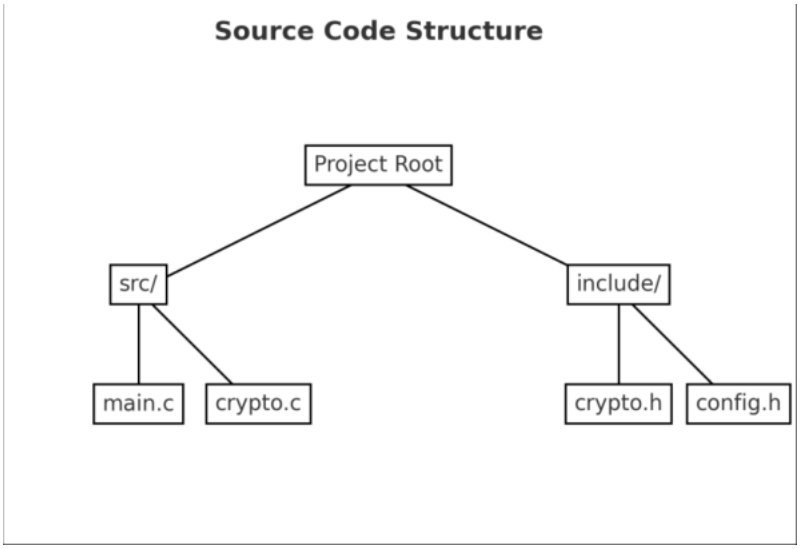


Figure 3-434 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-580 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

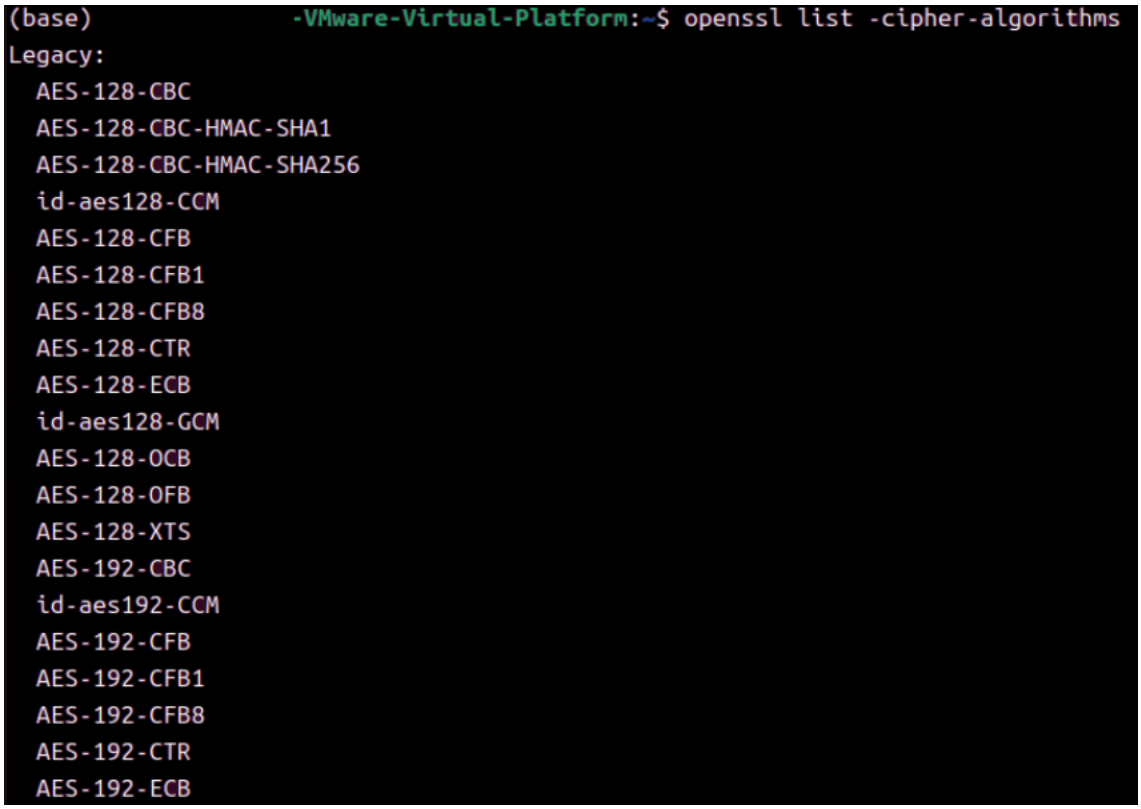


Figure 3-435 그림 제목

8.3.3 판정근거

Table 3-581 TE11.03.01 시험결과 판정근거

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

8.3.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.4 TE11.04.01

8.4.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.04.01	형상 항목을 포함한 형상 목록 제공 여부	개발문서 검토

8.4.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-582 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

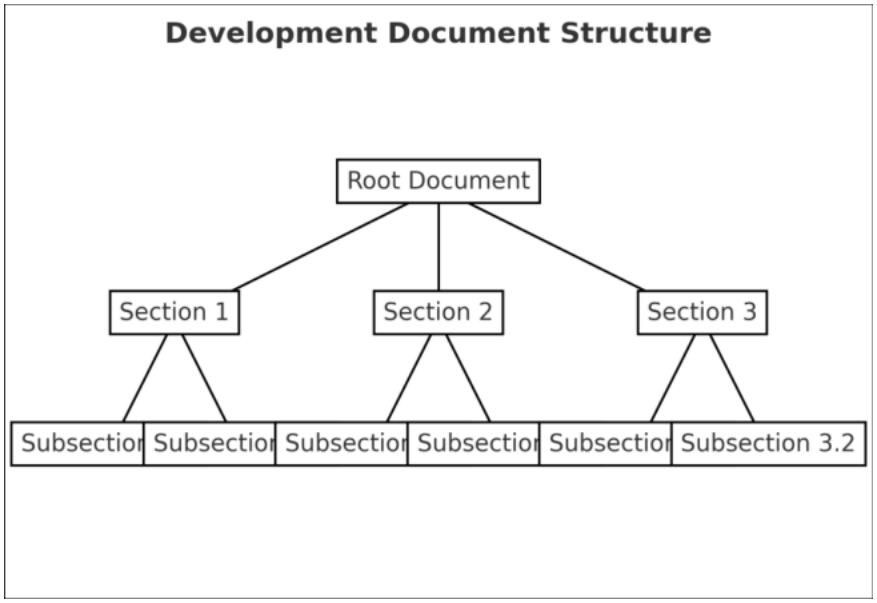


Figure 3-436 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-583 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

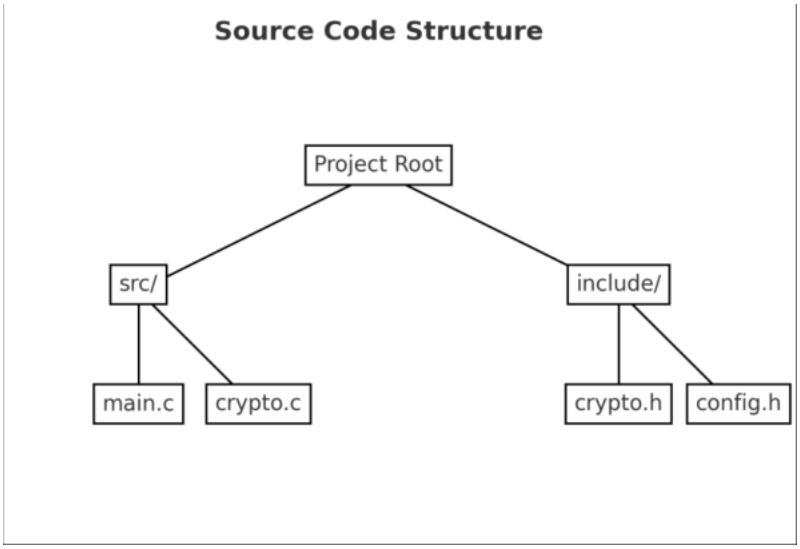


Figure 3-437 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-584 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

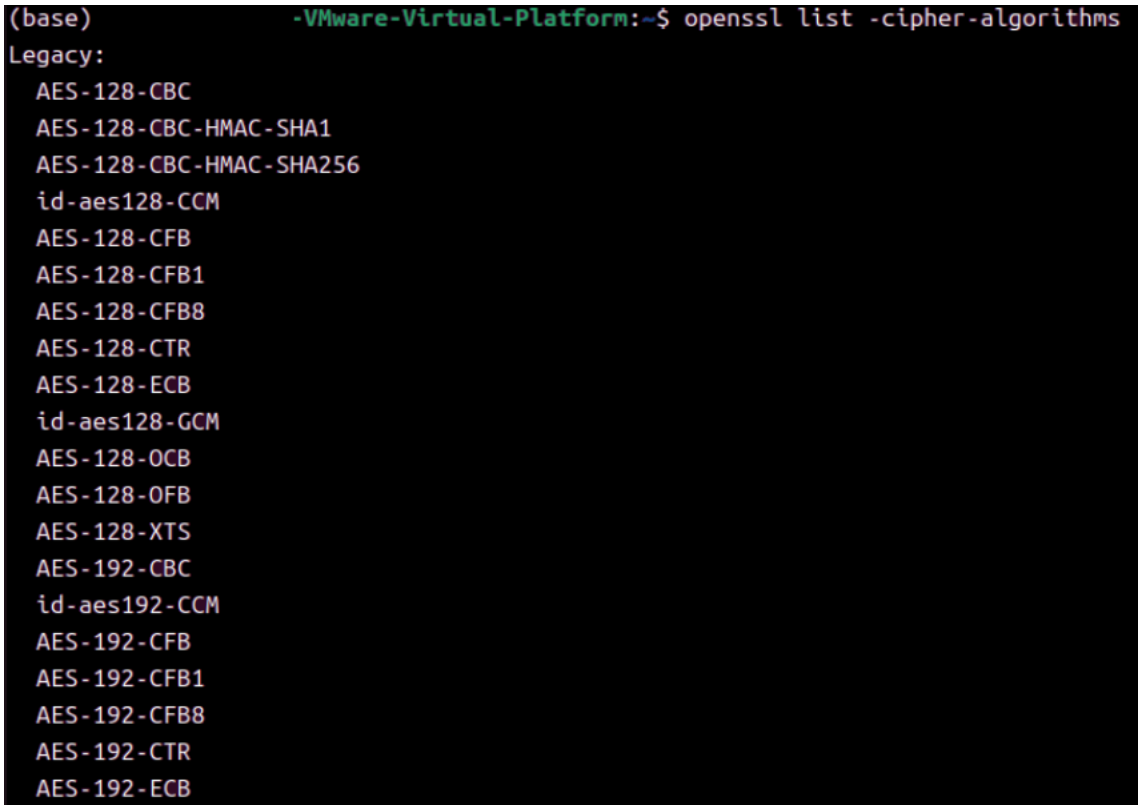


Figure 3-438 그림 제목

8.4.3 판정근거

Table 3-585 TE11.04.01 시험결과 판정근거

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

8.4.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.5 TE11.04.02

8.5.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.04.02	형상 항목 식별 방법	개발문서 검토

8.5.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-586 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

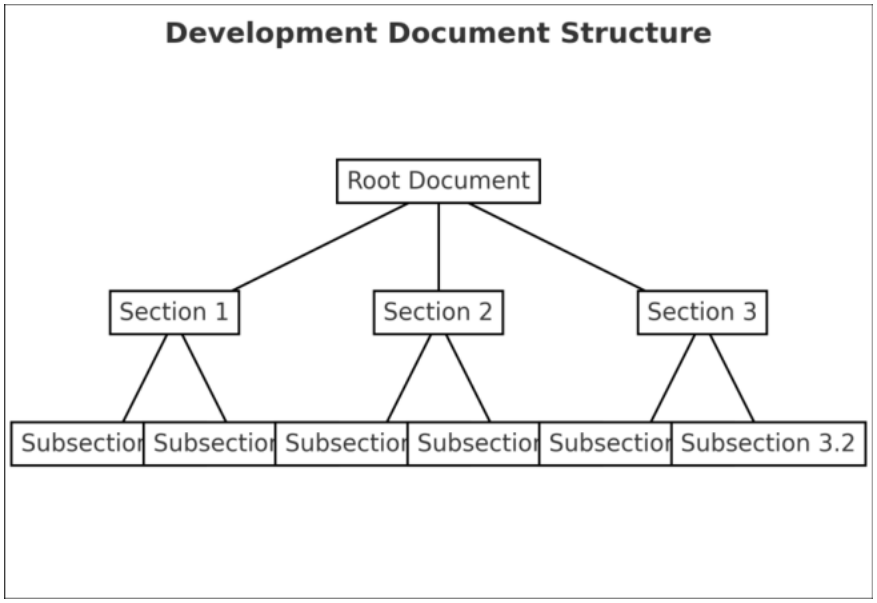


Figure 3-439 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-587 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

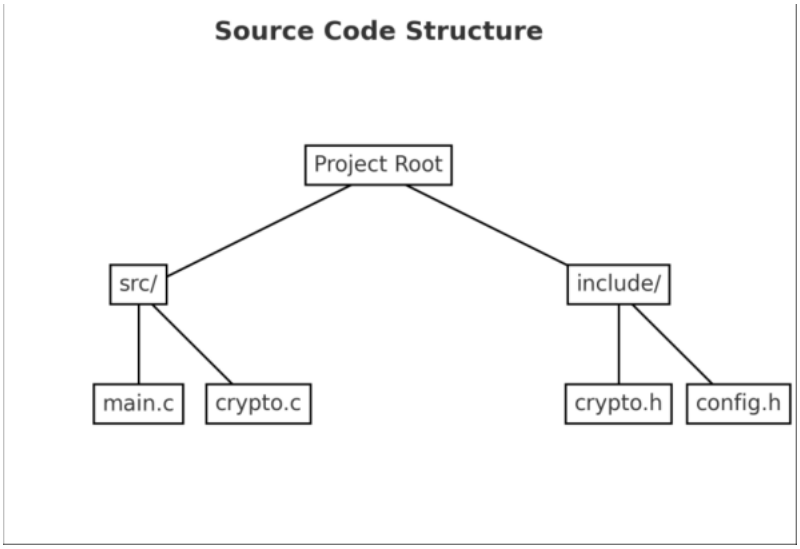


Figure 3-440 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-588 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

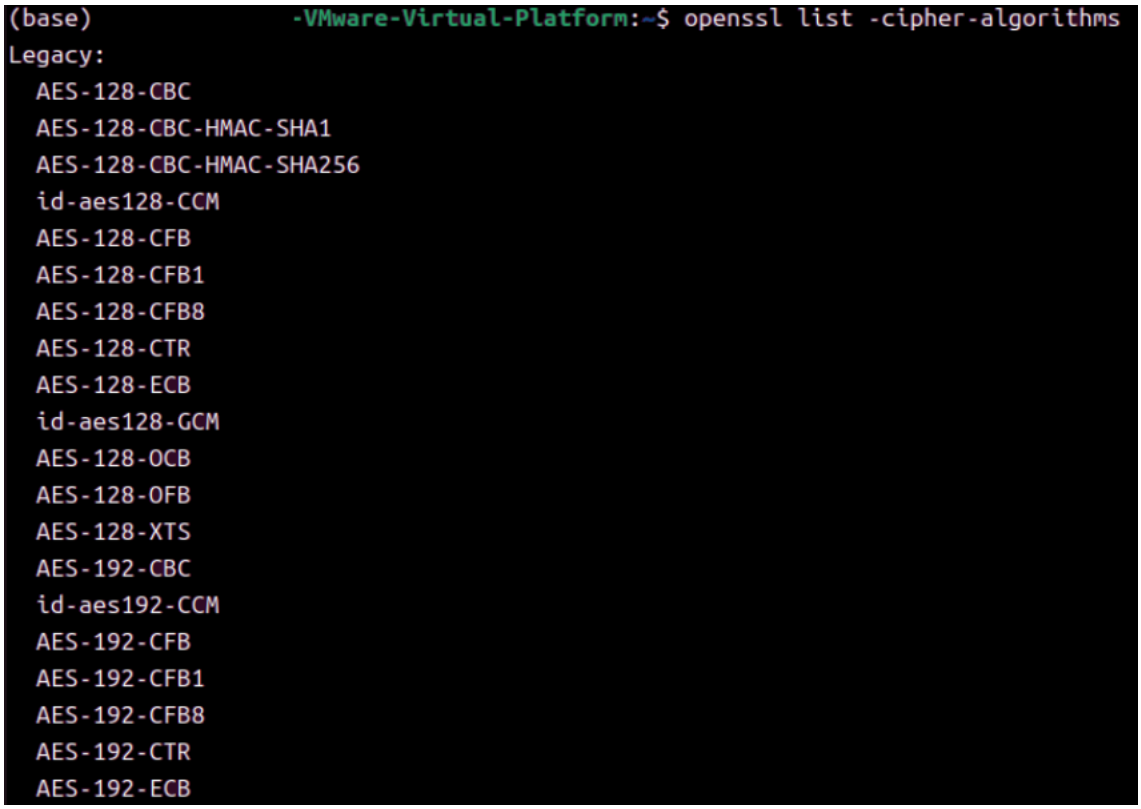


Figure 3-441 그림 제목

8.5.3 판정근거

Table 3-589 TE11.04.02 시험결과 판정근거

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

8.5.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.6 TE11.04.03

8.6.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.04.03	형상 항목의 버전 식별 방법	개발문서 검토

8.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-590 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

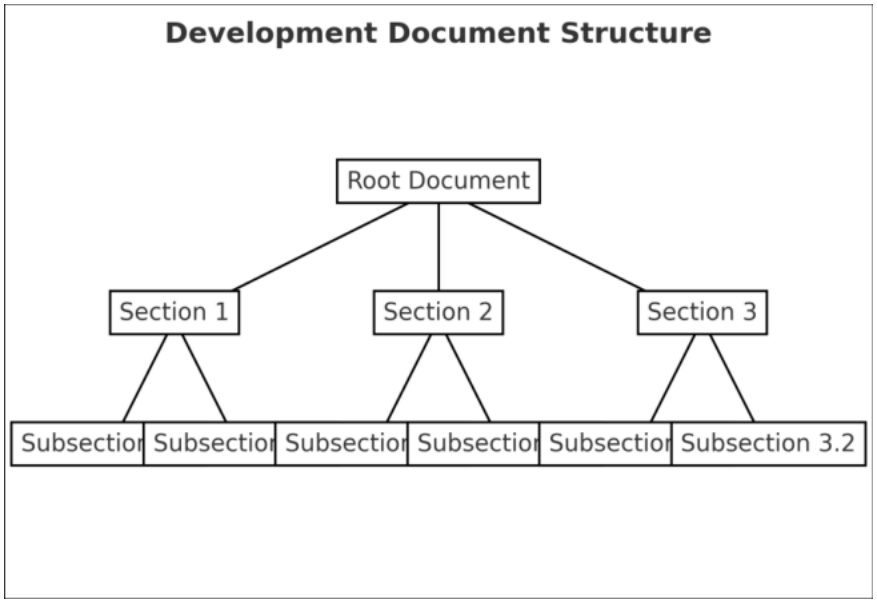


Figure 3-442 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-591 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

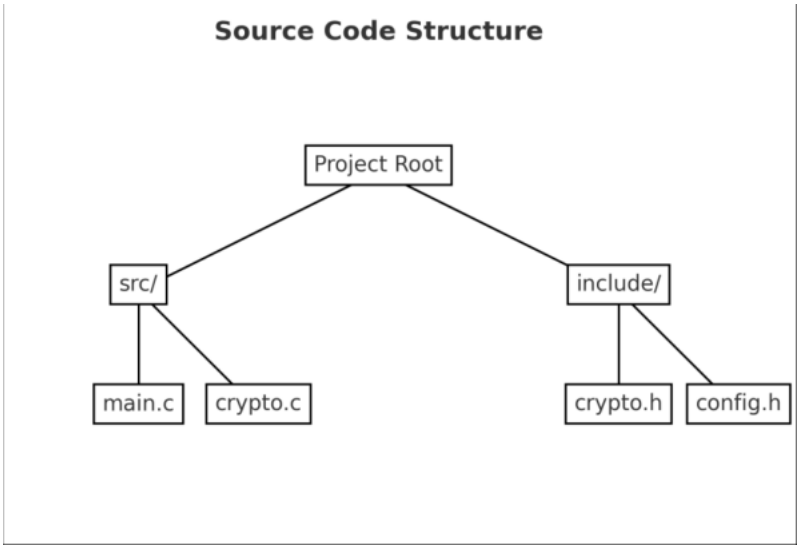


Figure 3-443 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-592 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

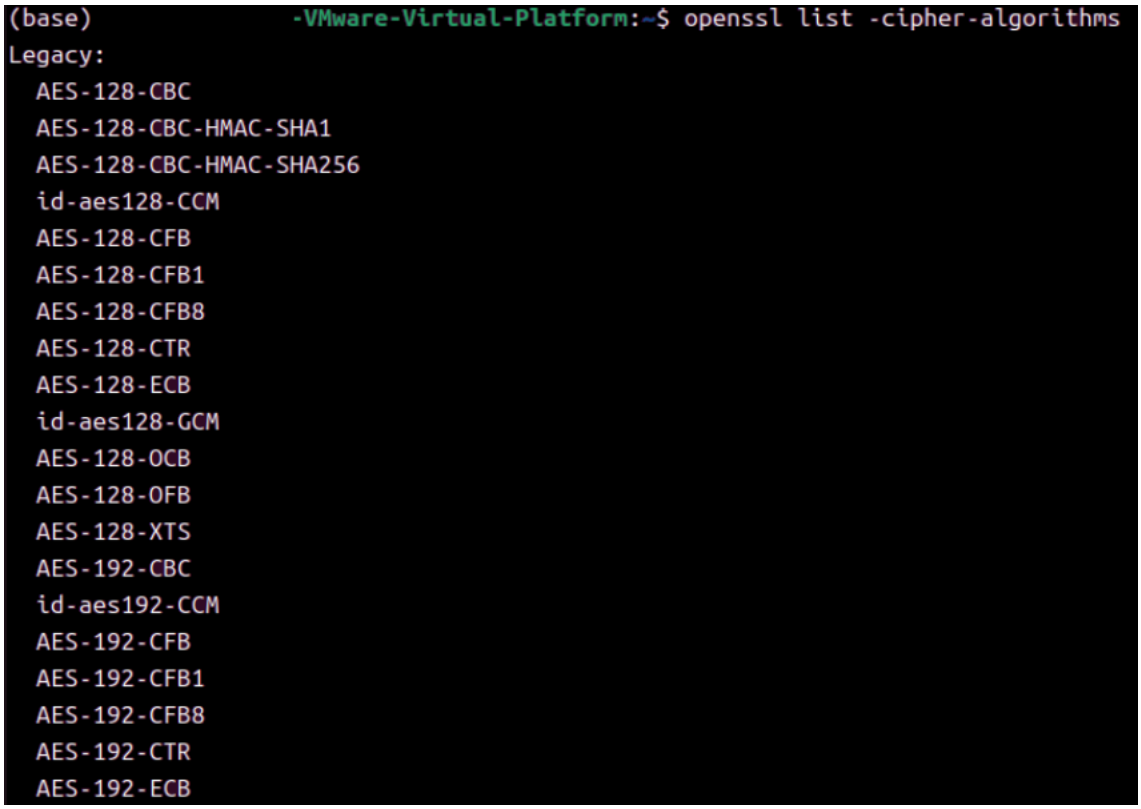


Figure 3-444 그림 제목

8.6.3 판정근거

Table 3-593 TE11.04.03 시험결과 판정근거

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

8.6.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.7 TE11.04.04

8.7.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.04.04	형상 항목의 버전 유일성	개발문서 검토

8.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-594 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

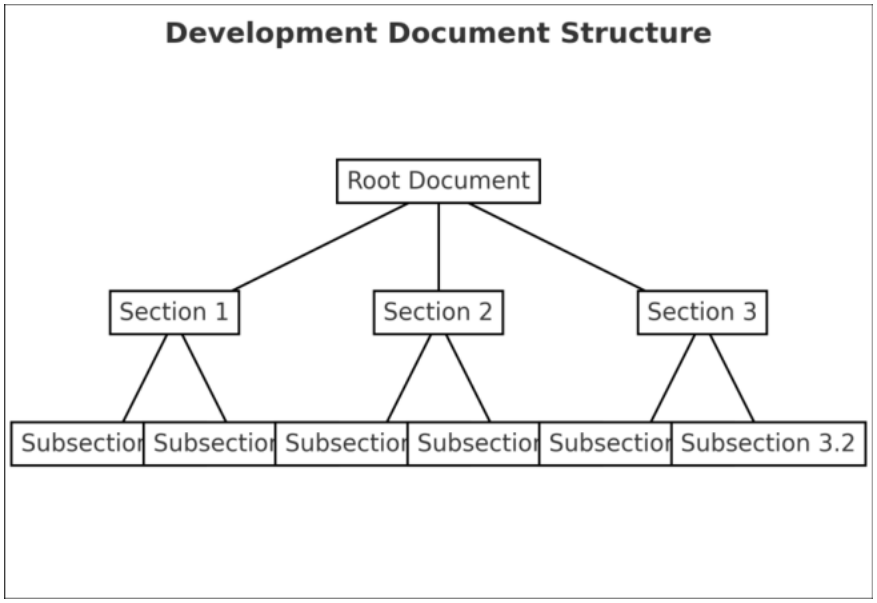


Figure 3-445 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-595 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

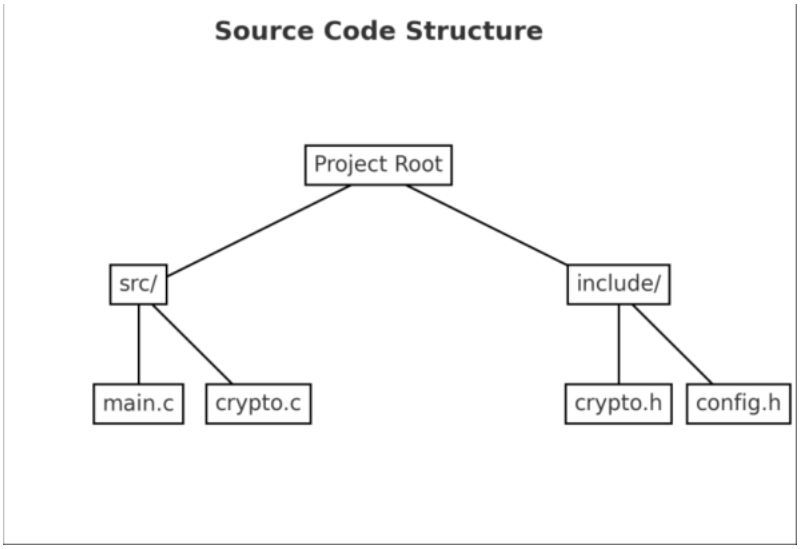


Figure 3-446 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-596 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

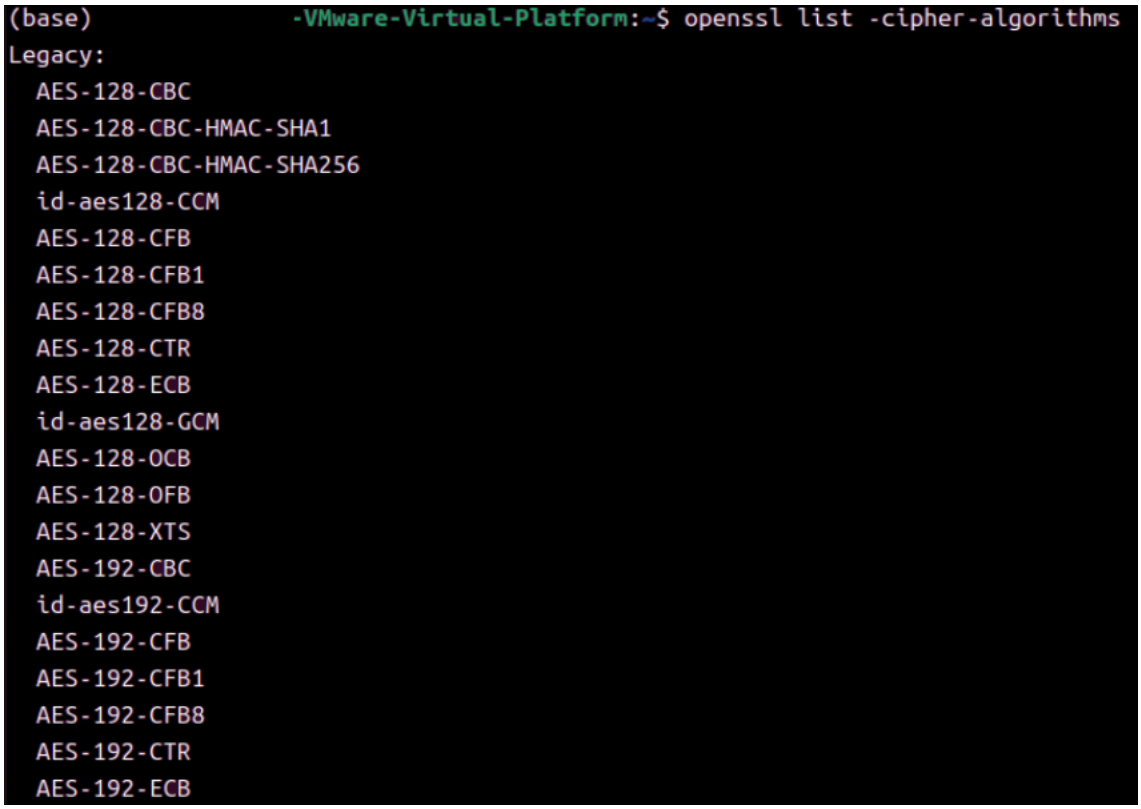


Figure 3-447 그림 제목

8.7.3 판정근거

Table 3-597 TE11.04.04 시험결과 판정근거

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

8.7.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.8 TE11.05.01

8.8.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.05.01	승인된 형상 변경 정보 적용 방법	개발문서 검토

8.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-598 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

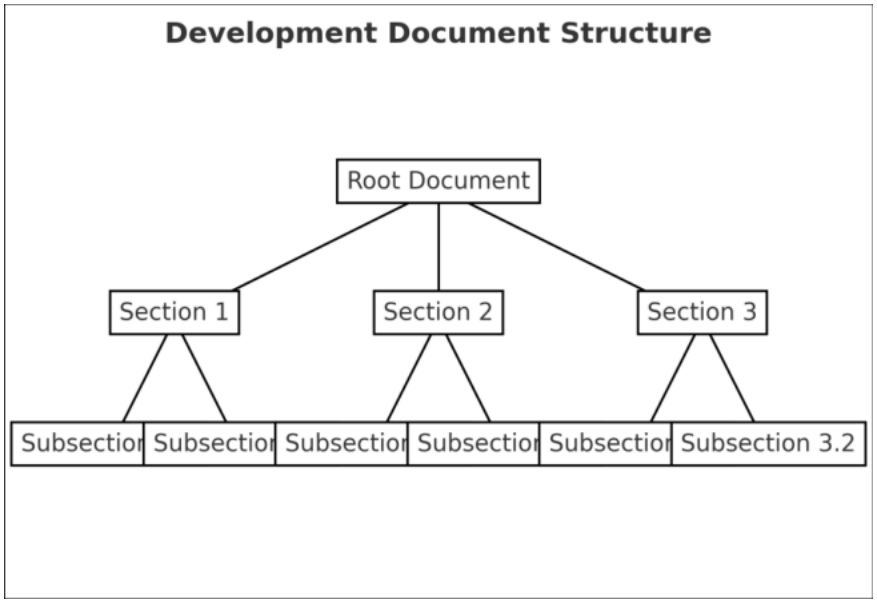


Figure 3-448 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-599 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

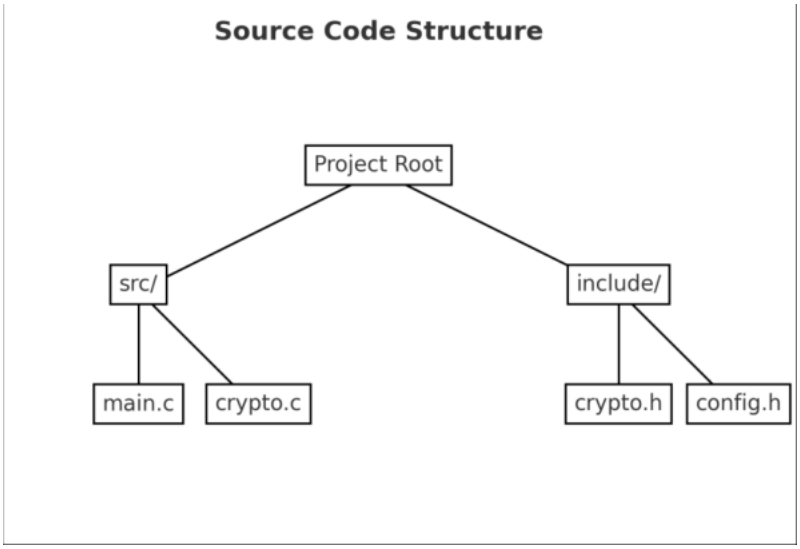


Figure 3-449 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-600 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

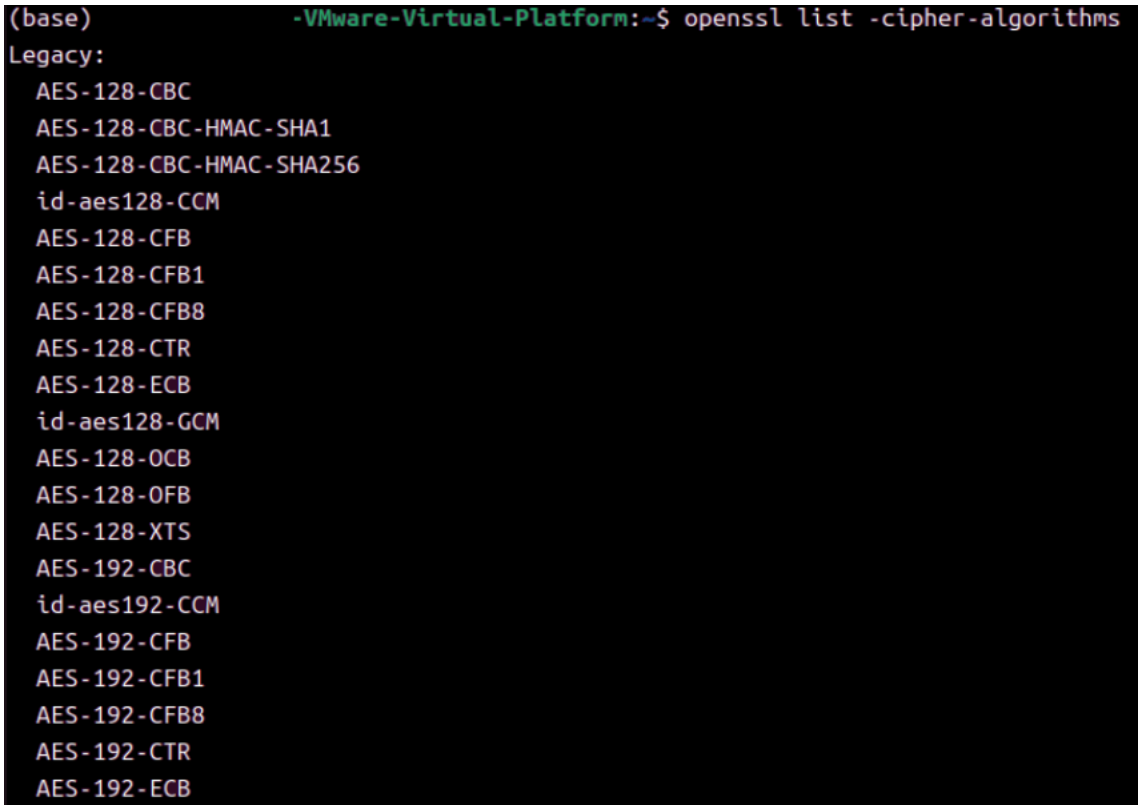


Figure 3-450 그림 제목

8.8.3 판정근거

Table 3-601 TE11.05.01 시험결과 판정근거

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

8.8.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.9 TE11.08.01

8.9.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.01	유한상태 모델 검증 (상태 천이 조건 , 입력 데이터 , 제어 입력 , 상태 천이 후 데이터 출력 및 상태 출력)	개발문서 검토

8.9.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-602 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

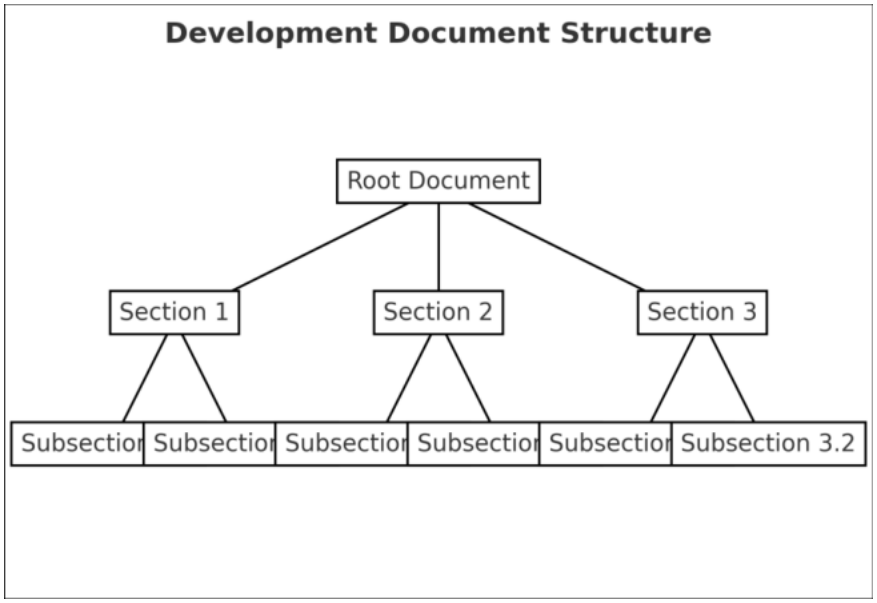


Figure 3-451 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-603 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

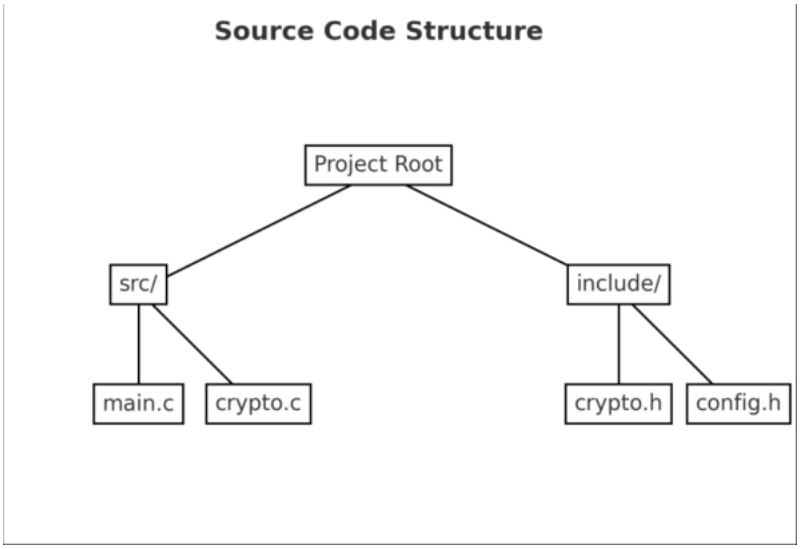


Figure 3-452 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-604 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

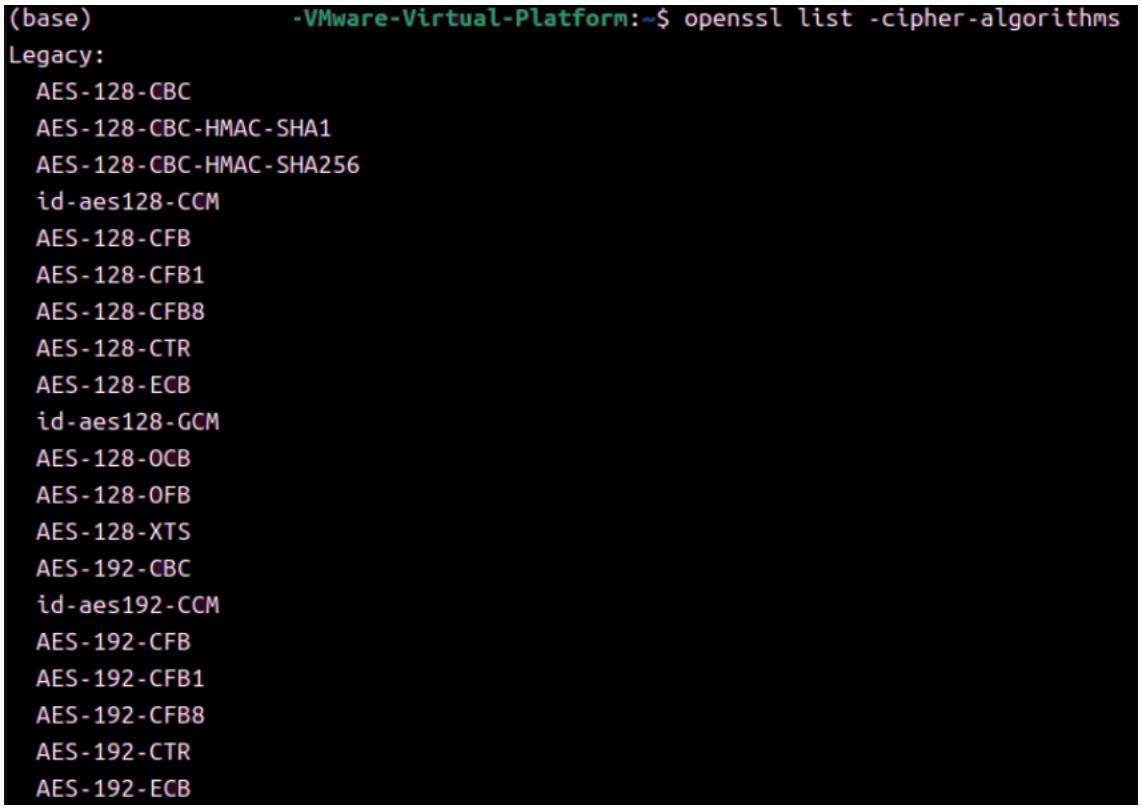


Figure 3-453 그림 제목

8.9.3 판정근거

Table 3-605 TE11.08.01 시험결과 판정근거

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

8.9.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.10 TE11.08.02

8.10.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.02	유한상태 천이도	개발문서 검토

8.10.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-606 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

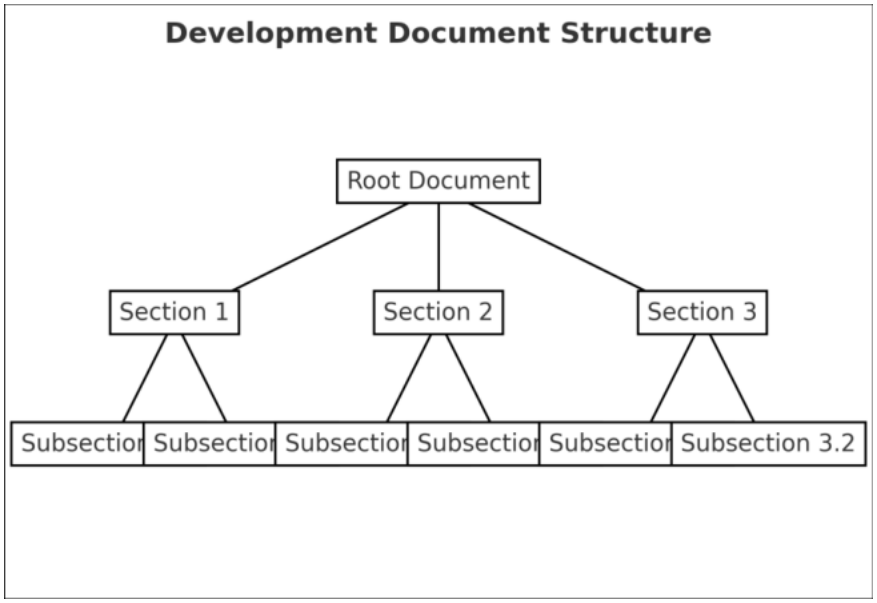


Figure 3-454 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-607 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

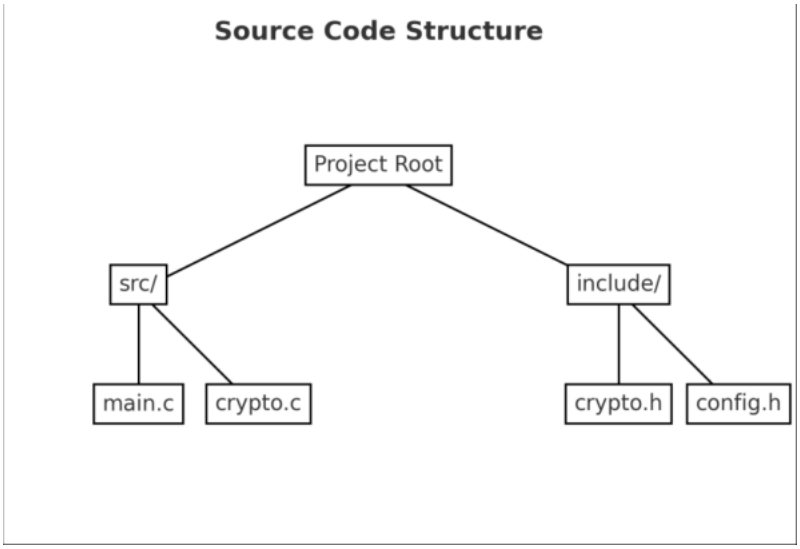


Figure 3-455 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-608 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

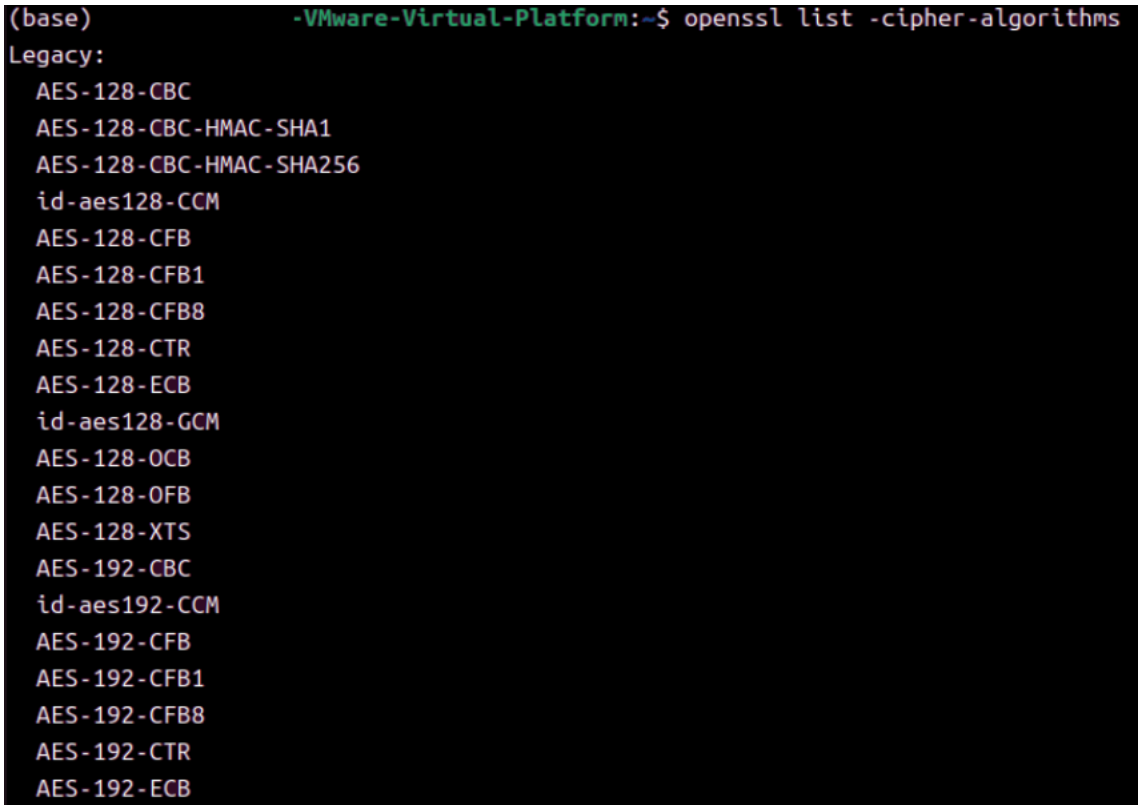


Figure 3-456 그림 제목

8.10.3 판정근거

Table 3-609 TE11.08.02 시험결과 판정근거

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

8.10.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.11 TE11.01.01

8.11.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.03	유한상태 모델의 상태 별 구분 정의	개발문서 검토

8.11.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-610 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

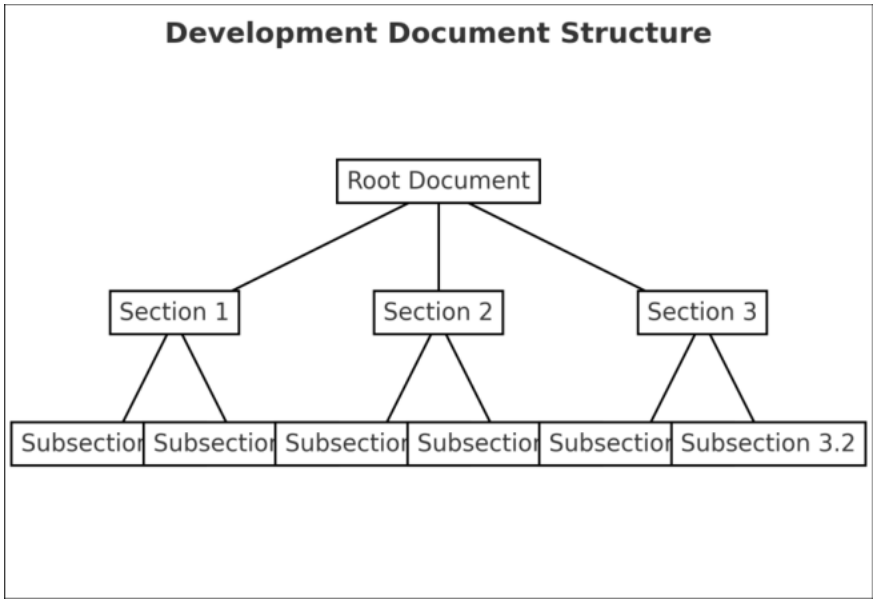


Figure 3-457 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-611 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

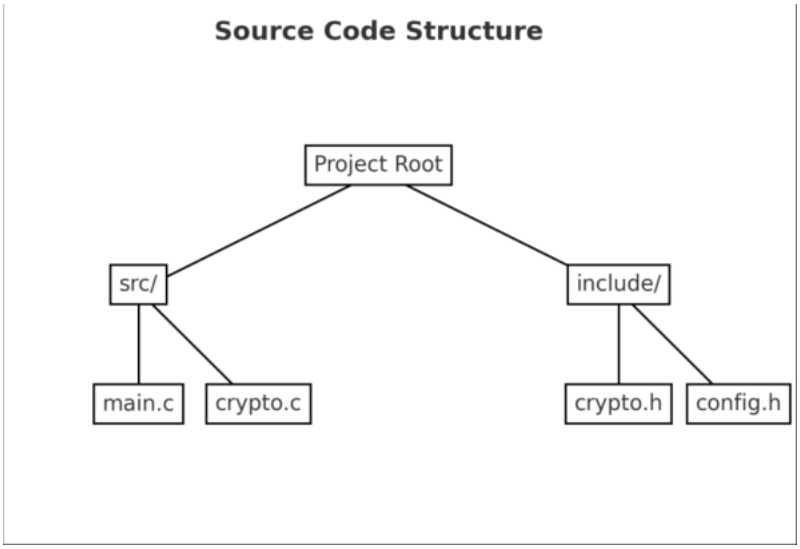


Figure 3-458 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-612 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

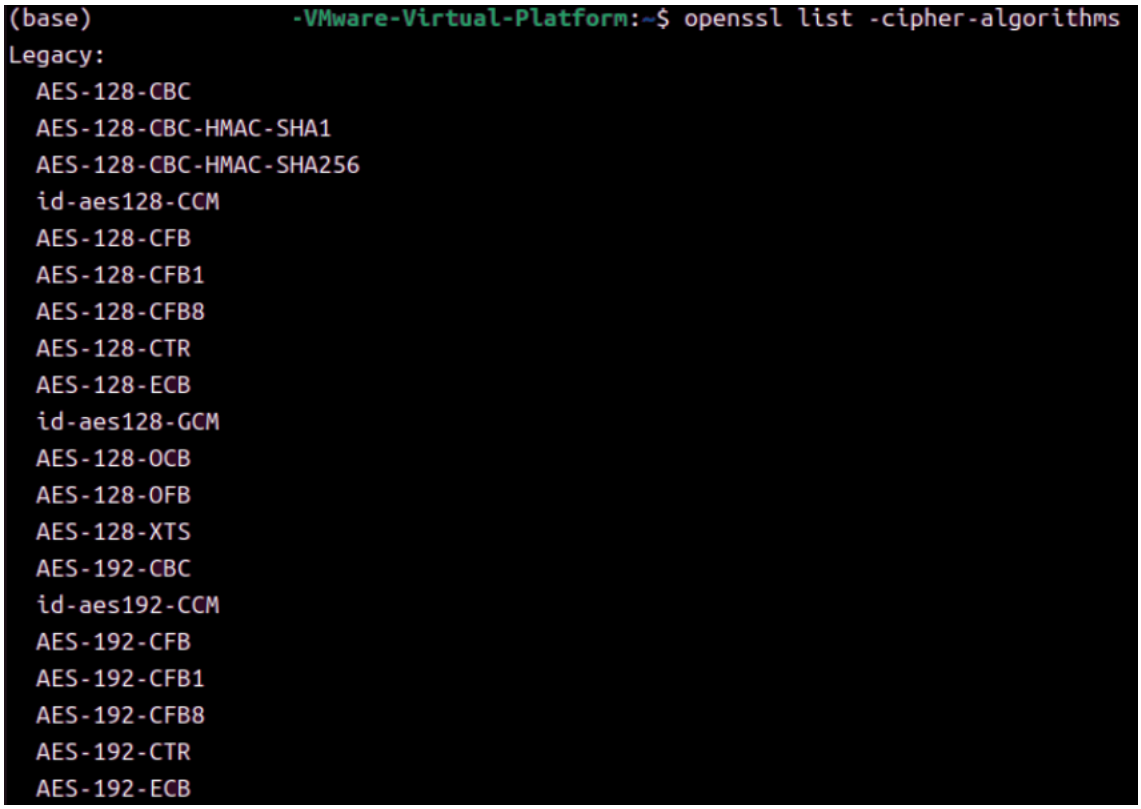


Figure 3-459 그림 제목

8.11.3 판정근거

Table 3-613 TE11.08.03 시험결과 판정근거

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

8.11.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.12 TE11.08.04

8.12.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.04	유한상태 천이도 모든 상태의 상태 천이표와 상태 설명	개발문서 검토

8.12.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-614 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

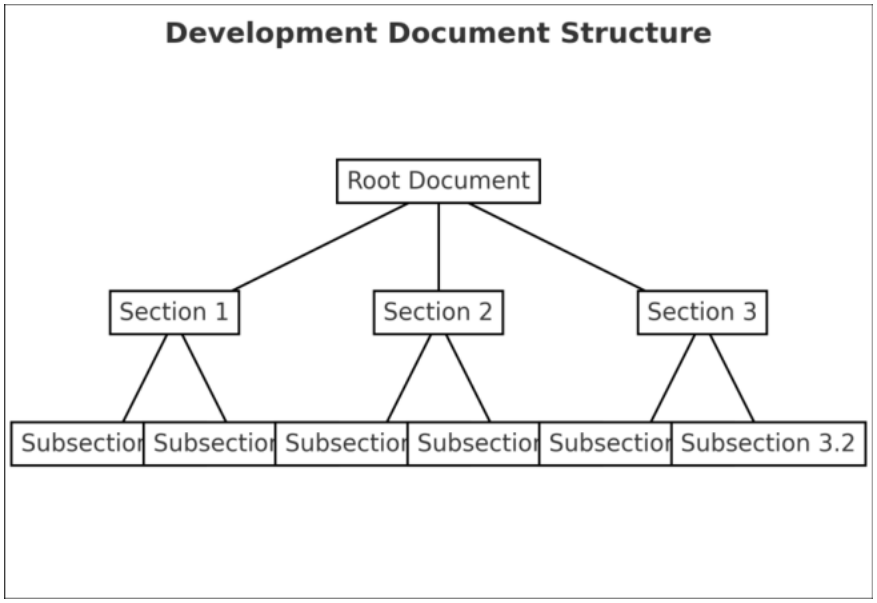


Figure 3-460 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-615 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

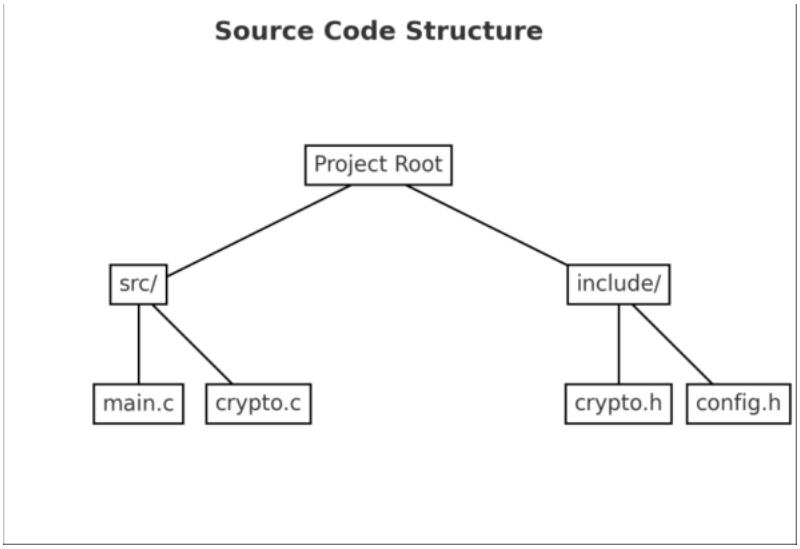


Figure 3-461 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-616 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

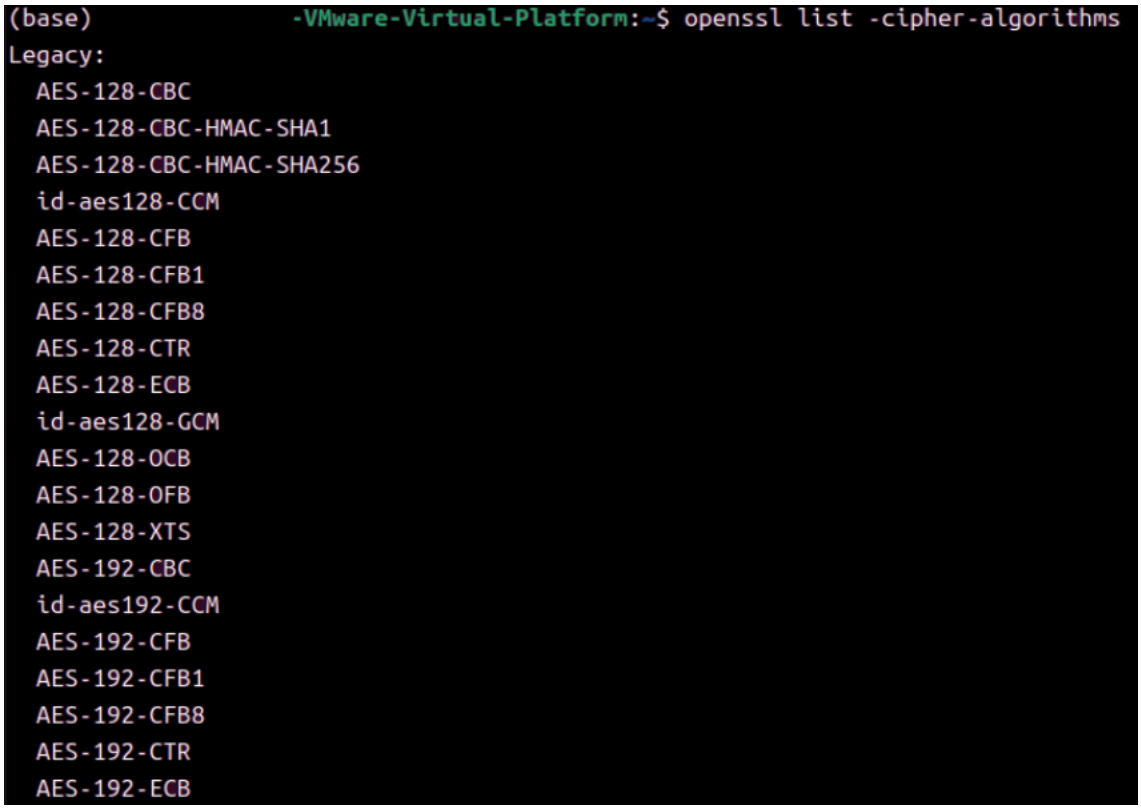


Figure 3-462 그림 제목

8.12.3 판정근거

Table 3-617 TE11.08.04 시험결과 판정근거

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

8.12.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.13 TE11.08.05

8.13.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.05	모든 상태의 상태 천이도 명세화	개발문서 검토

8.13.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-618 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

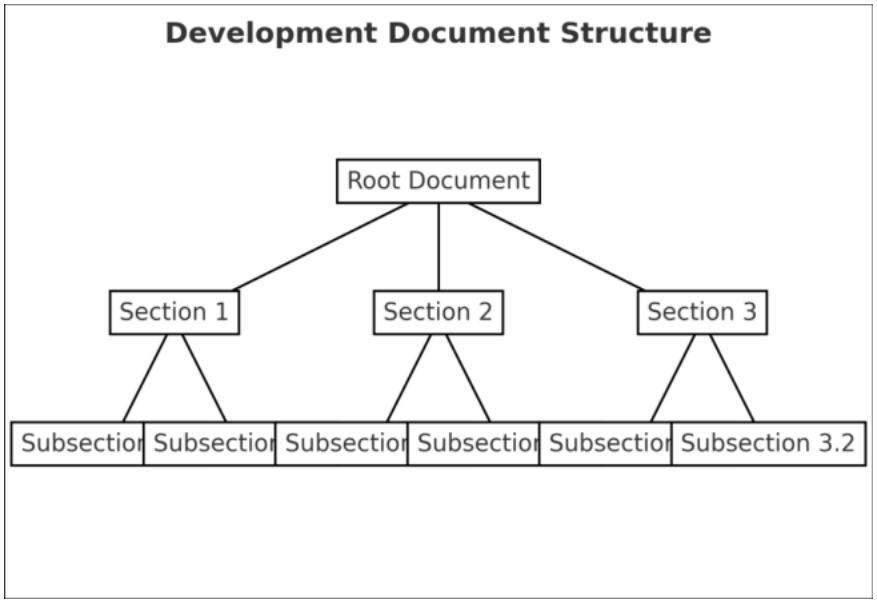


Figure 3-463 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-619 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

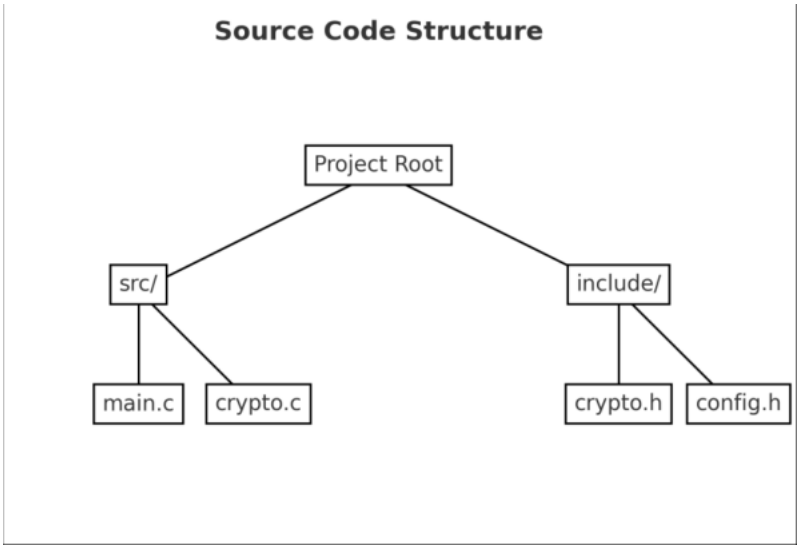


Figure 3-464 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-620 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

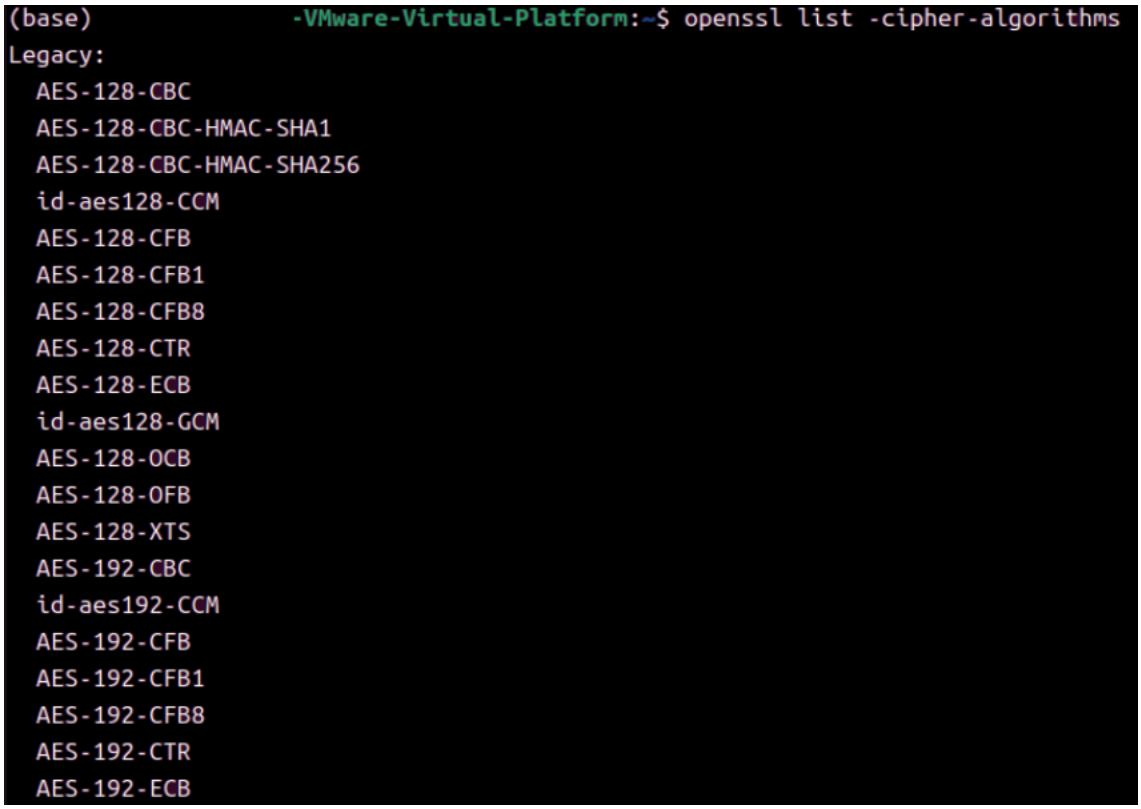


Figure 3-465 그림 제목

8.13.3 판정근거

Table 3-621 TE11.08.05 시험결과 판정근거

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

8.13.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.14 TE11.08.06

8.14.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.06	모듈 동작이 유한상태 천이도와 상태 천이표 및 상태 설명과의 일관성	암호모듈 검사

8.14.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-622 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

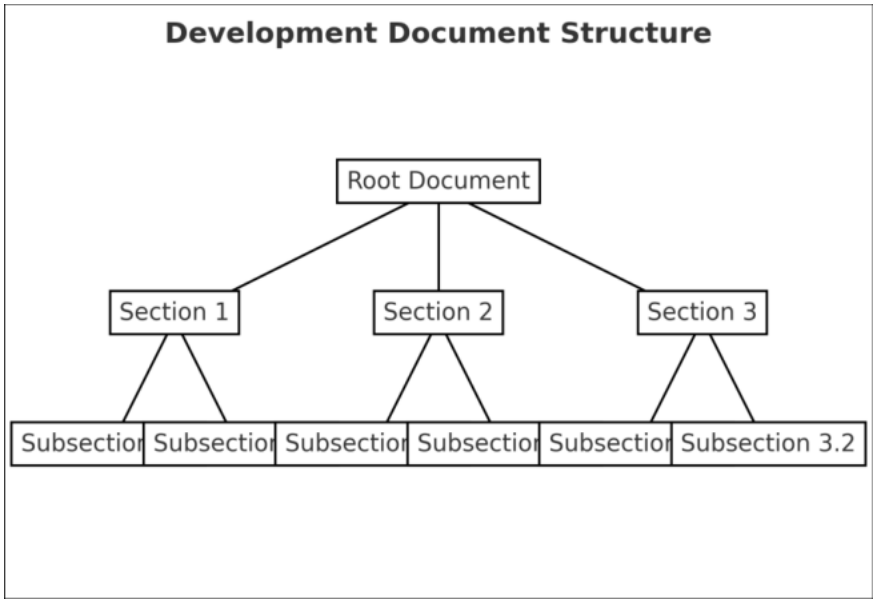


Figure 3-466 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-623 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

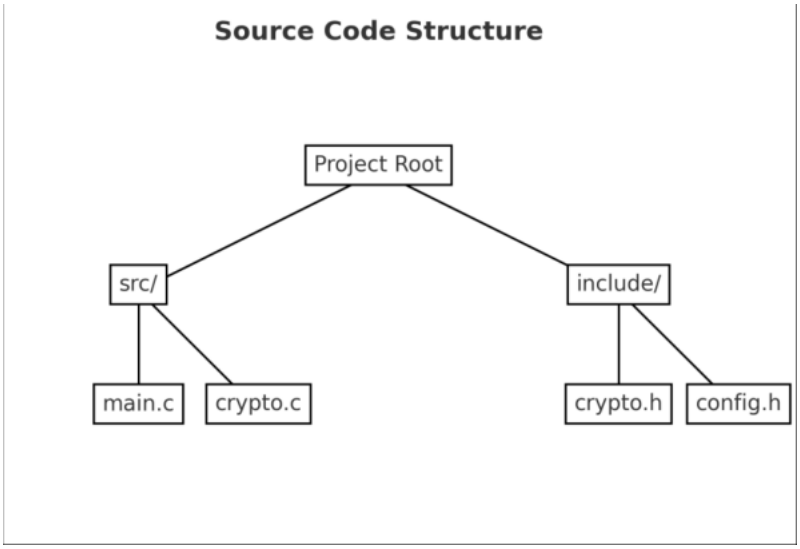


Figure 3-467 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-624 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

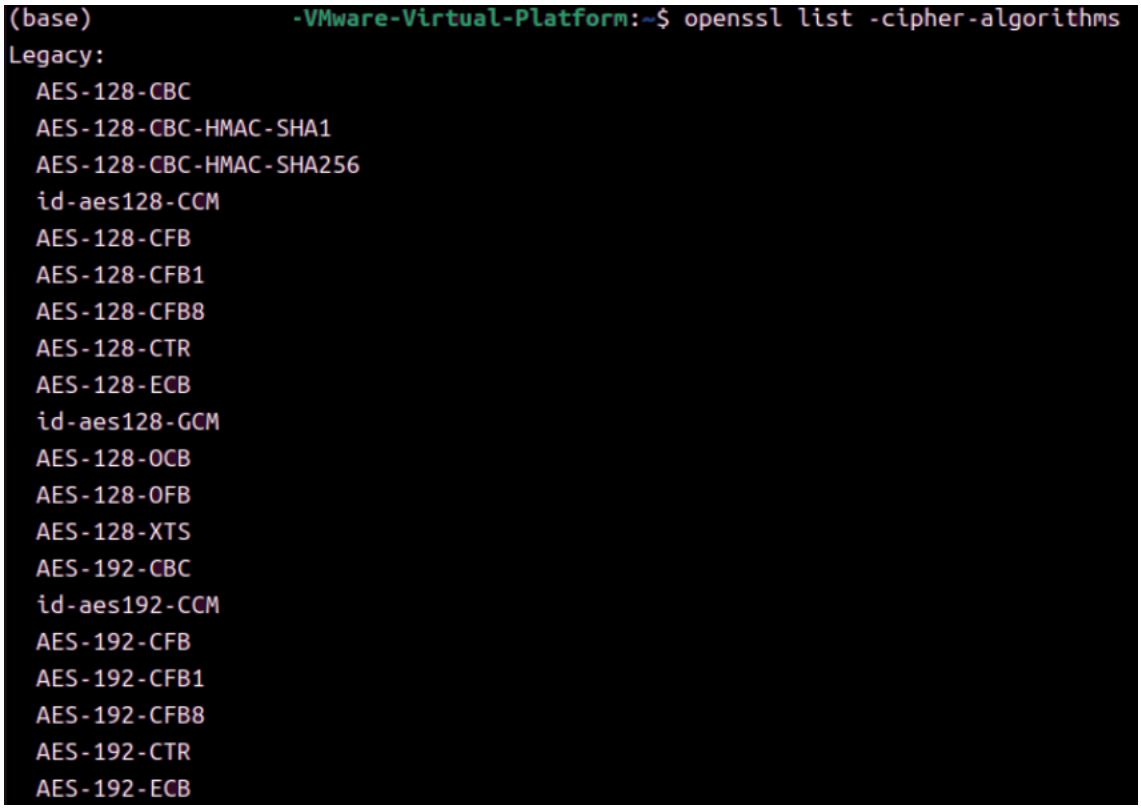


Figure 3-468 그림 제목

8.14.3 판정근거

Table 3-625 TE11.08.06 시험결과 판정근거

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

8.14.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.15 TE11.08.07

8.15.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.01.07	유지보수 인터페이스 포함 시 적어도 한 개 이상의 유지보수 상태 정의 및 유지보수 상태의 유한상태 모델 포함 여부	개발문서 검토

8.15.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-626 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

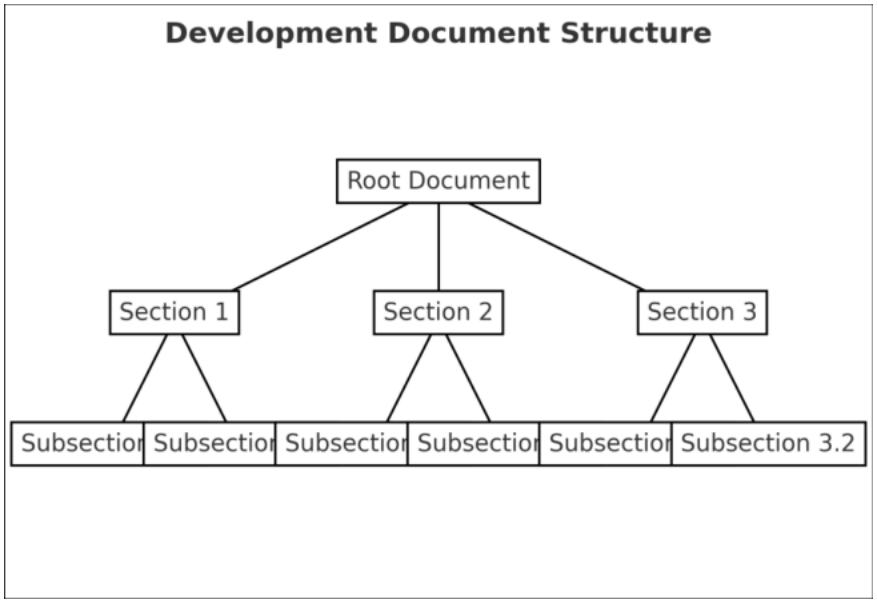


Figure 3-469 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-627 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

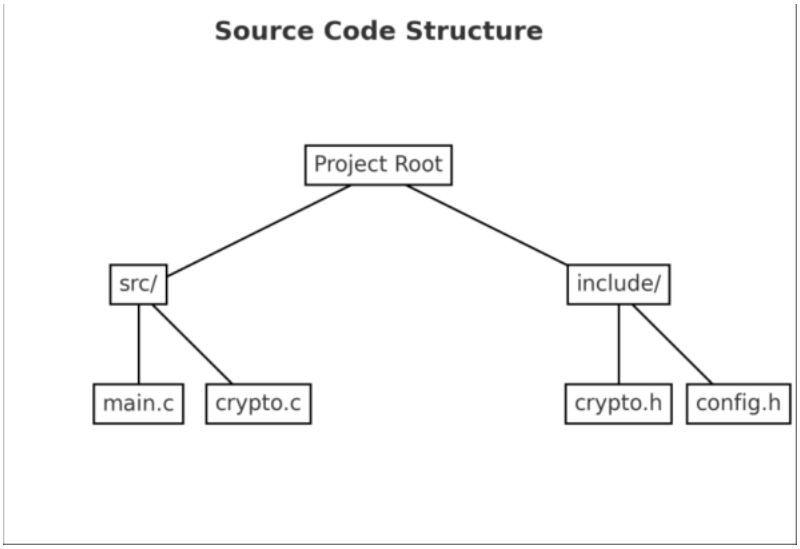


Figure 3-470 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-628 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

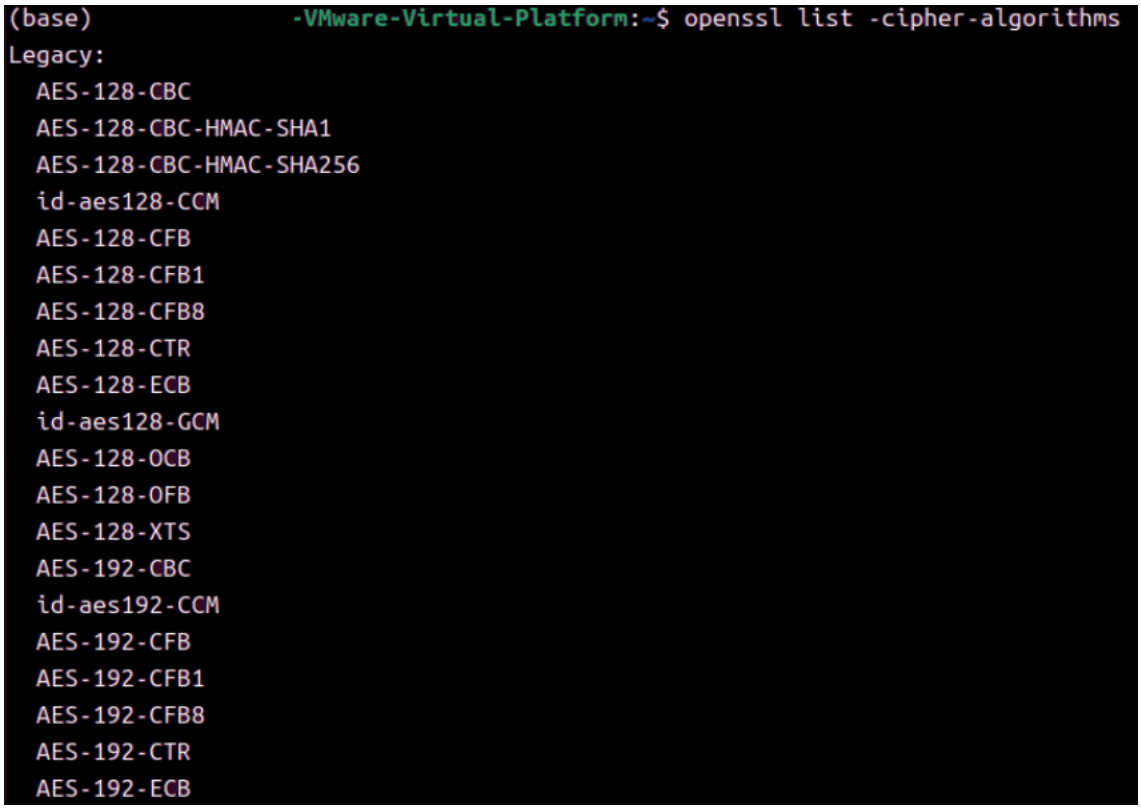


Figure 3-471 그림 제목

8.15.3 판정근거

Table 3-629 TE11.08.07 시험결과 판정근거

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

8.15.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.16 TE11.08.08

8.16.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.08	유한상태 모델 분기 상태 명세 및 동작	개발문서 검토

8.16.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-630 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

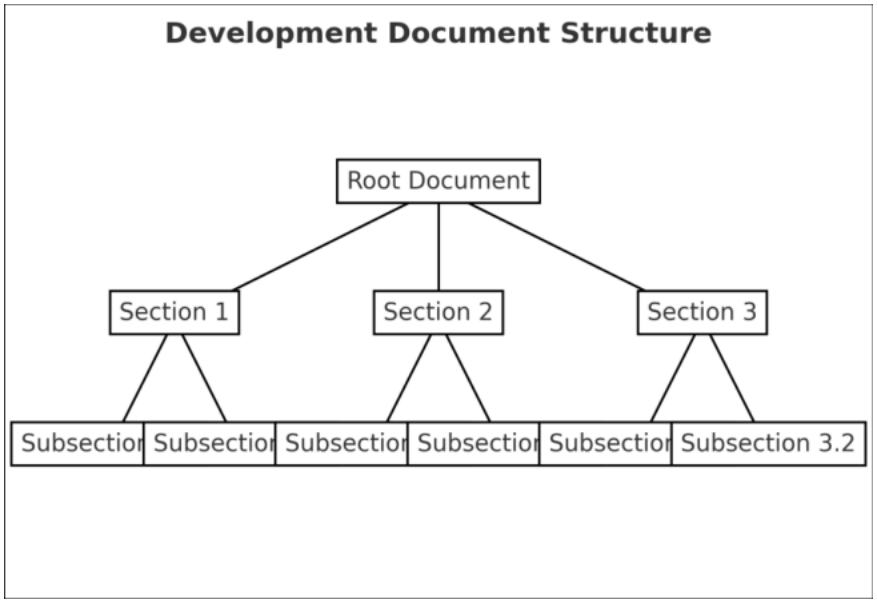


Figure 3-472 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-631 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

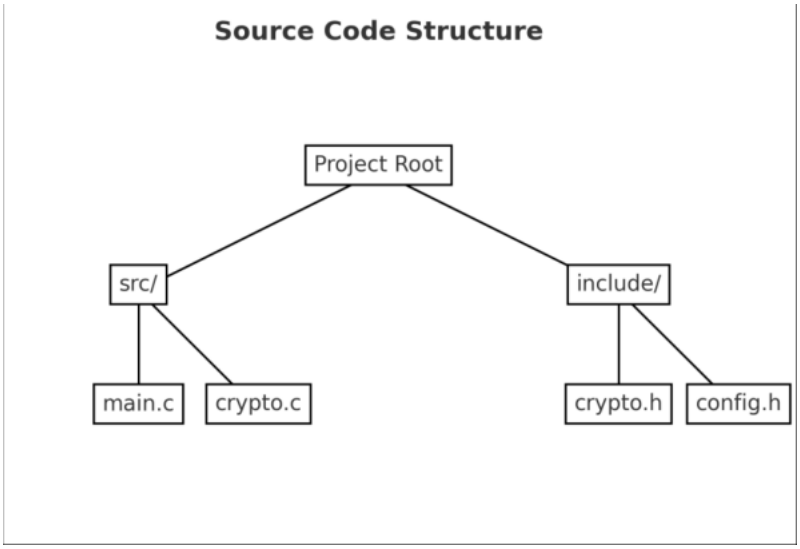


Figure 3-473 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-632 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

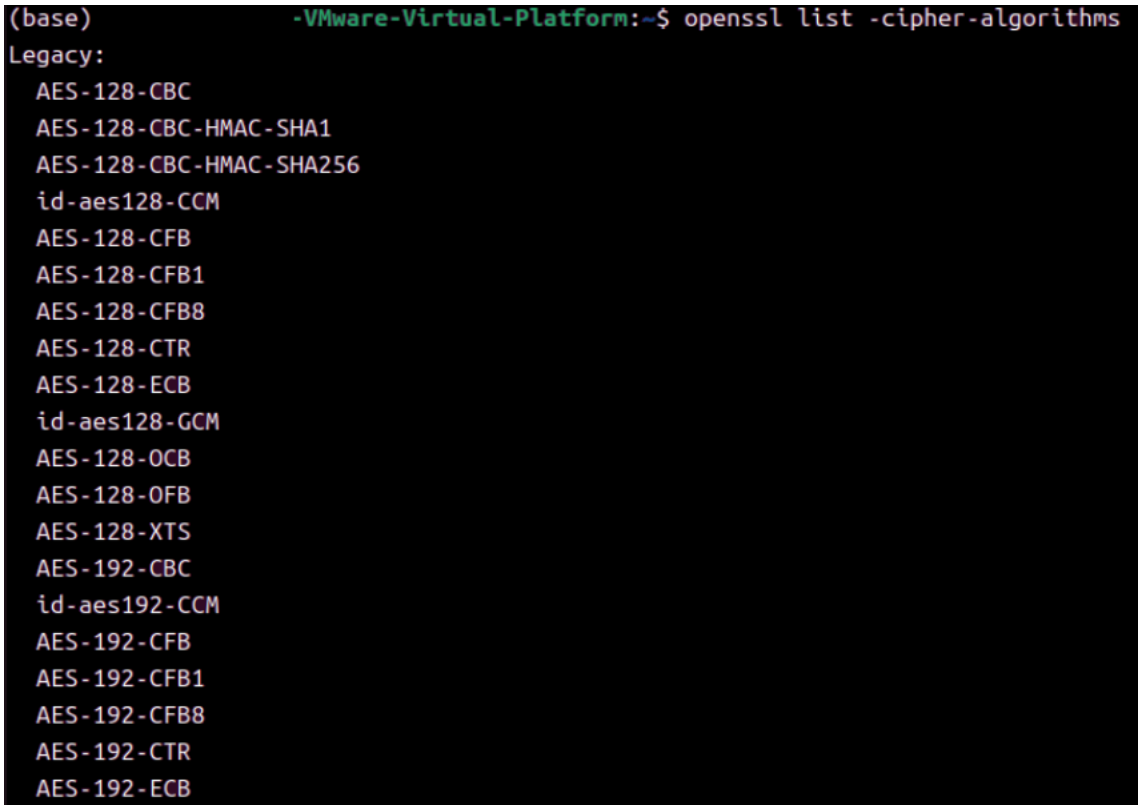


Figure 3-474 그림 제목

8.16.3 판정근거

Table 3-633 TE11.08.08 시험결과 판정근거

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

8.16.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.17 TE11.08.09

8.17.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.09	특정 상태에 있는 동안을 나타내는 상태 표시	암호모듈 검사

8.17.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-634 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

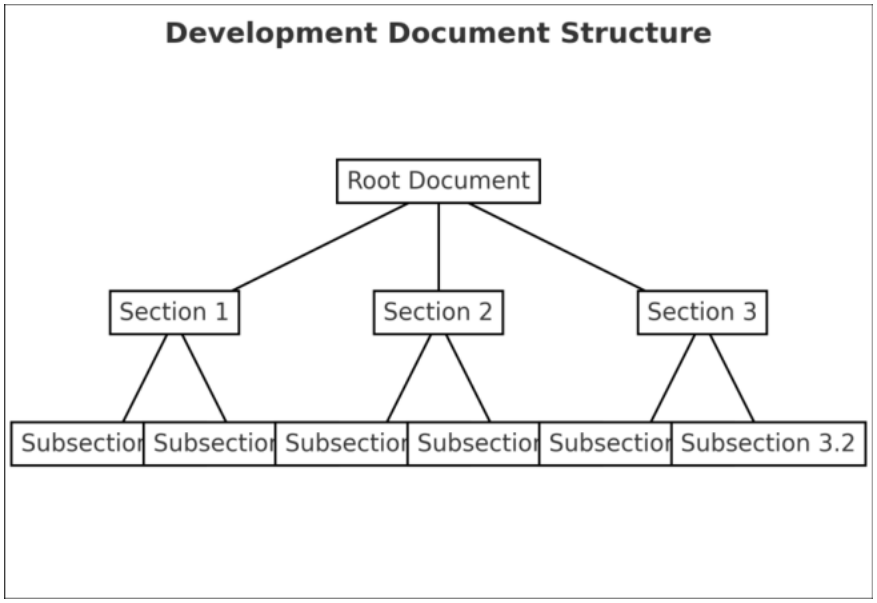


Figure 3-475 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-635 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

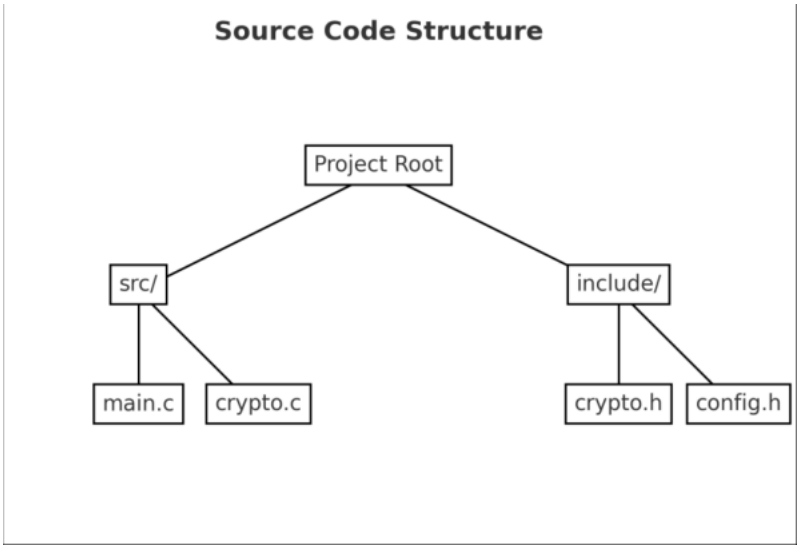


Figure 3-476 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-636 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

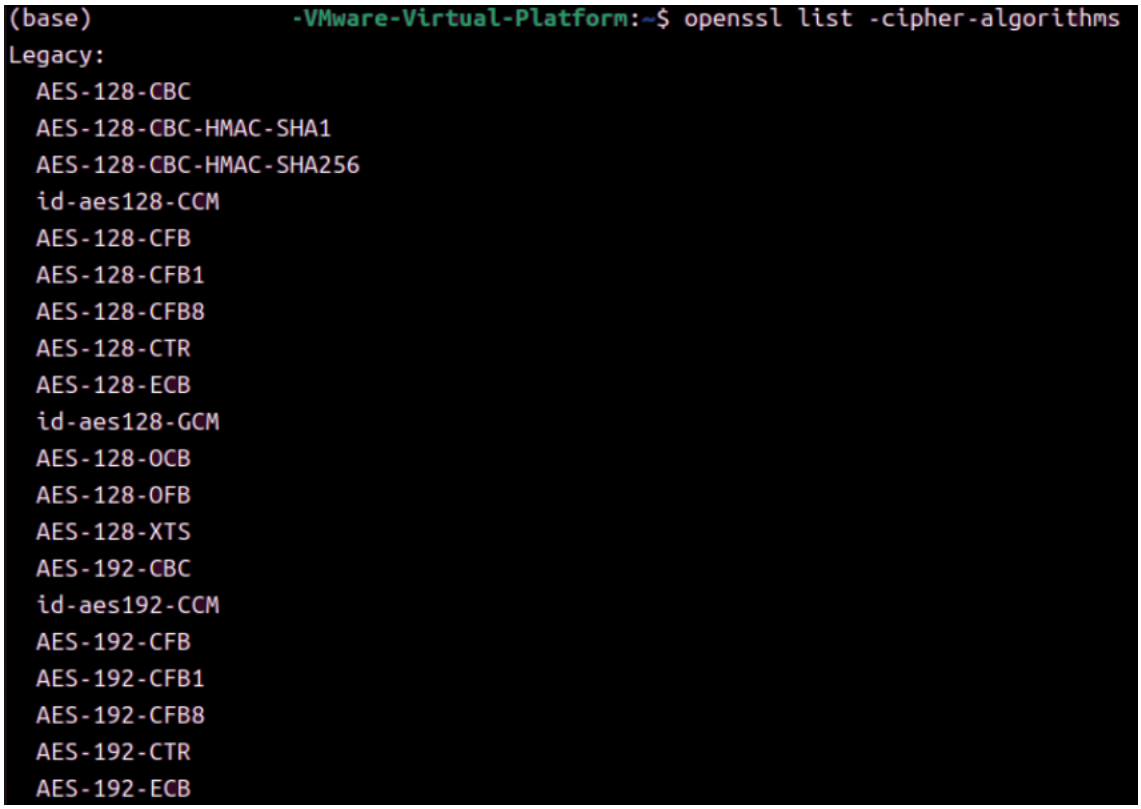


Figure 3-477 그림 제목

8.17.3 판정근거

Table 3-637 TE11.08.09 시험결과 판정근거

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

8.17.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.18 TE11.08.10

8.18.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.10	초기 전원 인가 상태에서 암호모듈의 다른 모든 상태로 천이 체인의 존재	암호모듈 검사

8.18.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-638 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

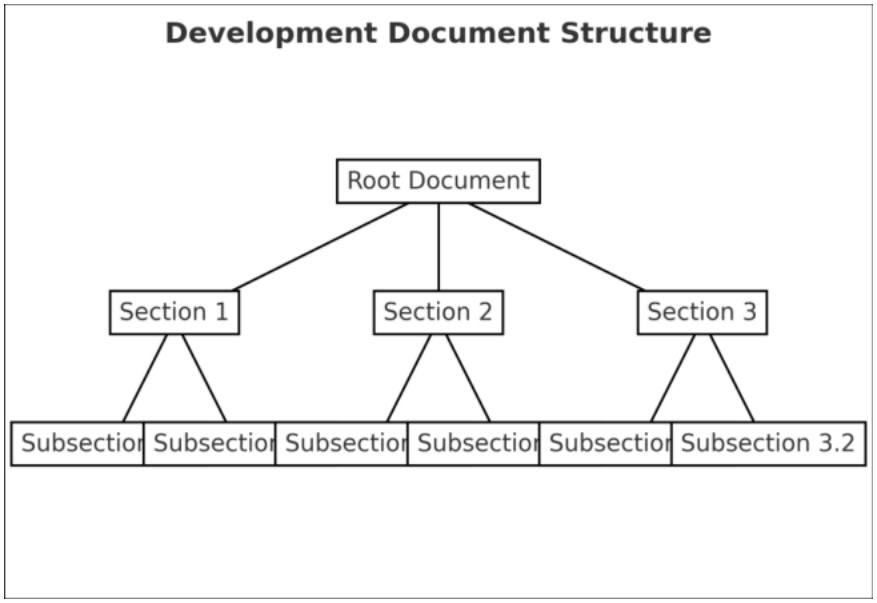


Figure 3-478 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-639 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

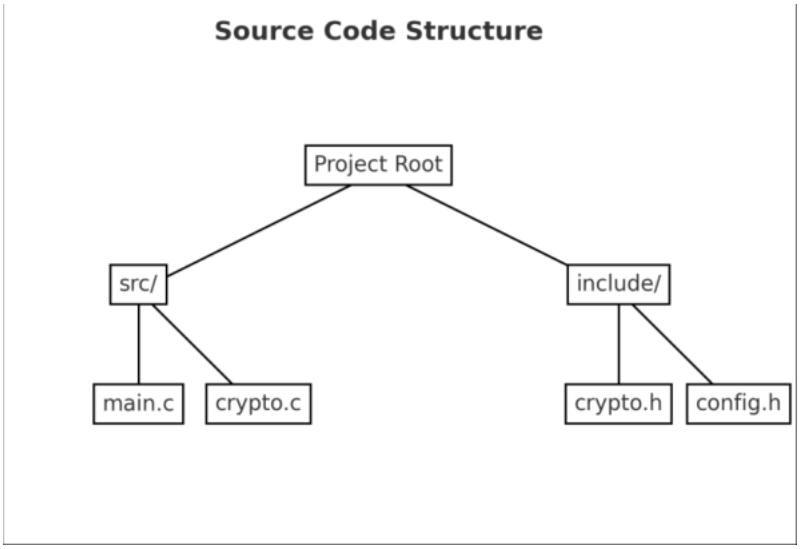


Figure 3-479 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-640 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

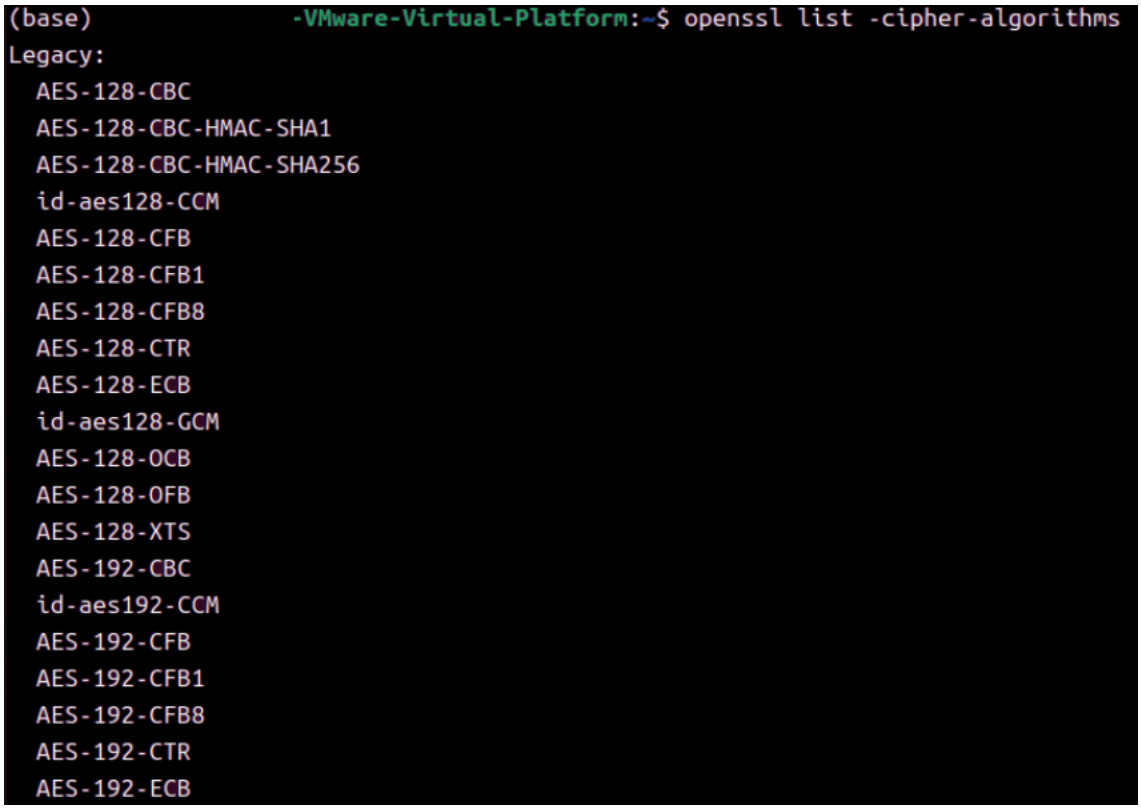


Figure 3-480 그림 제목

8.18.3 판정근거

Table 3-641 TE11.08.10 시험결과 판정근거

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

8.18.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.19 TE11.08.11

8.19.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.11	암호모듈의 다른 상태에서 전원 꺼진 상태로 천이하는 체인의 존재	개발문서 검토

8.19.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-642 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

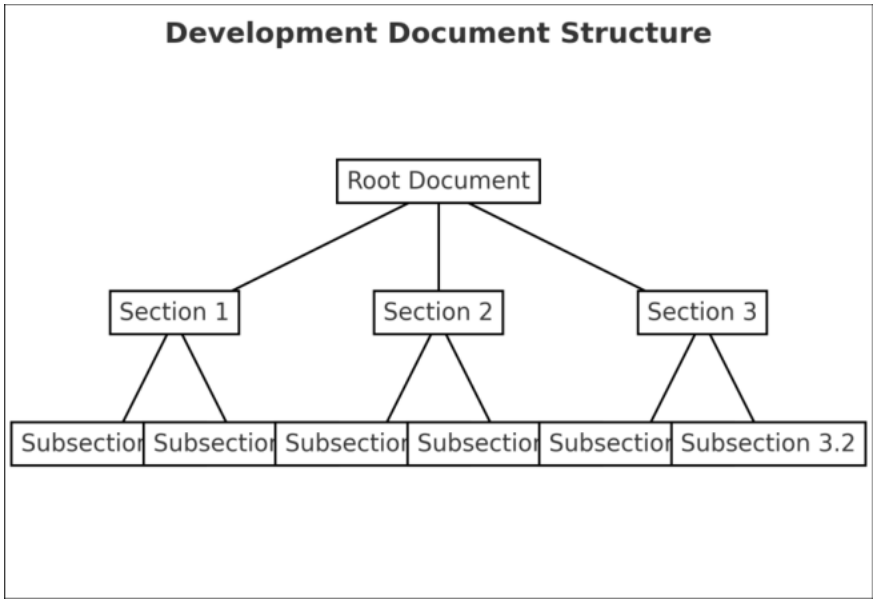


Figure 3-481 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-643 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

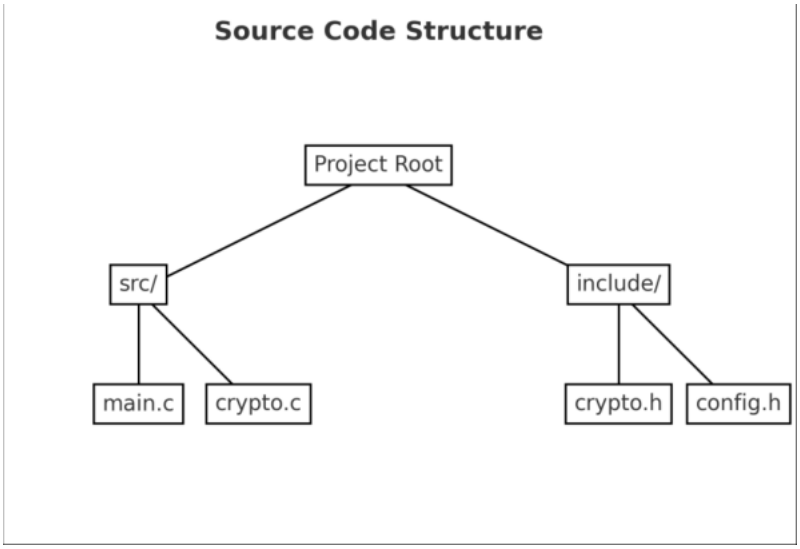


Figure 3-482 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-644 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

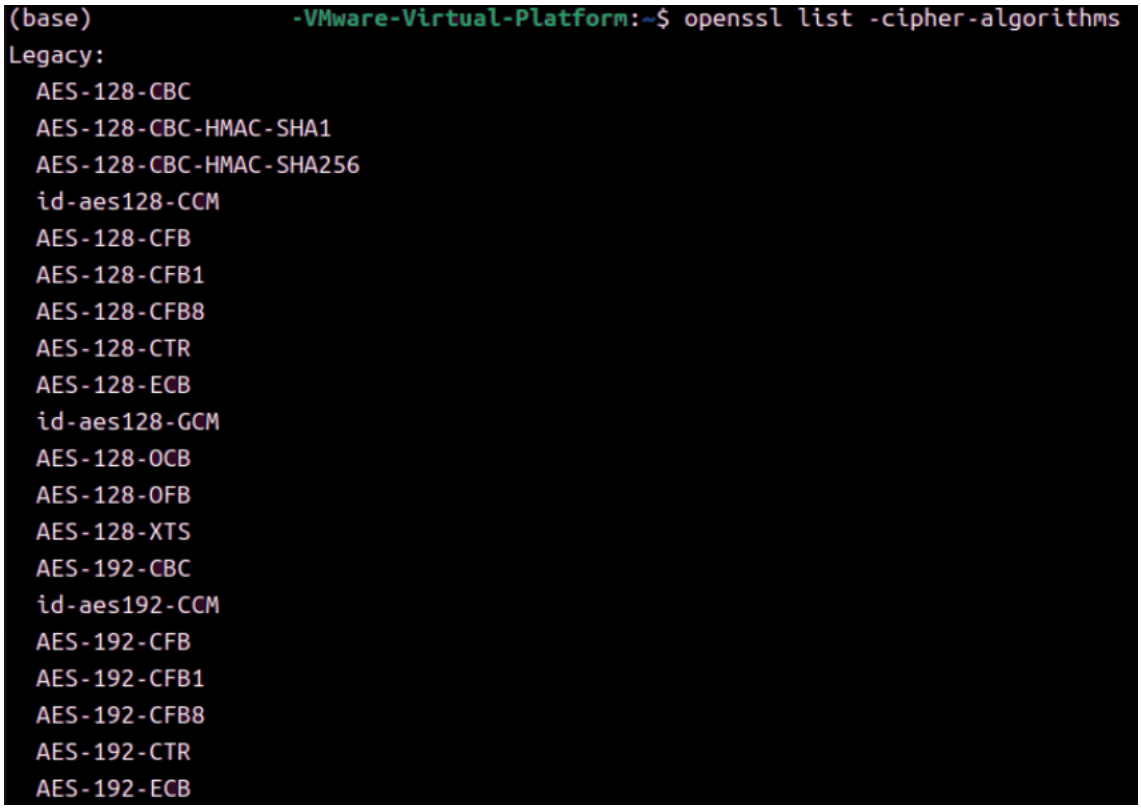


Figure 3-483 그림 제목

8.19.3 판정근거

Table 3-645 TE11.08.11 시험결과 판정근거

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

8.19.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.20 TE11.08.12

8.20.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.08.12	모든 가능한 데이터 입력 및 제어 입력에 의해 수행되는 유한상태 모델 작동 정의	개발문서 검토

8.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-646 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

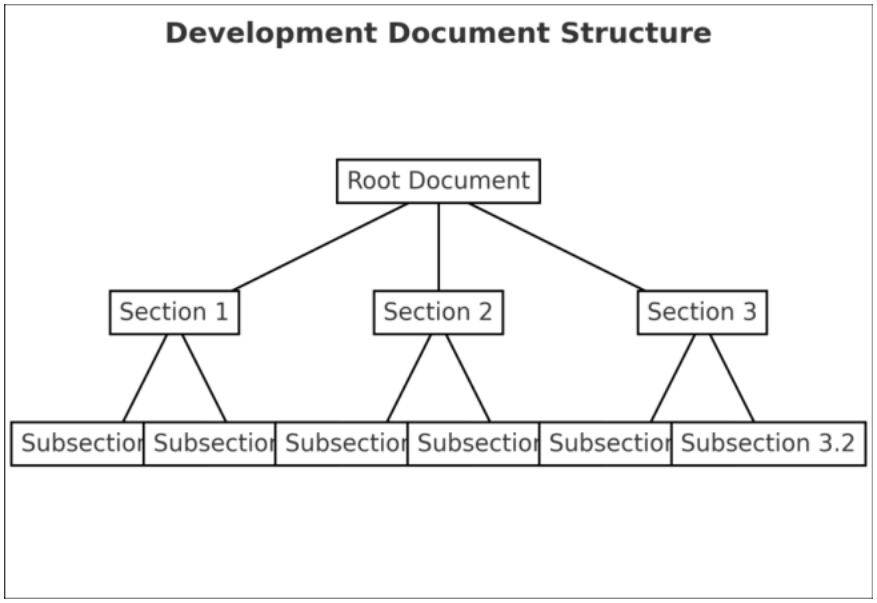


Figure 3-484 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-647 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

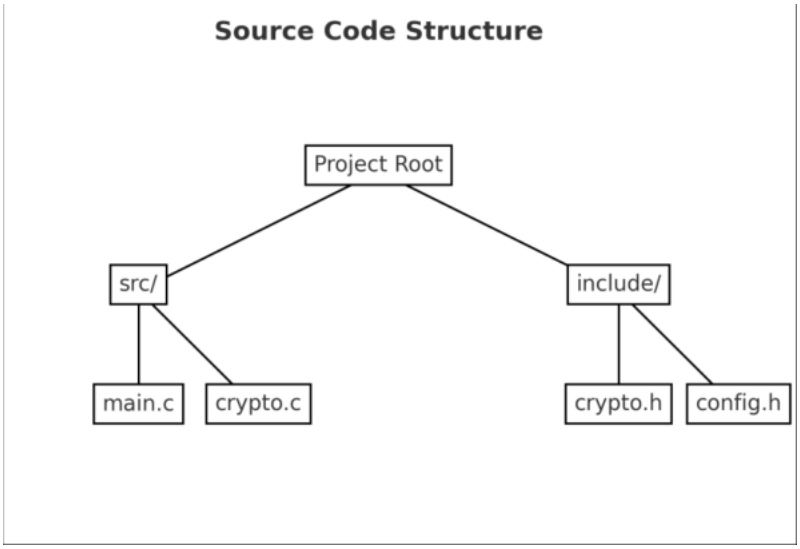


Figure 3-485 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-648 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

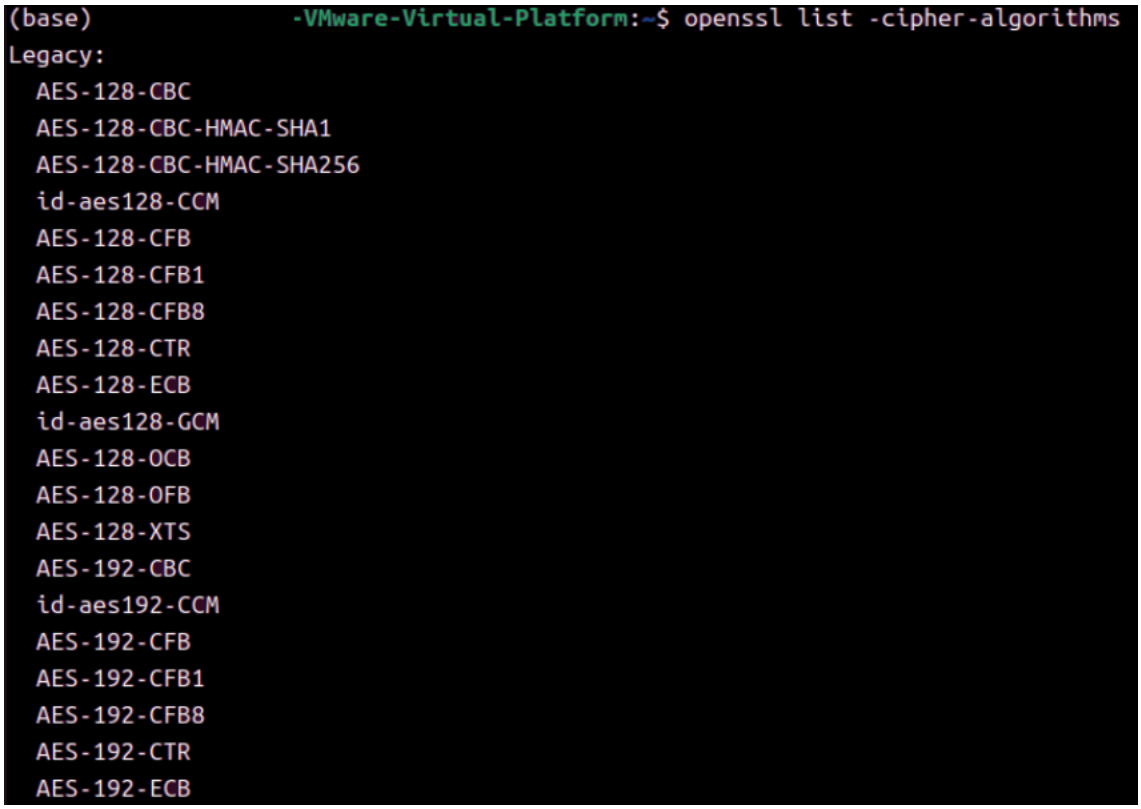


Figure 3-486 그림 제목

8.20.3 판정근거

Table 3-649 TE11.08.12 시험결과 판정근거

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

8.20.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.21 TE11.11.01

8.21.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.11.01	심각한 오류 상태가 아닌 모든 오류 상태로부터의 복구 방법	개발문서 검토

8.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-650 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

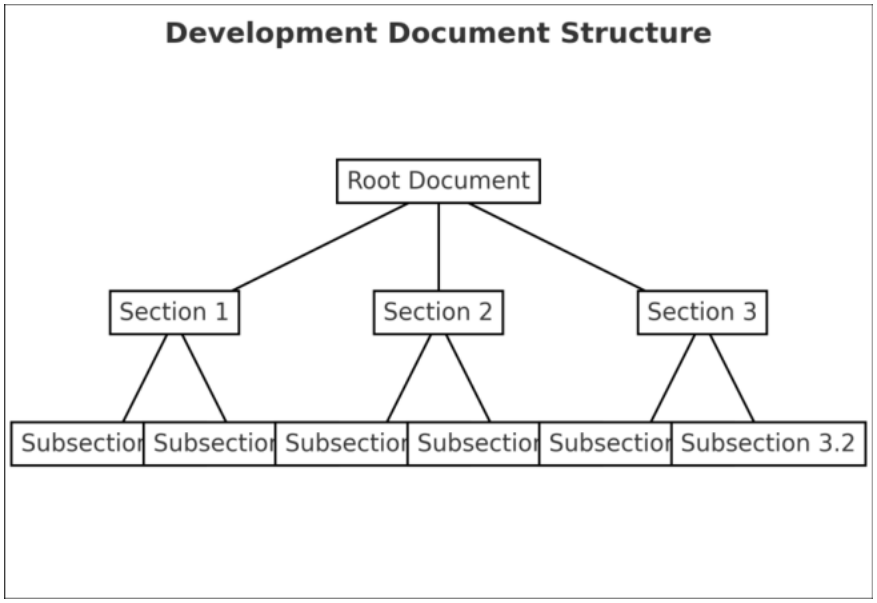


Figure 3-487 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-651 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

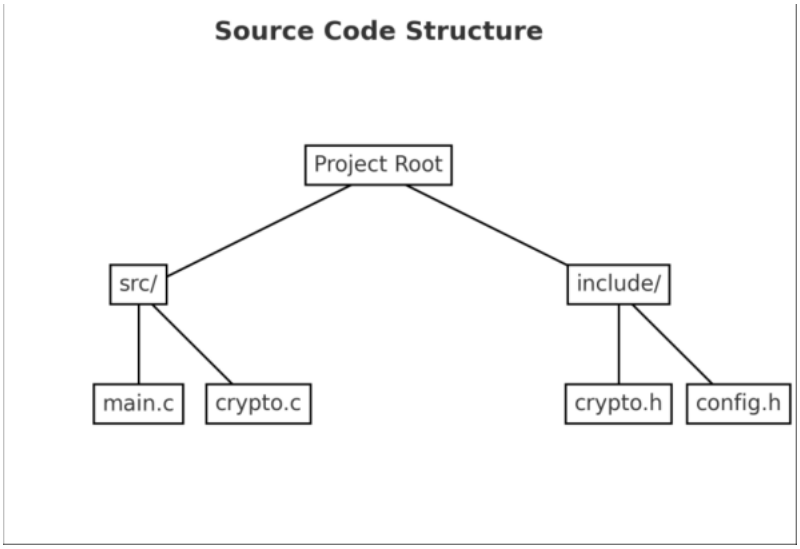


Figure 3-488 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-652 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

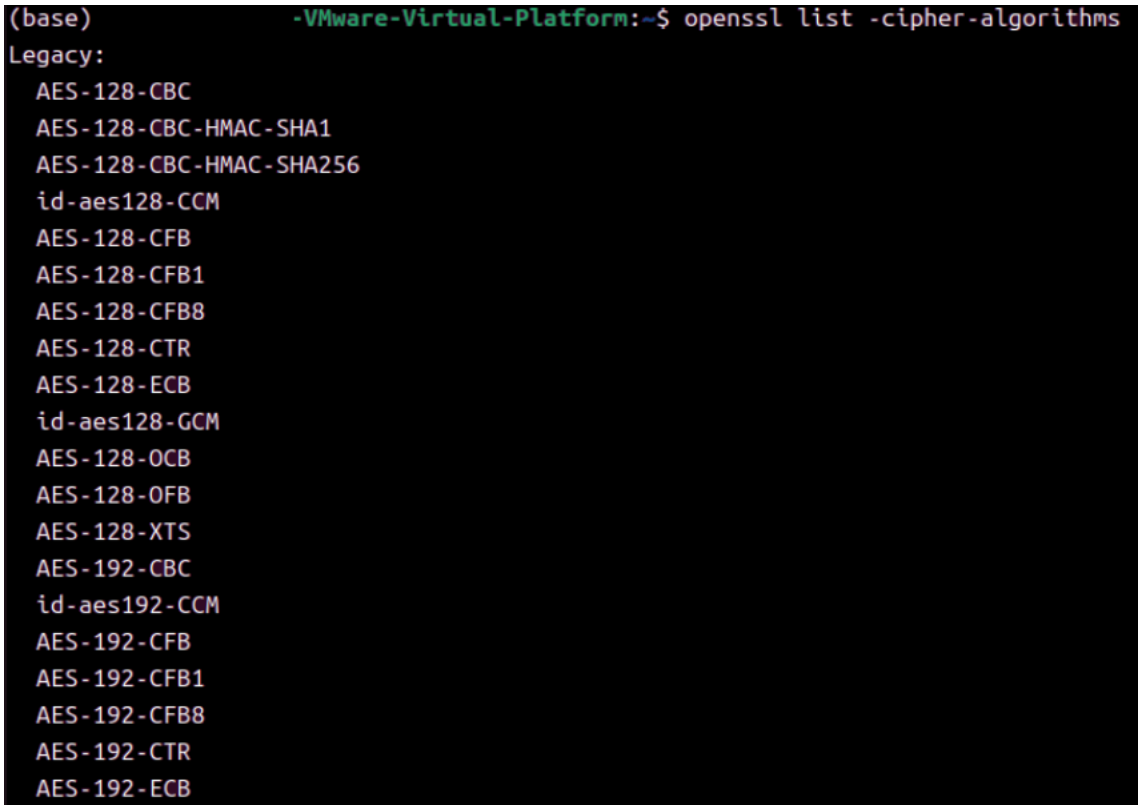


Figure 3-489 그림 제목

8.21.3 판정근거

Table 3-653 TE11.11.01 시험결과 판정근거

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

8.21.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.22 TE11.15.01

8.22.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.15.01	소프트웨어나 펌웨어를 포함하는 암호모듈 개발환경 정보 명세화 개발문서 검토	개발문서 검토

8.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-654 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

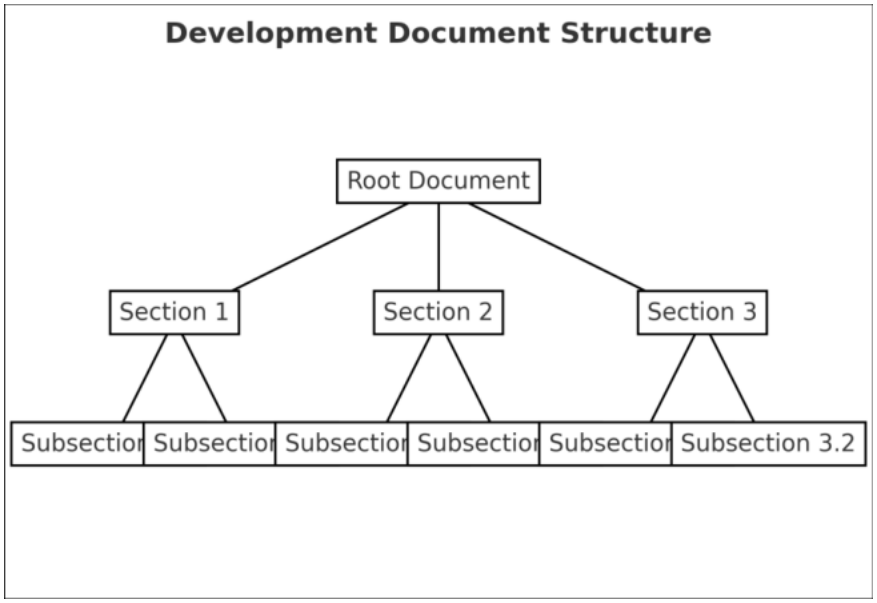


Figure 3-490 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-655 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

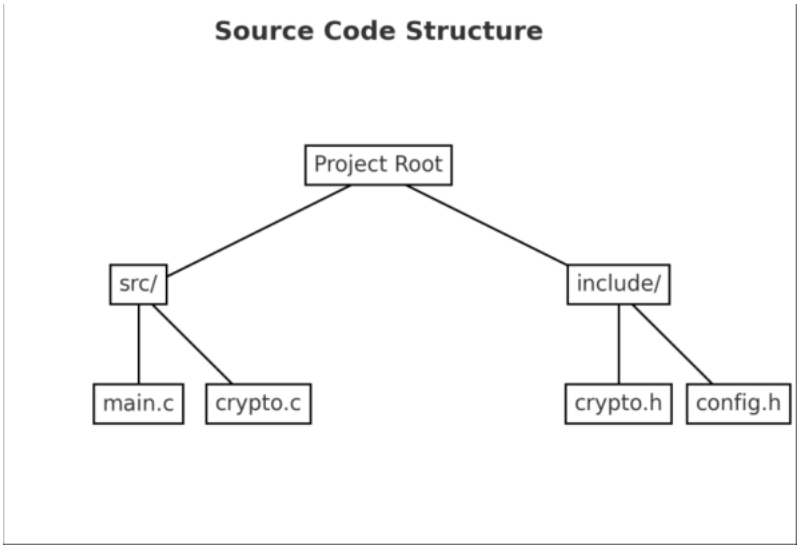


Figure 3-491 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-656 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

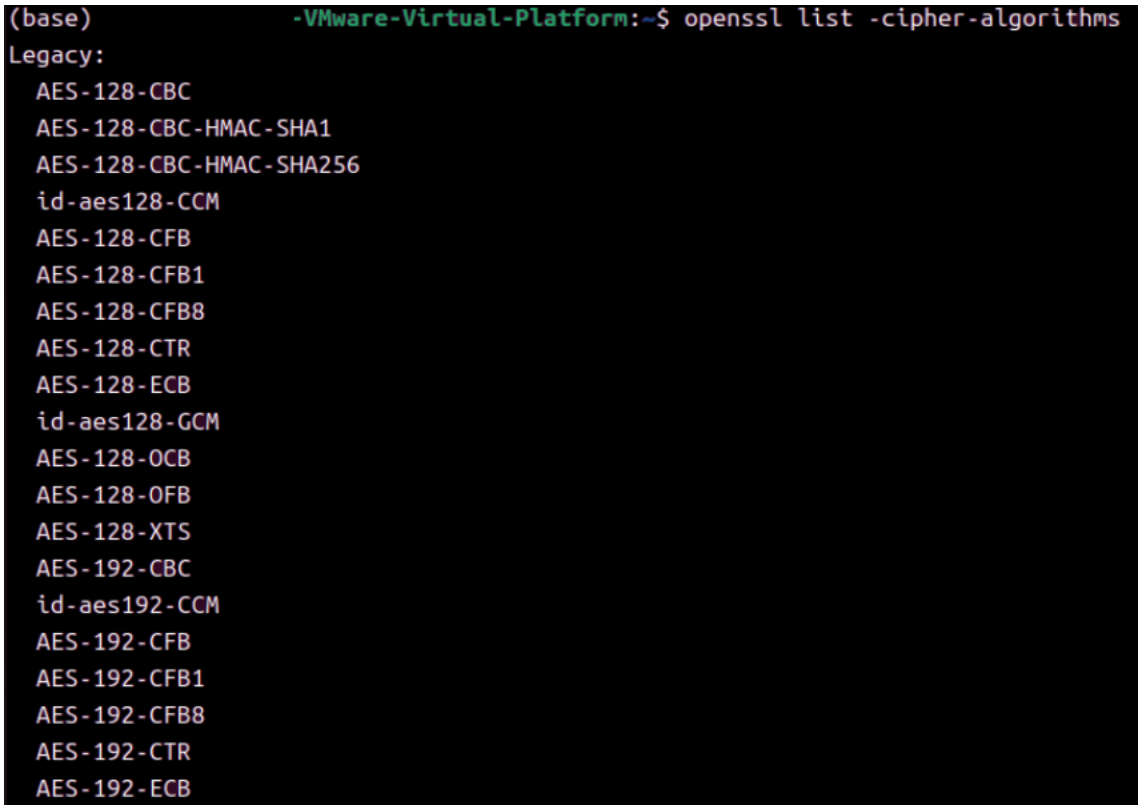


Figure 3-492 그림 제목

8.22.3 판정근거

Table 3-657 TE11.15.01 시험결과 판정근거

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

8.22.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.23 TE11.15.02

8.23.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.15.02	암호모듈 개발환경에 대한 항목 별 형상관리 시스템을 이용한 관리	개발문서 검토

8.23.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-658 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

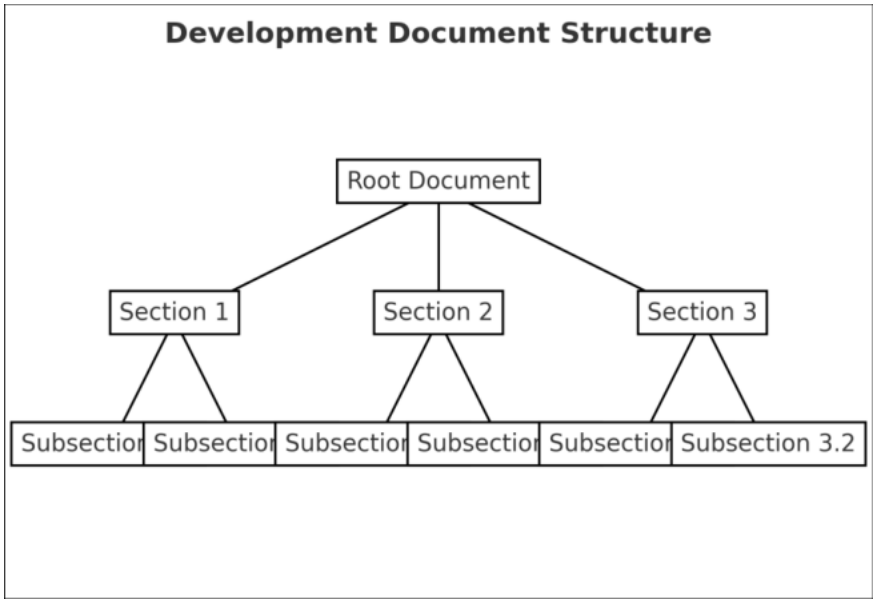


Figure 3-493 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-659 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

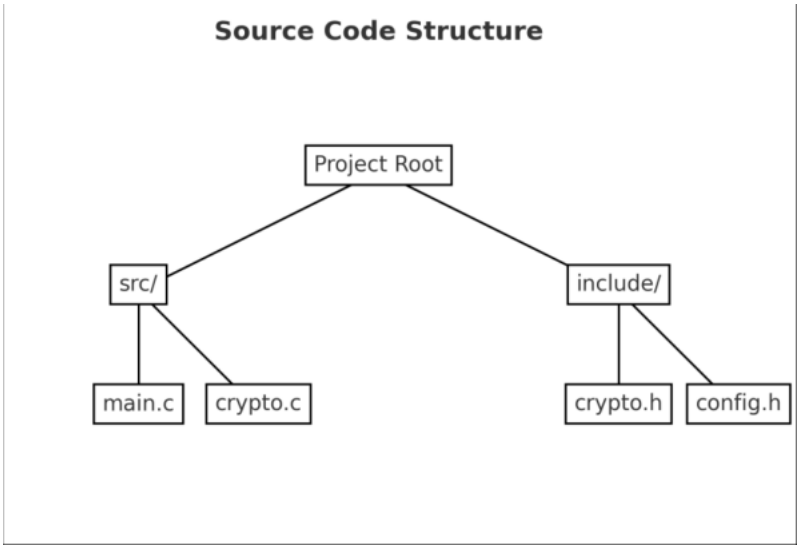


Figure 3-494 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-660 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

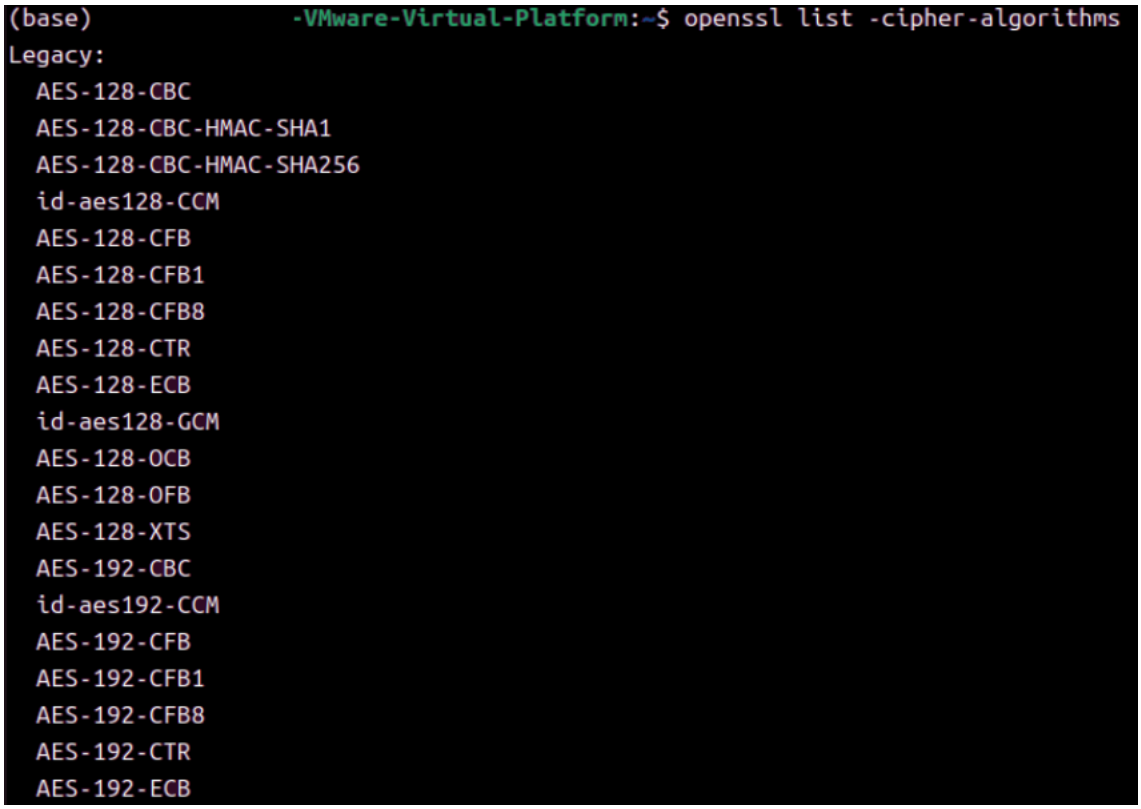


Figure 3-495 그림 제목

8.23.3 판정근거

Table 3-661 TE11.15.02 시험결과 판정근거

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

8.23.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.24 TE11.11.21

8.24.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.11.21	암호모듈 개발도구 (예 : 컴파일러 등) 서술	개발문서 검토

8.24.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-662 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

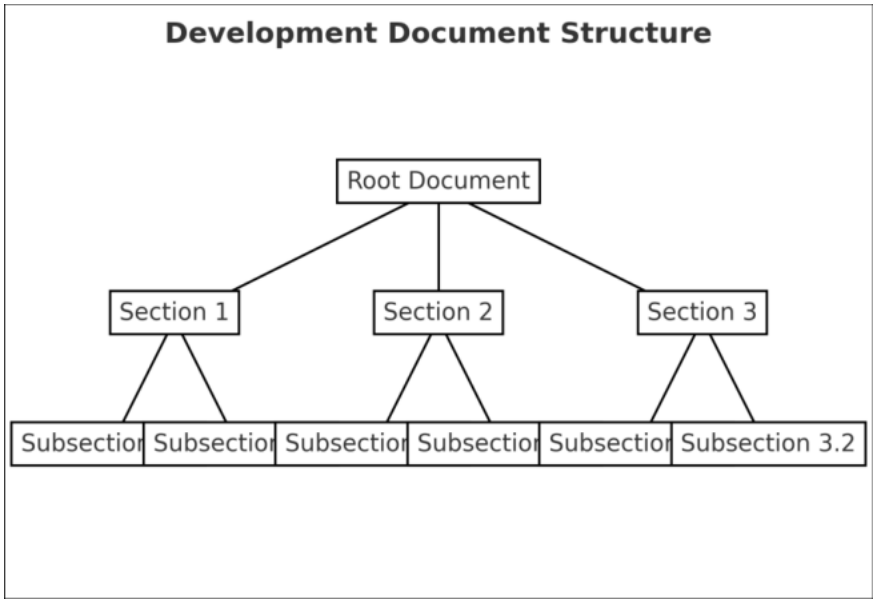


Figure 3-496 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-663 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

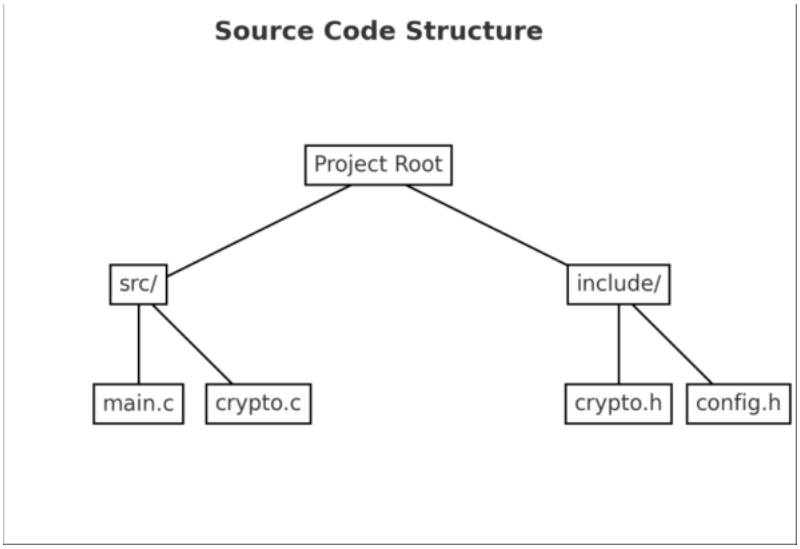


Figure 3-497 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-664 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

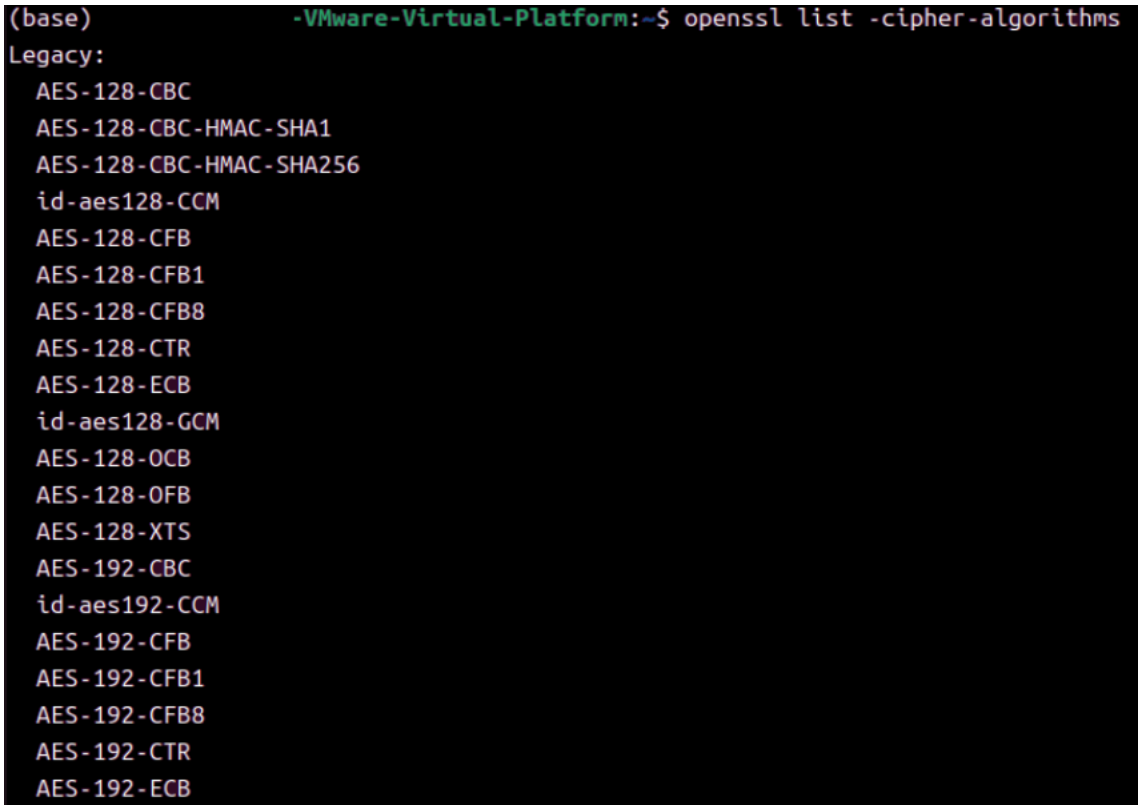


Figure 3-498 그림 제목

8.24.3 판정근거

Table 3-665 TE11.11.21 시험결과 판정근거

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

8.24.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.25 TE11.16.01

8.25.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.16.01	소스코드 목록 확인	개발문서 검토 암호모듈 검사

8.25.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-666 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

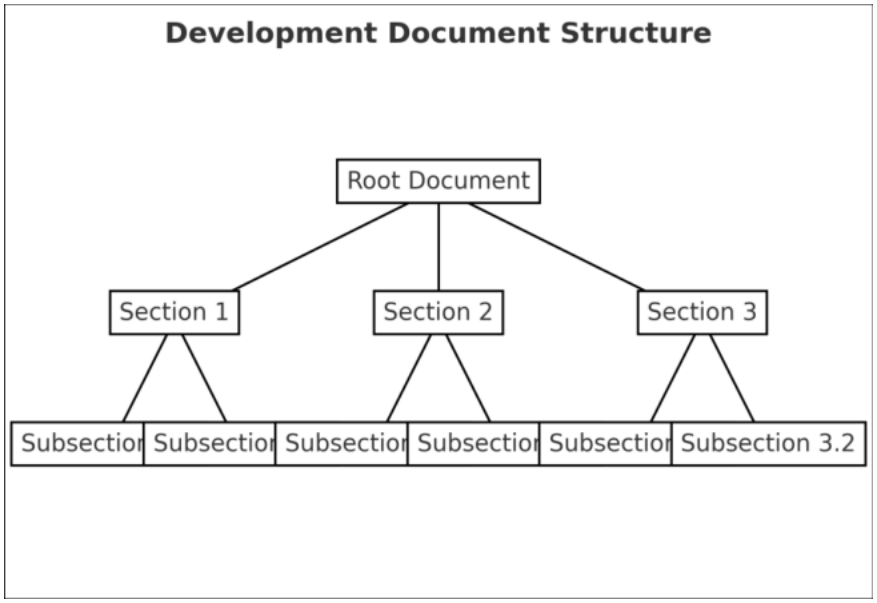


Figure 3-499 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-667 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

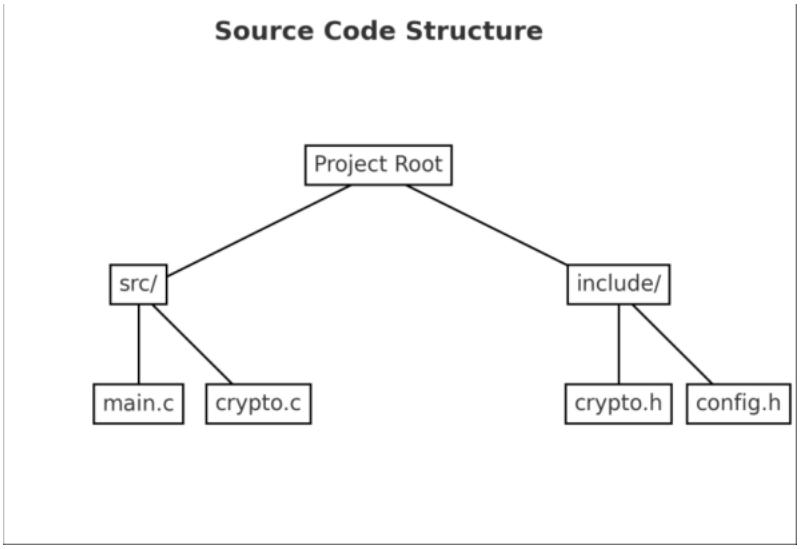


Figure 3-500 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-668 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

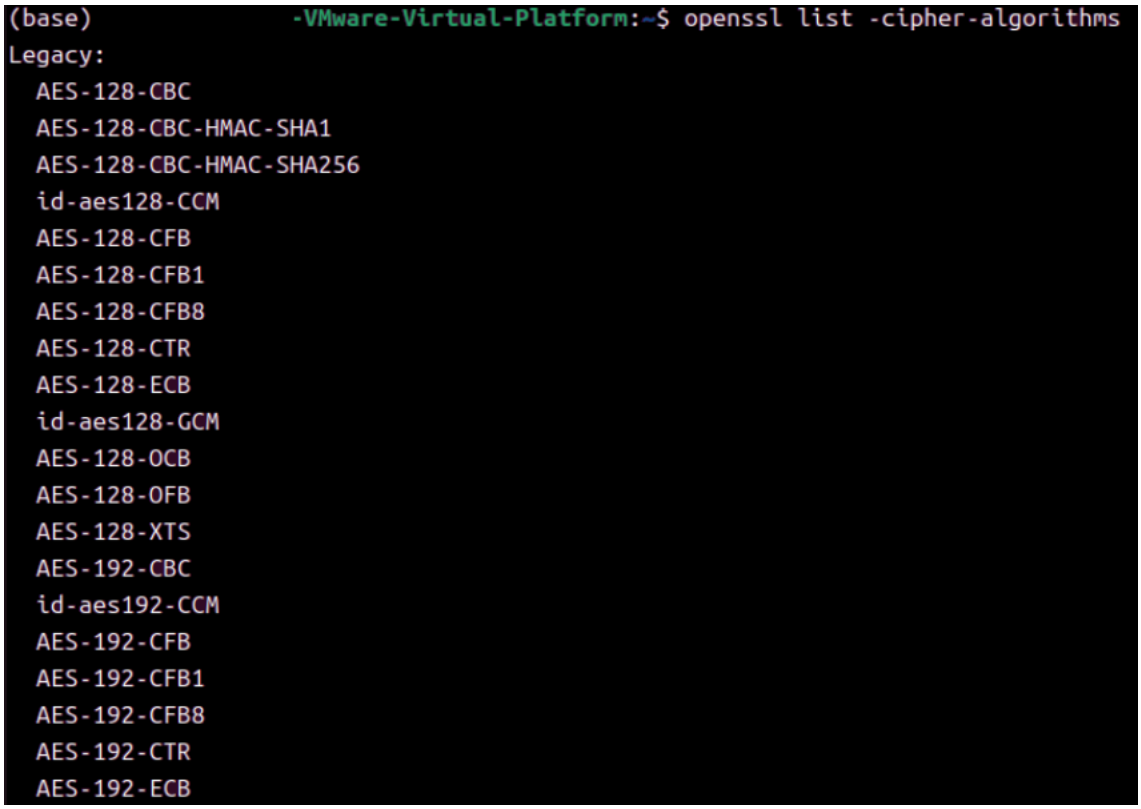


Figure 3-501 그림 제목

8.25.3 판정근거

Table 3-669 TE11.16.01 시험결과 판정근거

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

8.25.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.26 TE11.19.01

8.26.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.19.01	소프트웨어 무결성 인증 기법의 결과 코드 생성 및 관리 방법과 결과 코드 사용방법	개발문서 검토

8.26.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-670 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

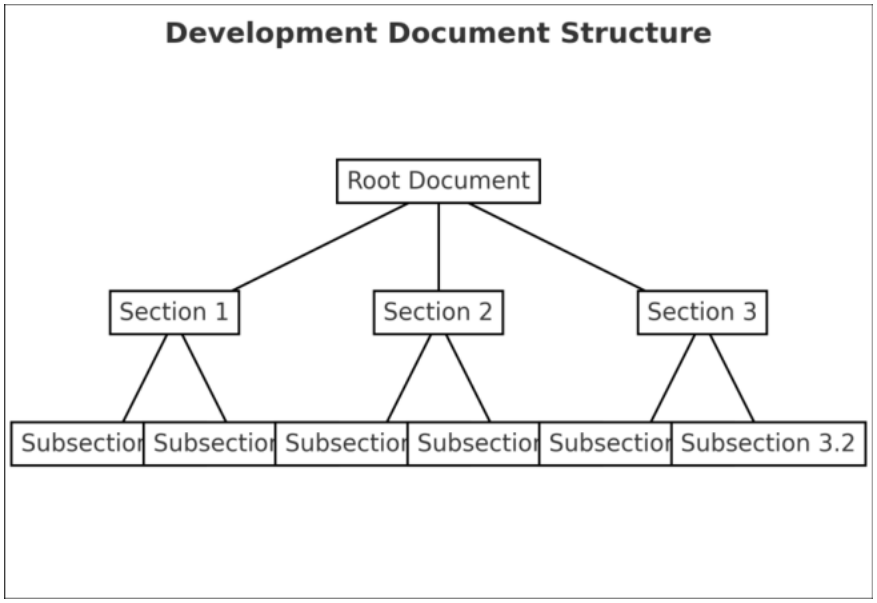


Figure 3-502 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-671 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

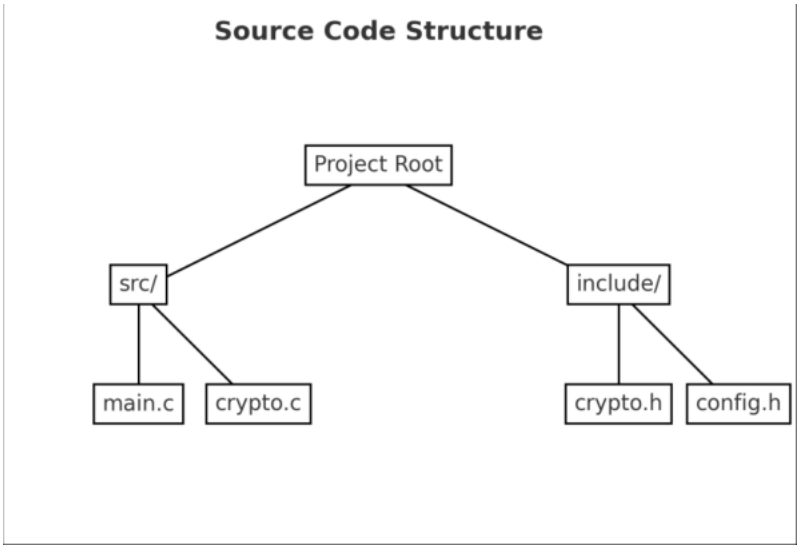


Figure 3-503 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-672 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

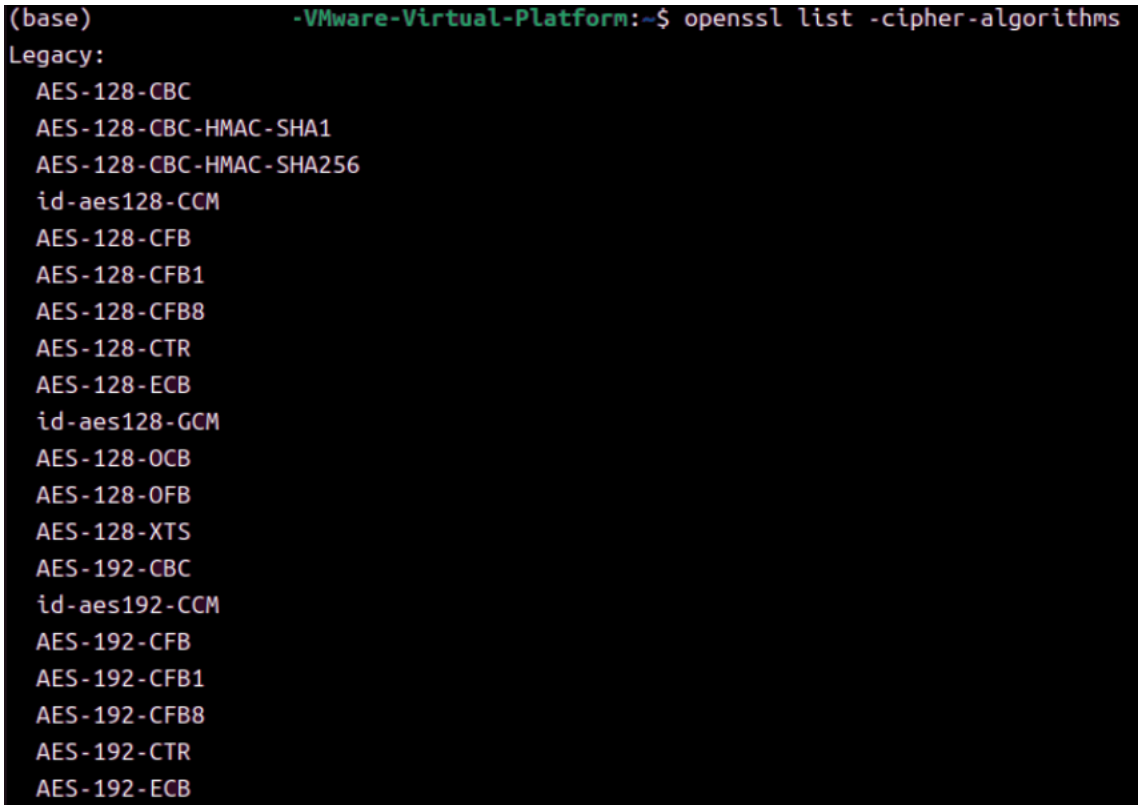


Figure 3-504 그림 제목

8.26.3 판정근거

Table 3-673 TE11.19.01 시험결과 판정근거

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

8.26.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.27 TE11.29.01

8.27.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.11.29	개발업체 자체 기능시험 항목 및 결과	개발문서 검토

8.27.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-674 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

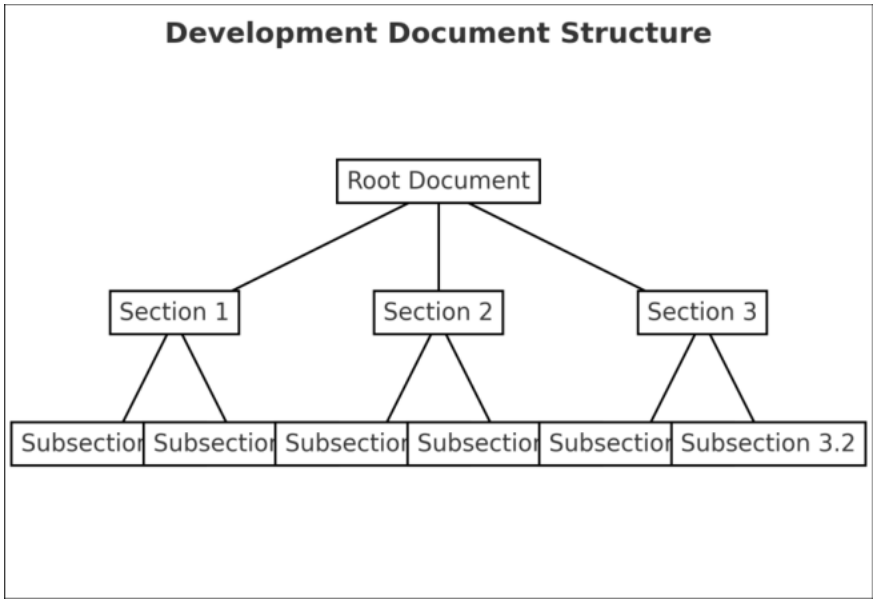


Figure 3-505 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-675 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

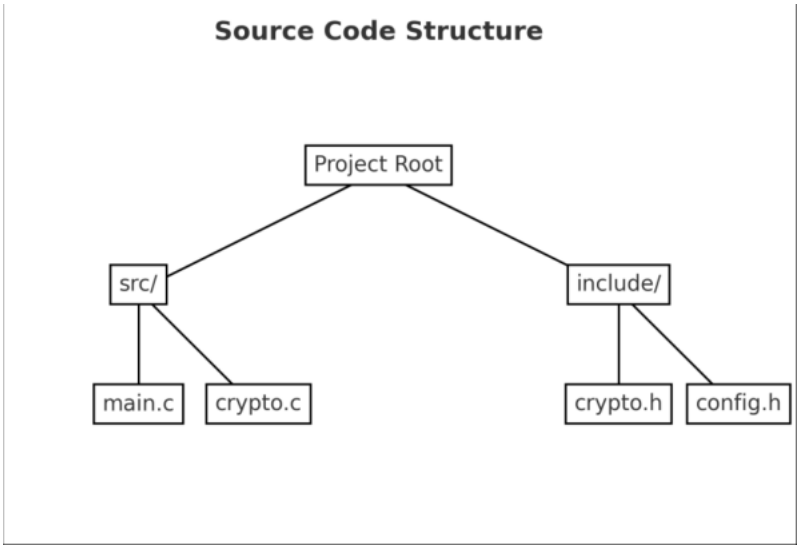


Figure 3-506 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-676 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

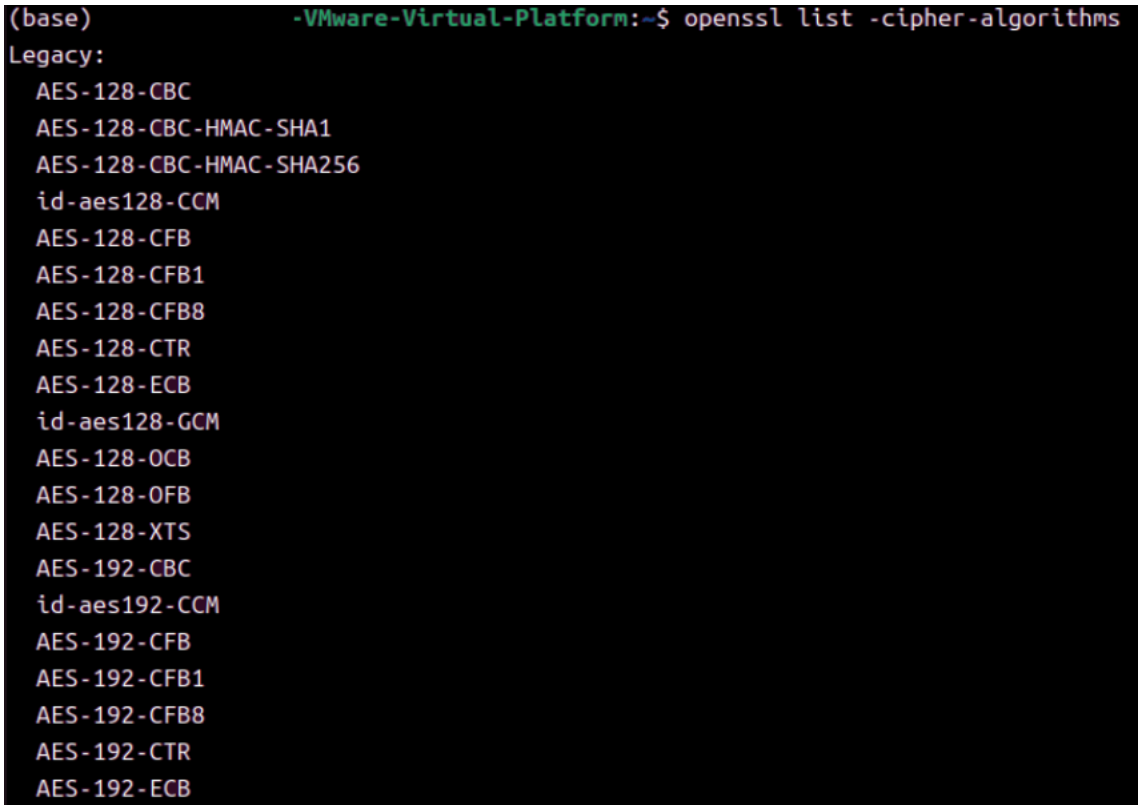


Figure 3-507 그림 제목

8.27.3 판정근거

Table 3-677 TE11.29.01 시험결과 판정근거

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

8.27.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.28 TE11.30.01

8.28.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.30.01	소프트웨어 구성요소의 소스코드에 대한 자동화 보안진단도구 자체 적용 결과	개발문서 검토

8.28.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-678 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

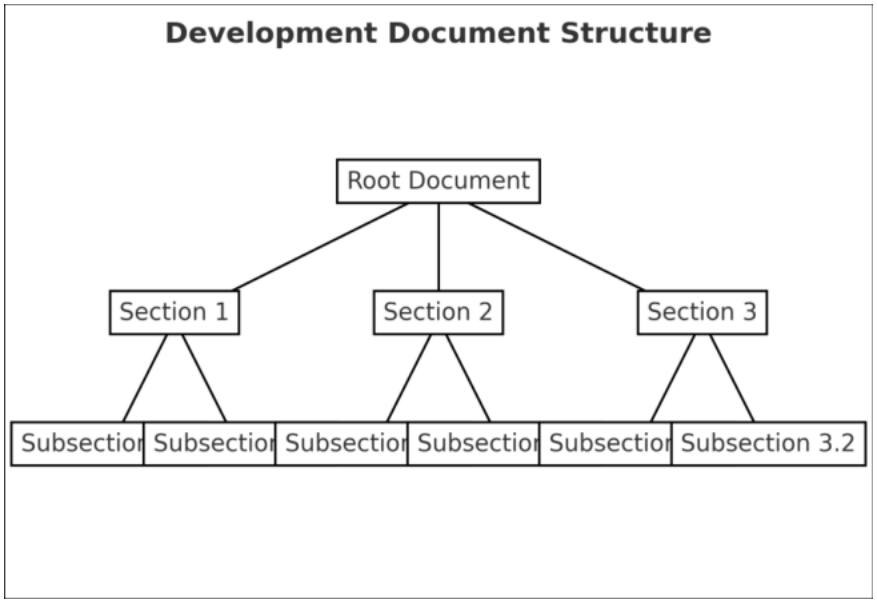


Figure 3-508 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-679 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

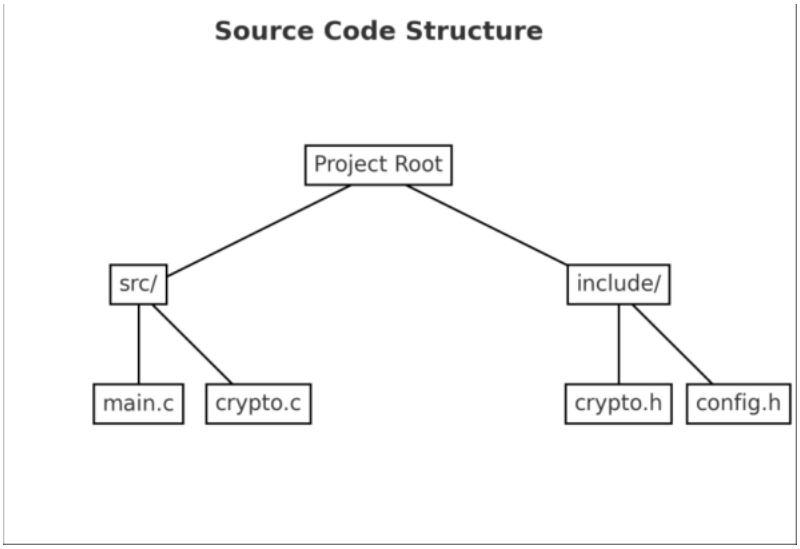


Figure 3-509 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-680 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

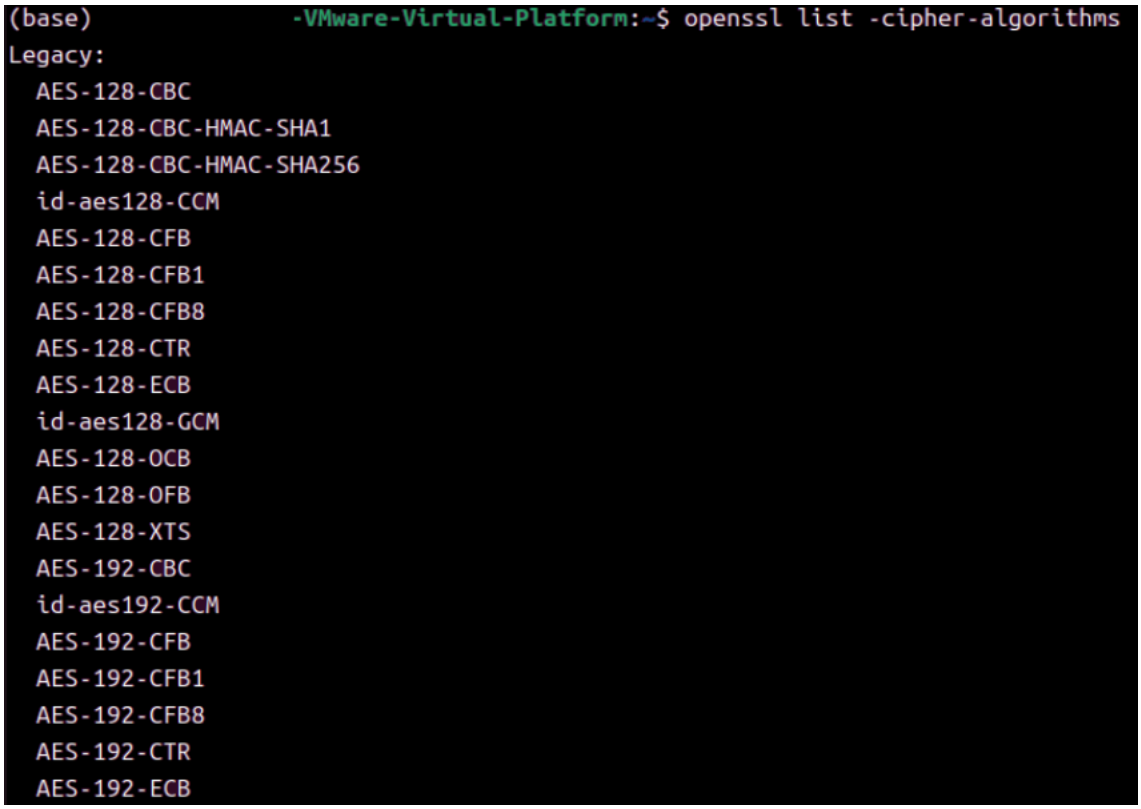


Figure 3-510 그림 제목

8.28.3 판정근거

Table 3-681 TE11.30.01 시험결과 판정근거

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

8.28.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.29 TE11.01.01

8.29.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.01.01	암호모듈의 안전한 설치 , 초기화 및 시동 절차 명세	개발문서 검토

8.29.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-682 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

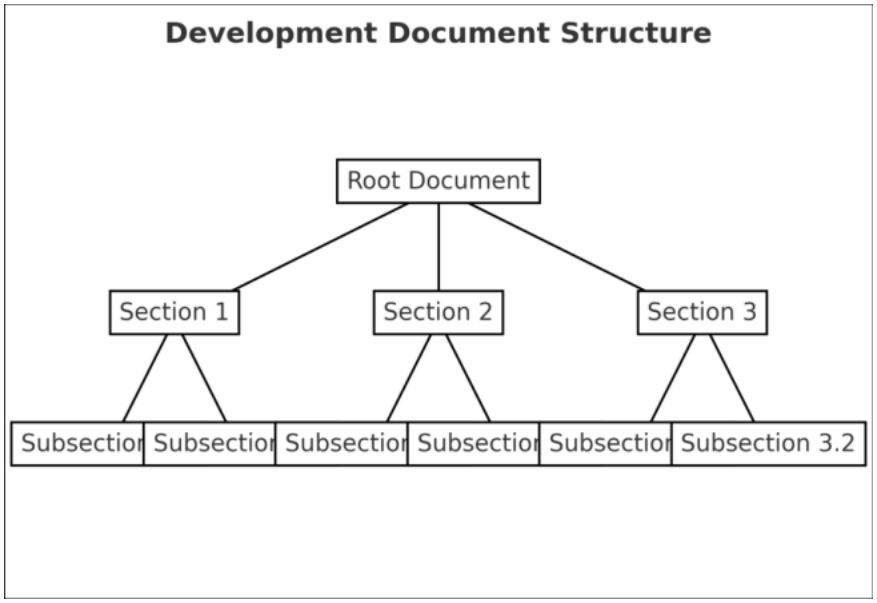


Figure 3-511 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-683 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

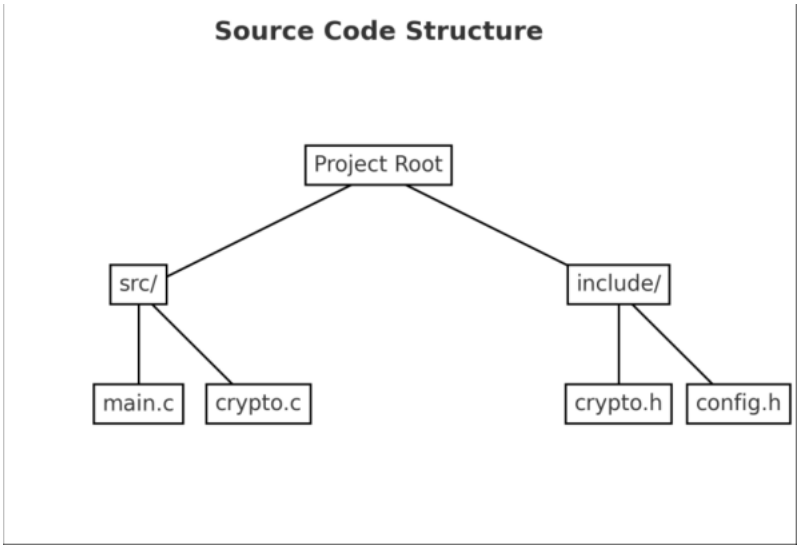


Figure 3-512 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-684 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

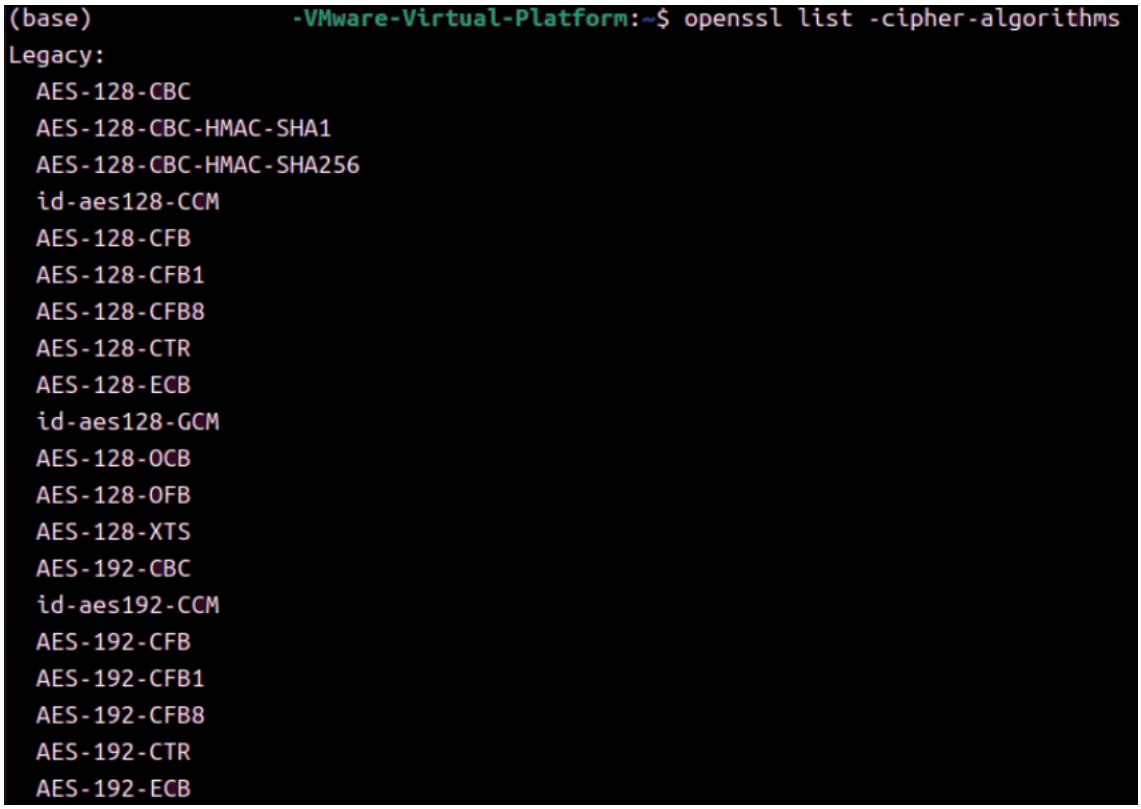


Figure 3-513 그림 제목

8.29.3 판정근거

Table 3-685 TE11.32.01 시험결과 판정근거

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

8.29.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.30 TE11.32.02

8.30.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.32.02	안전한 설치 , 초기화 , 시동 절차에 따른 동작 일치	암호모듈 검사

8.30.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-686 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

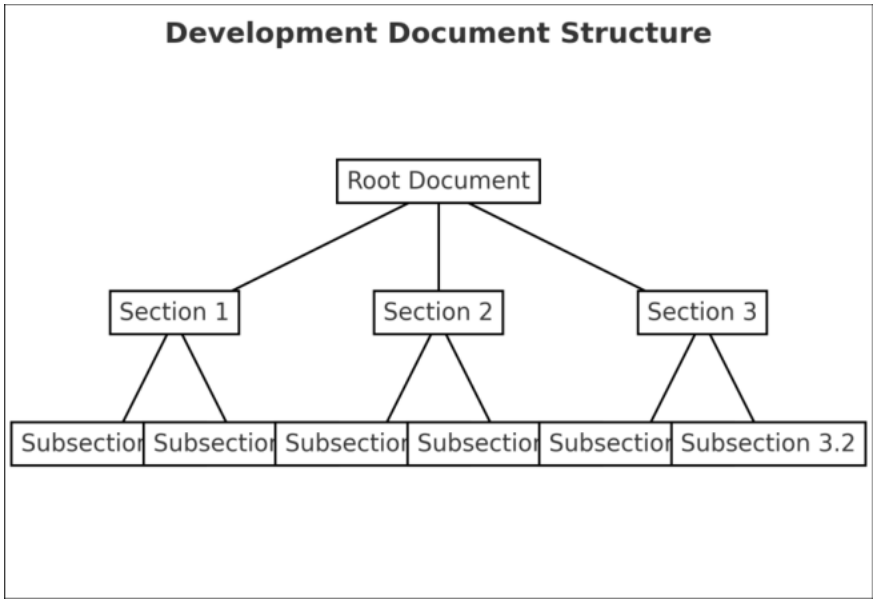


Figure 3-514 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-687 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

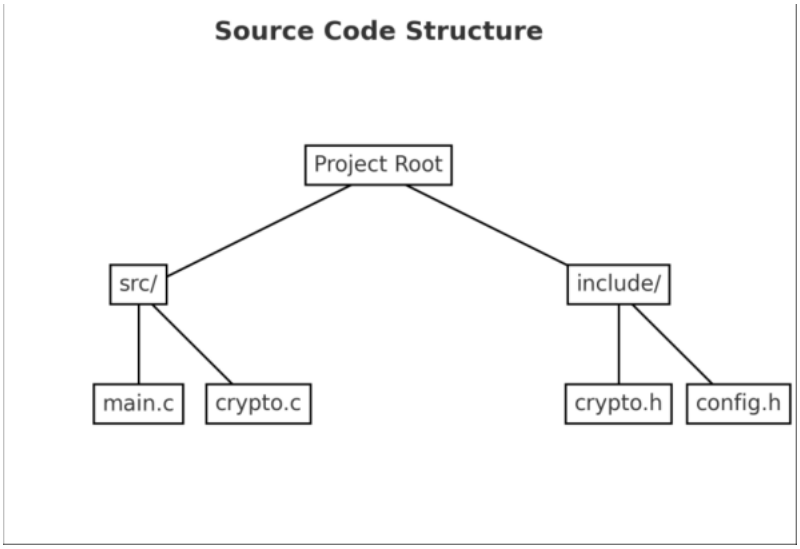


Figure 3-515 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-688 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

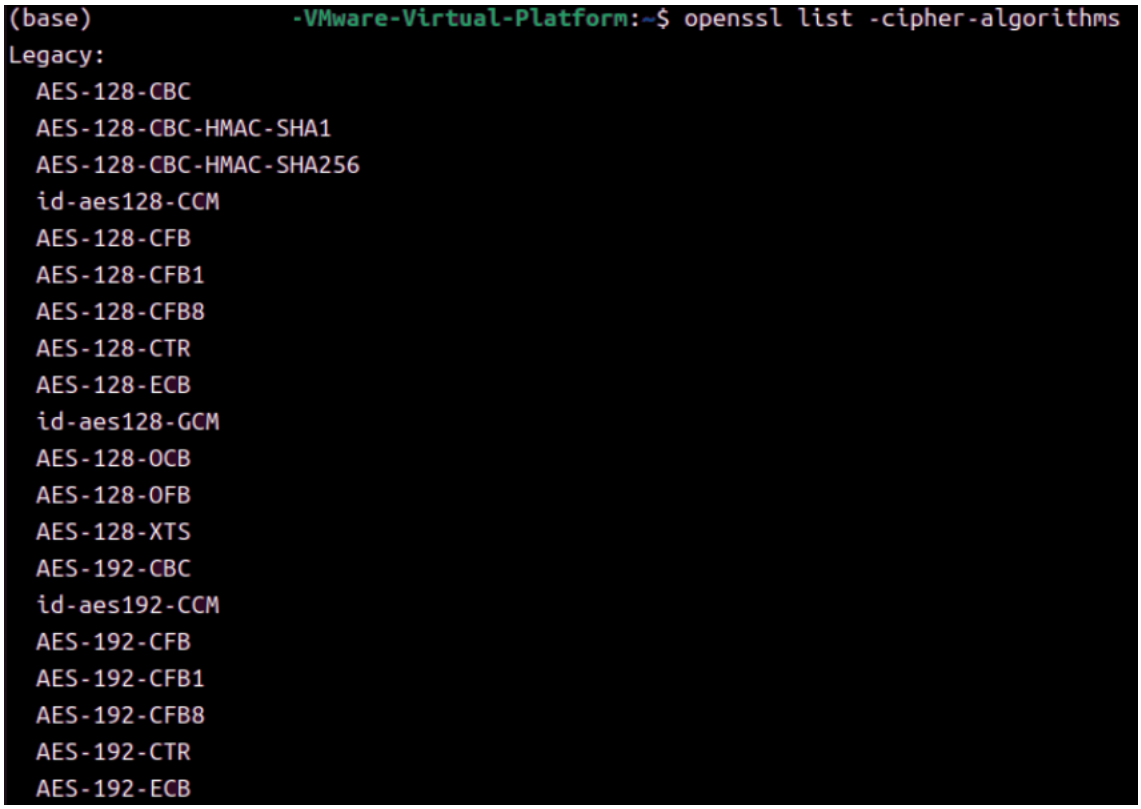


Figure 3-516 그림 제목

8.30.3 판정근거

Table 3-689 TE11.32.02 시험결과 판정근거

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

8.30.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.31 TE11.36.01

8.31.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.36.01	암호모듈의 안전한 소거 절차 명세화	개발문서 검토

8.31.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-690 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

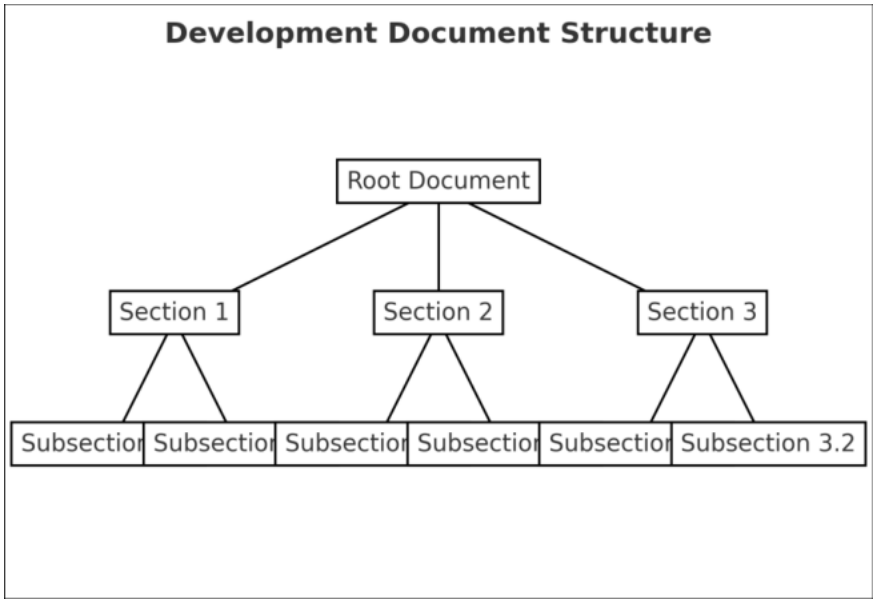


Figure 3-517 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-691 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

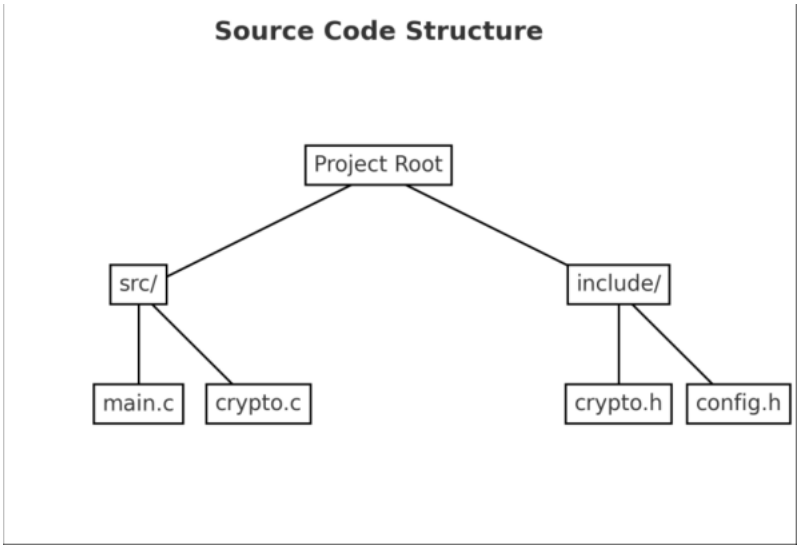


Figure 3-518 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-692 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

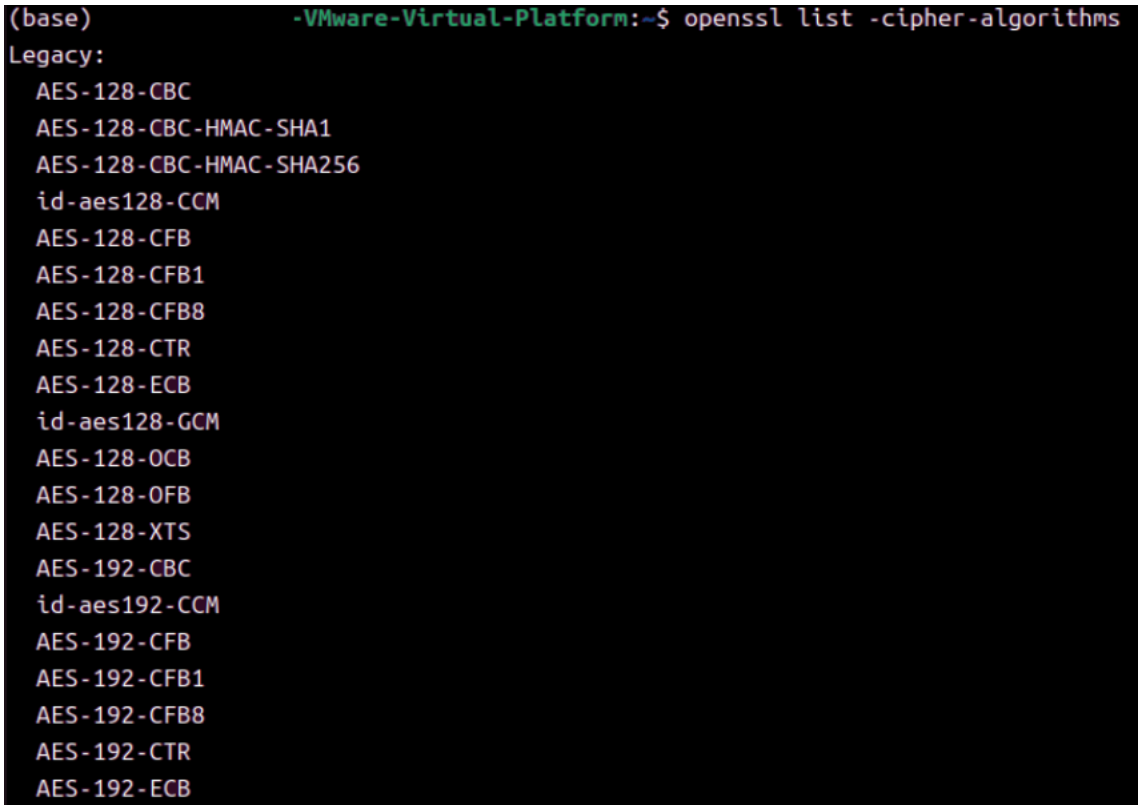


Figure 3-519 그림 제목

8.31.3 판정근거

Table 3-693 TE11.36.01 시험결과 판정근거

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

8.31.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.32 TE11.38.01

8.32.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.38.01	관리자 안내서	개발문서 검토

8.32.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-694 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

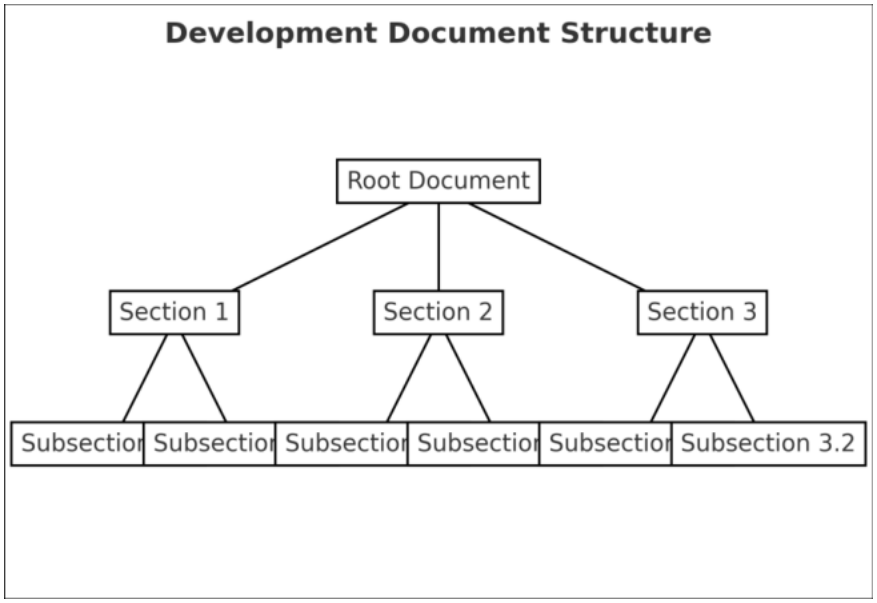


Figure 3-520 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-695 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

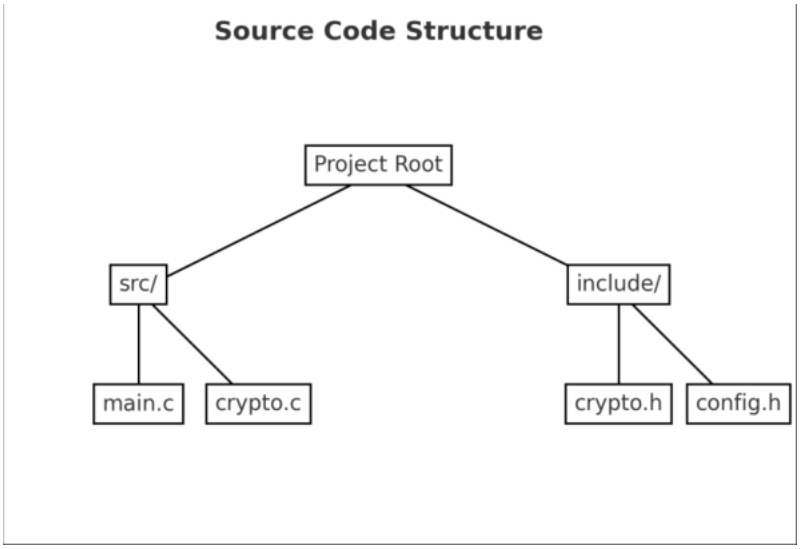


Figure 3-521 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-696 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

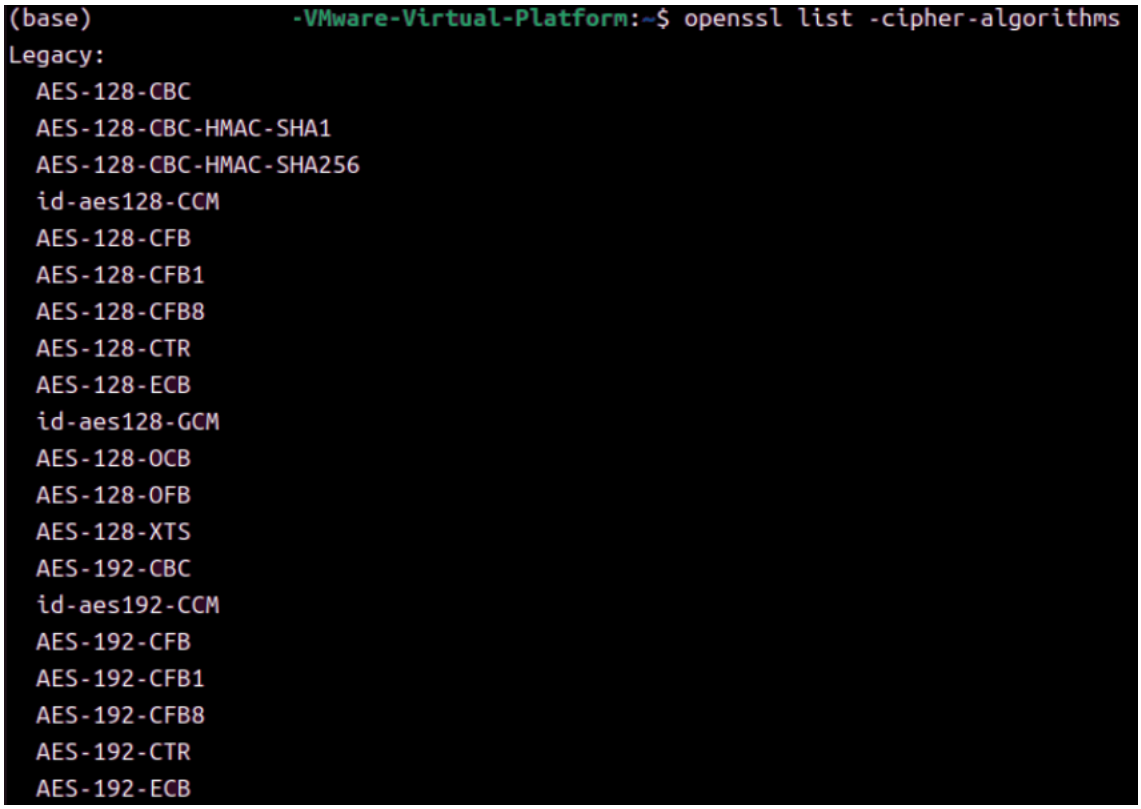


Figure 3-522 그림 제목

8.32.3 판정근거

Table 3-697 TE11.38.01 시험결과 판정근거

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

8.32.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

8.33 TE11.39.01

8.33.1 시험 요구사항

TE	주요 확인사항	확인방법
TE11.39.01	비관리자 안내서	개발문서 검토

8.33.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-698 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

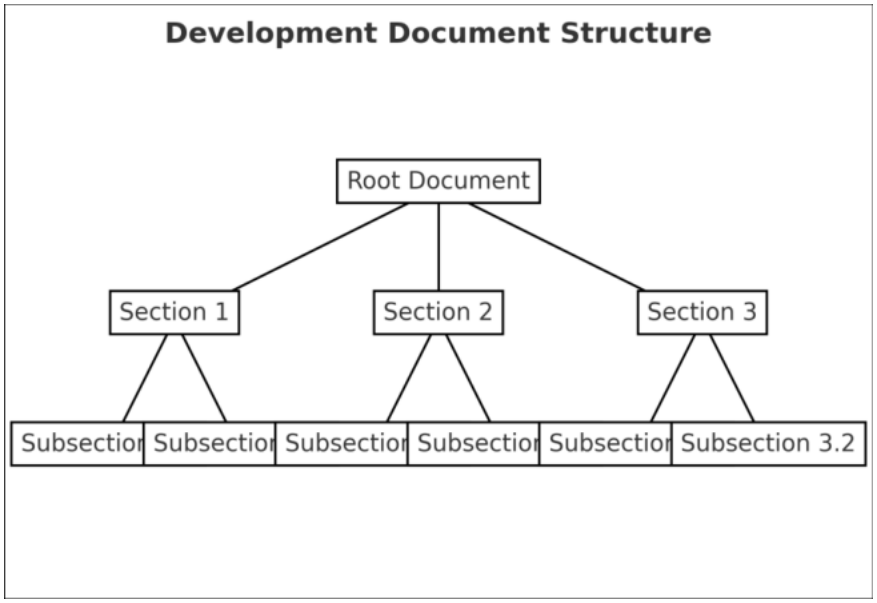


Figure 3-523 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-699 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

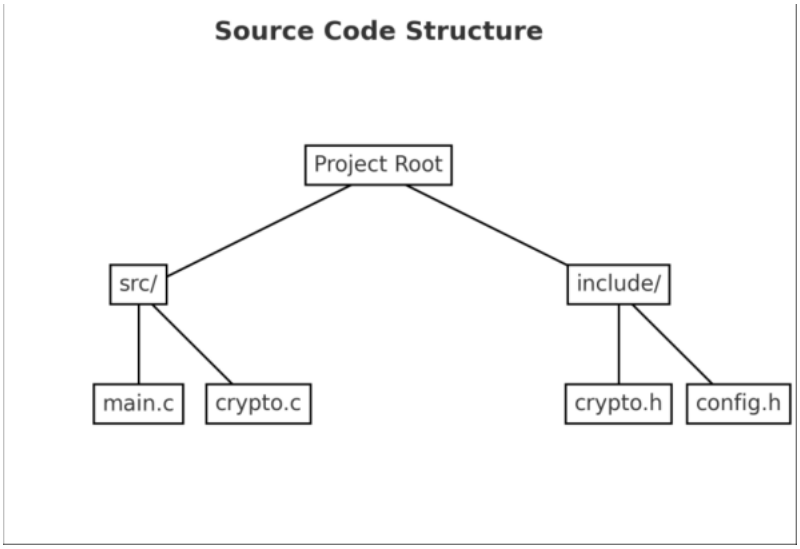


Figure 3-524 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-700 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

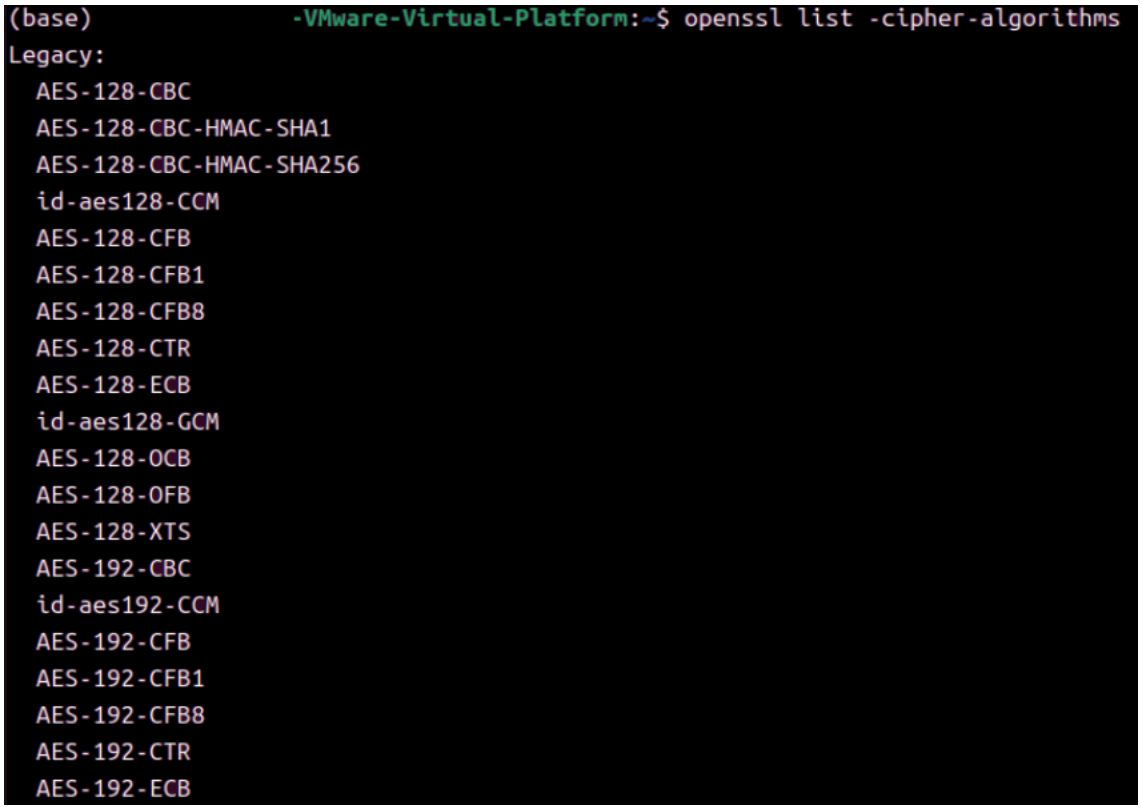


Figure 3-525 그림 제목

8.33.3 판정근거

Table 3-701 TE11.39.01 시험결과 판정근거

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

8.33.4 판정결과

판정 : <“ 통과 ” 또는 “ 실패 ”>

9. 기타 공격에 대한 대응 (AS12)

□ 하나 이상의 암호모듈의 특정 공격에 대해 완화시키는 방법을 제시하는 경우에 한해서 암호모듈이 구현하고 있는 방법을 확인한다 .

9.1 AS12 시험항목

AS	TE	확인사항
AS12.01	1	개발문서의 최소 문서 요구사항 만족 여부
AS12.02	1	특정 공격에 대한 대응

9.2 TE12.01.01

9.2.1 시험 요구사항

TE	주요 확인사항	확인방법
TE12.01.01	개발문서의 최소 문서 요구사항	개발문서 검토

9.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-702 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

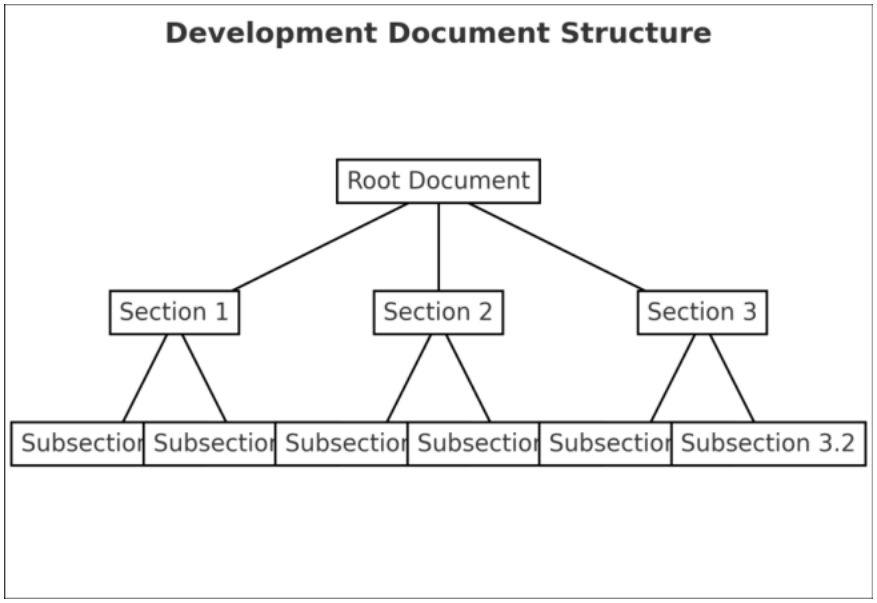


Figure 3-526 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-703 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

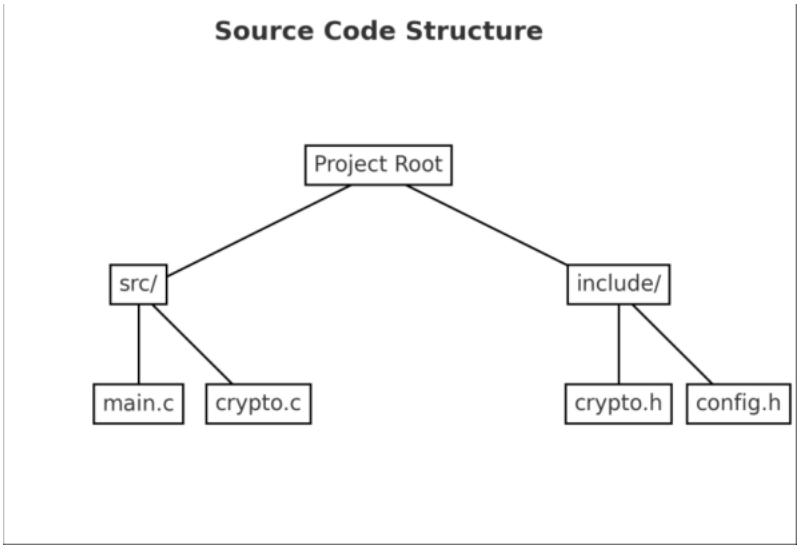


Figure 3-527 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-704 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

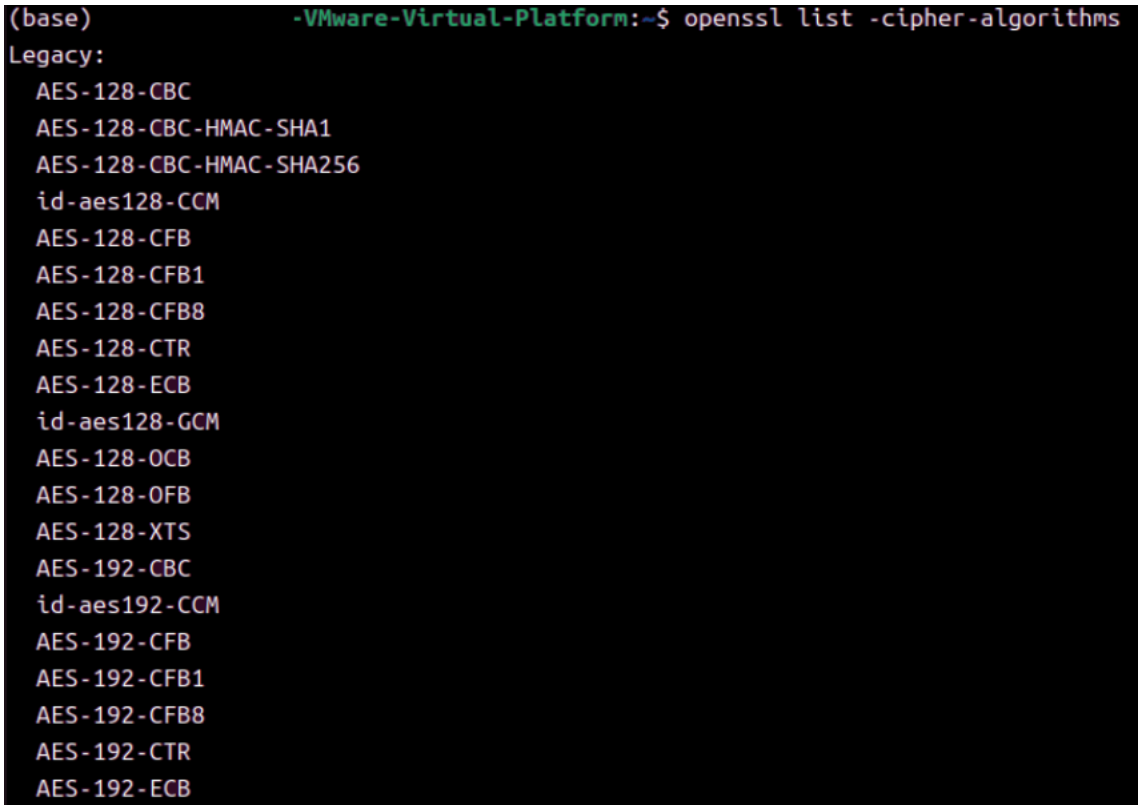


Figure 3-528 그림 제목

9.2.3 판정근거

Table 3-705 TE12.01.01 시험결과 판정근거

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

9.2.4 판정결과

☒ 판정 : <“ 통과 ” 또는 “ 실패 ”>

9.3 TE12.01.02

9.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE12.01.02	특정 공격에 대한 대응 방법 명세화	개발문서 검토

9.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

☒ < 개발문서명 >

나) 개발문서 검토내용

☒ < 개발문서 검토내용 설명 >

다) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-706 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

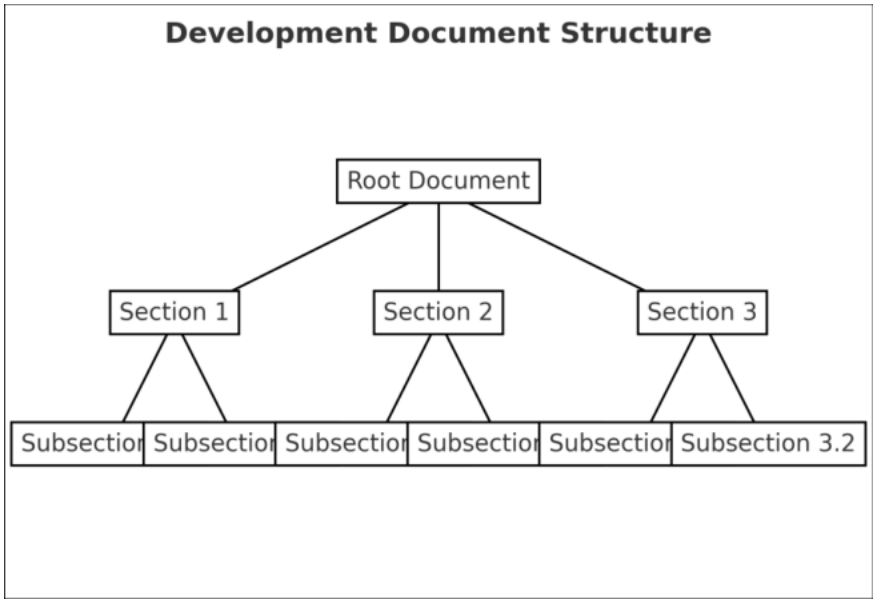


Figure 3-529 그림 제목

2) 소스코드 검토

라) 소스코드명

☒ < 소스코드명 >

마) 소스코드 검토내용

☒ < 개발문서 검토내용 설명 >

바) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-707 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

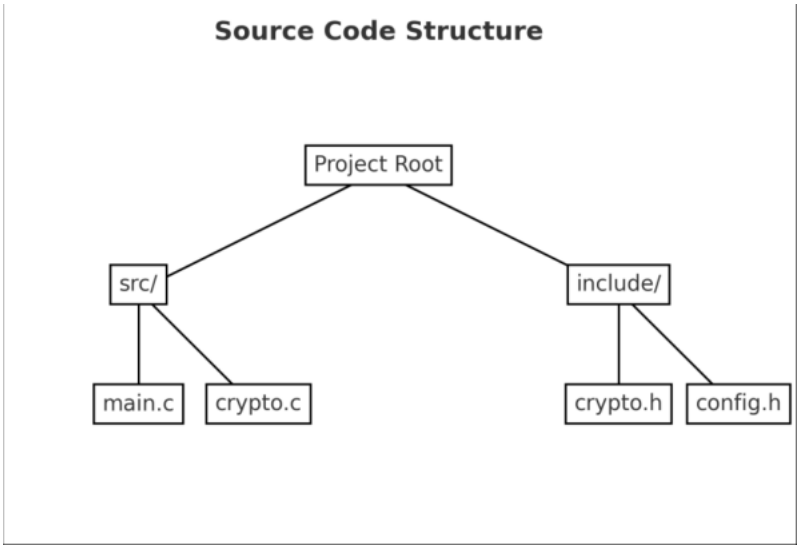


Figure 3-530 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

☒ < 암호모듈 시험명칭 >

아) 암호모듈 시험내용

☒ < 암호모듈 시험내용 설명 >

자) 증빙자료

☒ < 증빙자료 내용 설명 >

Table 3-708 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

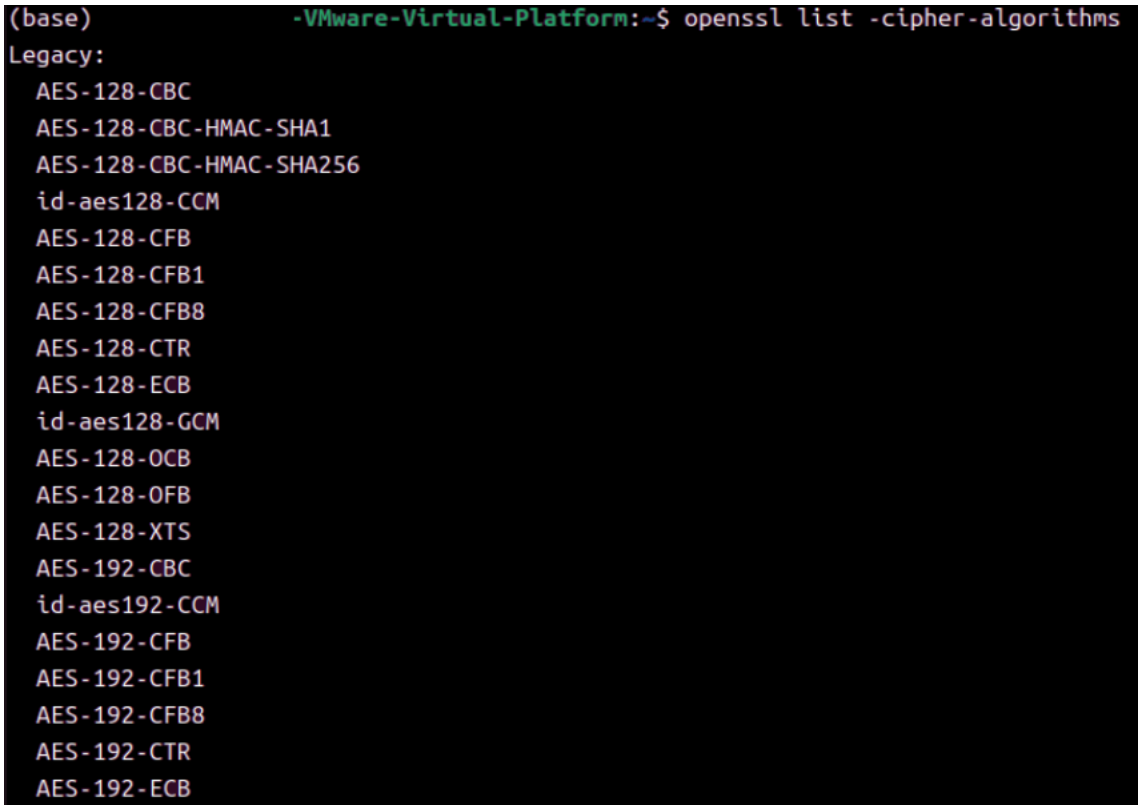


Figure 3-531 그림 제목

9.3.3 판정근거

Table 3-709 TE12.01.02 시험결과 판정근거

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

9.3.4 판정결과

☒ 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