ABC V1.0

시험결과보고서

V2.00

2025 년 00 월 00 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	2024.09.25.
V1.00	기술책임자 검토 완료	2024.09.25.
V1.90	검증기관 검토의견 반영	2024.12.18.
V2.00	기술책임자 검토 완료	2025.02.24.

목 차

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 = 128비트 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 = 128비트
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 V1.0은 보안수준 1을 만족하도록 설계된 소프트웨어 라이브러리 형태 암호모듈로 <KS X ISO/IEC 24759:2015>의 적용 가능한 시험항목에 대한 요구사항을 **만족**한다.

<table>
<tr><td>암호모듈 명</td><td>ABC V1.0</td><td>모듈 형태</td><td>S/W(라이브러리)</td></tr>
<tr><td>개발사 명</td><td>개발업체(주)</td><td>적용 기준</td><td>KS X ISO/IEC 19790:2015
KS X ISO/IEC 24759:2015</td></tr>
<tr><td>보안수준</td><td colspan="3">• 전체 수준: 보안수준 1
• 시험영역별 보안수준
<table>
<tr><th>시험영역</th><th>보안수준</th></tr>
<tr><td>암호모듈 명세</td><td>1</td></tr>
<tr><td>암호모듈 인터페이스</td><td>1</td></tr>
<tr><td>역할, 서비스 및 인증</td><td>1</td></tr>
<tr><td>소프트웨어/펌웨어 보안</td><td>1</td></tr>
<tr><td>운영환경</td><td>1</td></tr>
<tr><td>물리적 보안</td><td>해당사항 없음</td></tr>
<tr><td>비침투 보안</td><td>해당사항 없음</td></tr>
<tr><td>중요 보안매개변수 관리</td><td>1</td></tr>
<tr><td>자가시험</td><td>1</td></tr>
<tr><td>생명주기 보증</td><td>1</td></tr>
<tr><td>기타 공격에 대한 대응</td><td>1</td></tr>
</table></td></tr>
<tr><td>비고</td><td colspan="3">SSO(Single Sign On) 정보보호제품에 탑재되는 암호모듈 라이브러리</td></tr>
</table>

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 (00종의 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	00일

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	소스코드 & 인터페이스 분석	AS03. 암호모듈 인터페이스 AS05. 소프트웨어/펌웨어 보안 AS09. 중요 보안매개변수 관리 AS10. 자가시험 AS12. 기타 공격에 대한 대응
	- GDB 15.2	중요보안매개 변수 분석	
	- 암호모듈 사전검증 서비스	엔트로피 분석	
	- Code-RAY XG V6.0	소스코드 취약점 분석	
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 정의	개발문서 검토

1.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-1 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

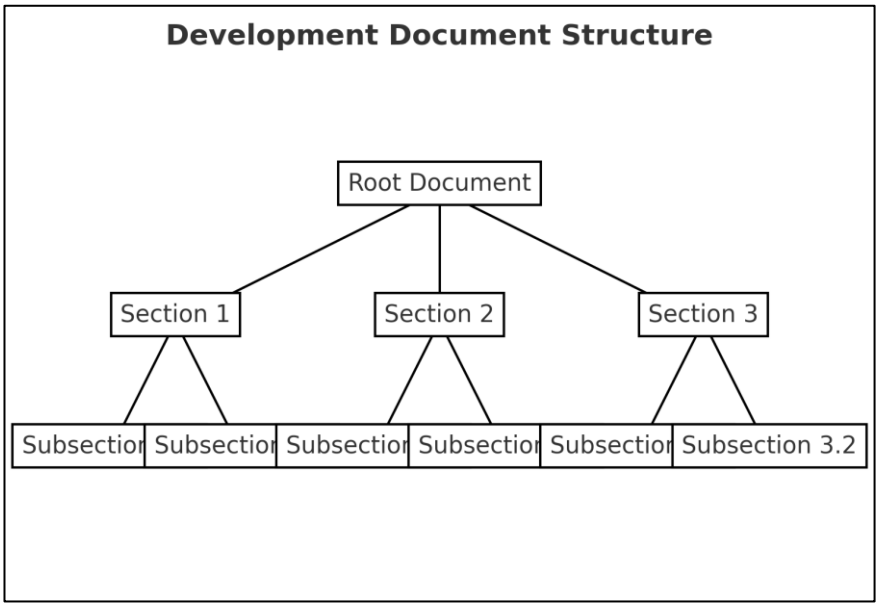

Figure 3-1 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-2 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

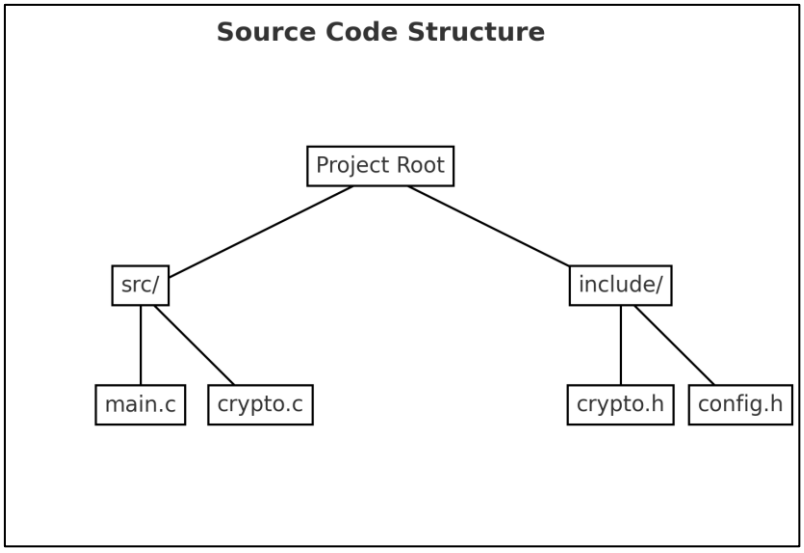

Figure 3-2 그림 제목

3) 암호모듈 시험

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-3 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

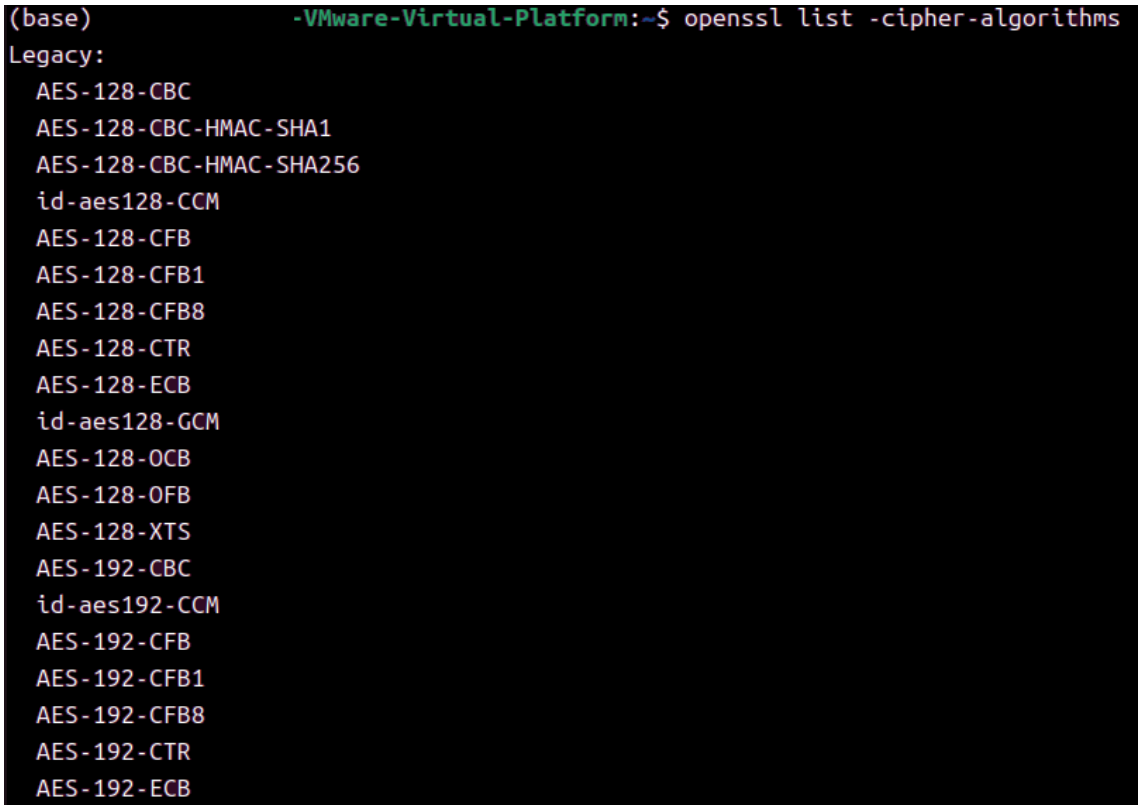

Figure 3-3 그림 제목

1.2.3 판정근거

Table 3-4 TE02.03.01 시험결과 판정 근거

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

1.2.4 판정결과

차) 판정: <“통과” 또는 “실패”>

1.3 TE02.03.02

1.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE02.03.02	구성요소들을 통한 암호모듈의 유형	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			

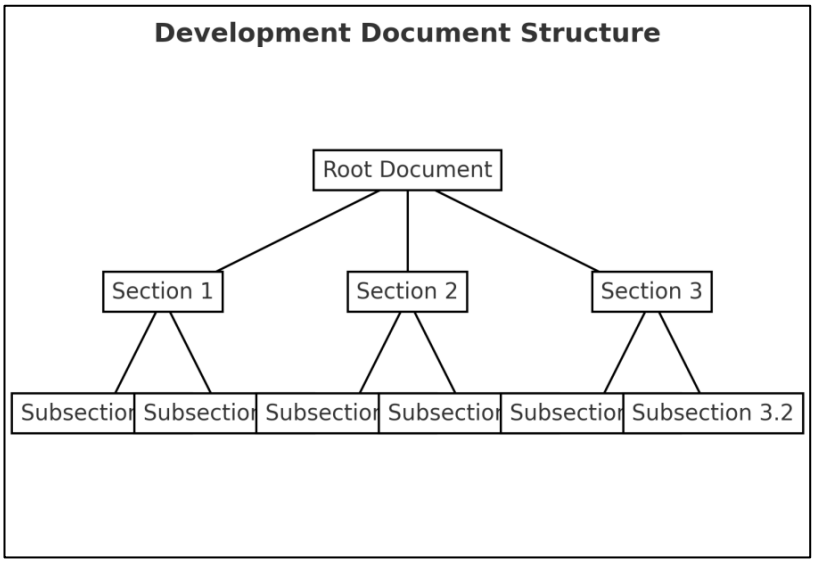

Figure 3-4 그림 제목

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			

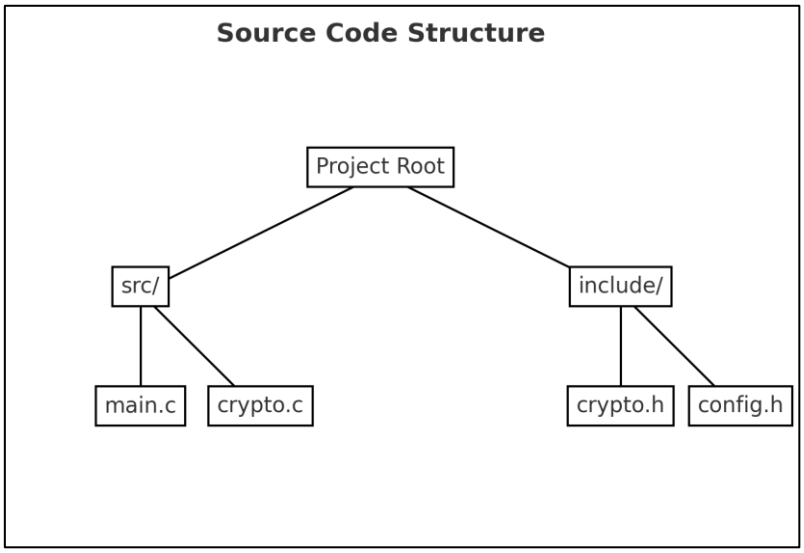

Figure 3-5 그림 제목

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			

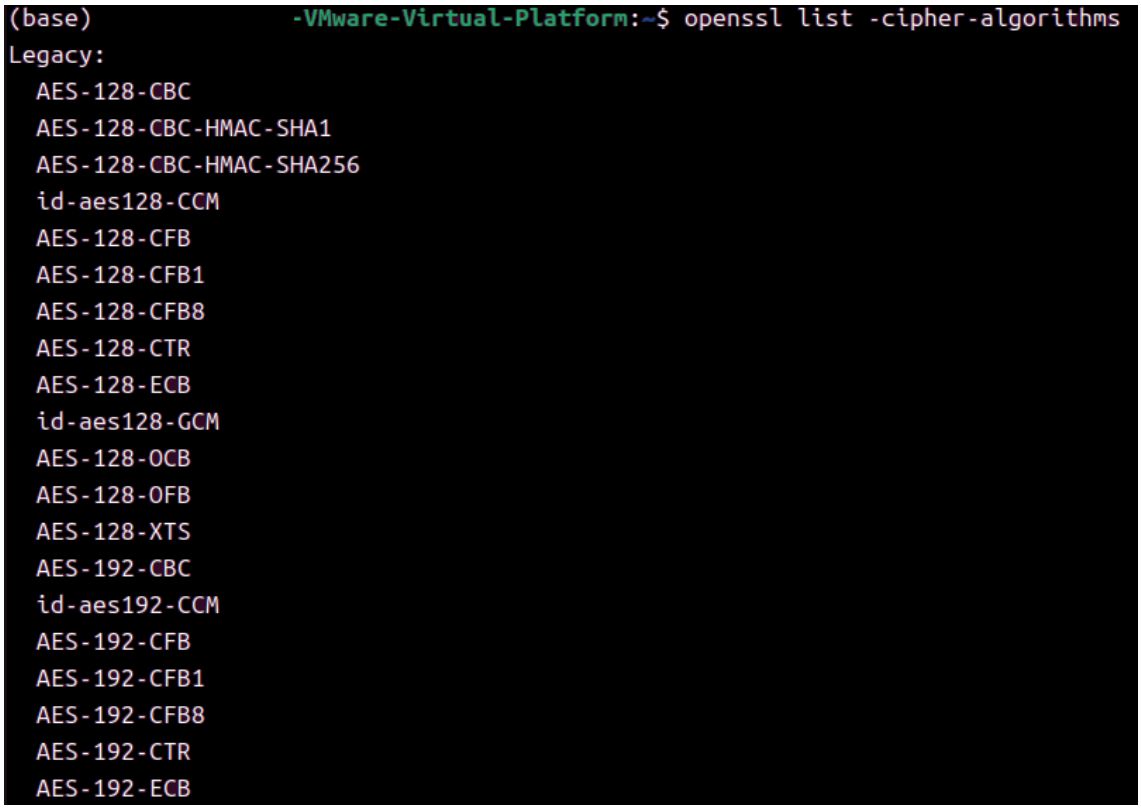

Figure 3-6 그림 제목

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”>

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	5개의 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 물리적 포트 및 논리적 인터페이스 명세	개발문서 검토

2.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-9 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

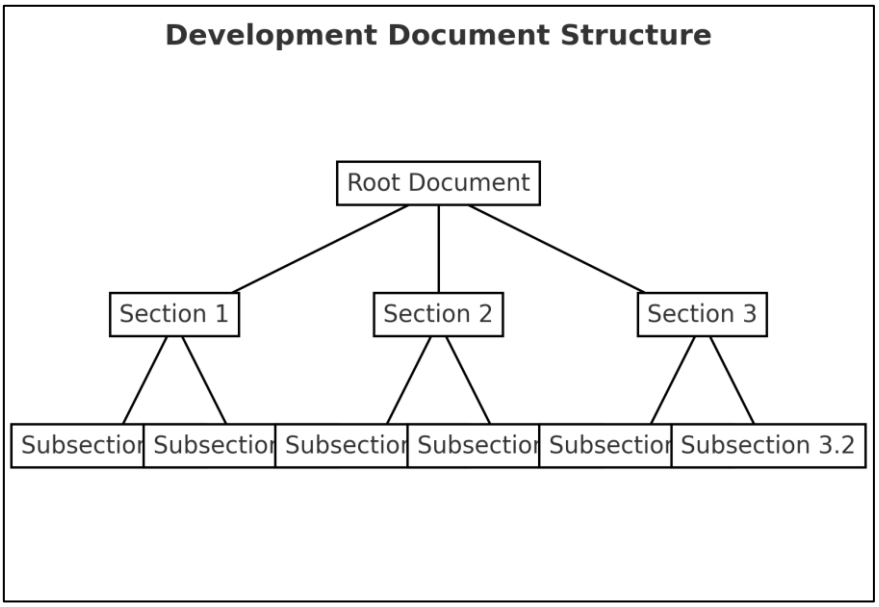

Figure 3-7 그림 제목

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			

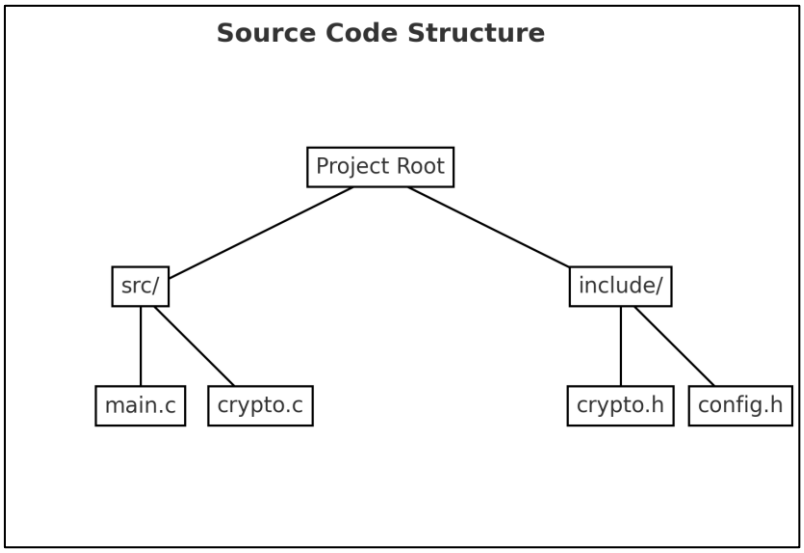

Figure 3-8 그림 제목

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			

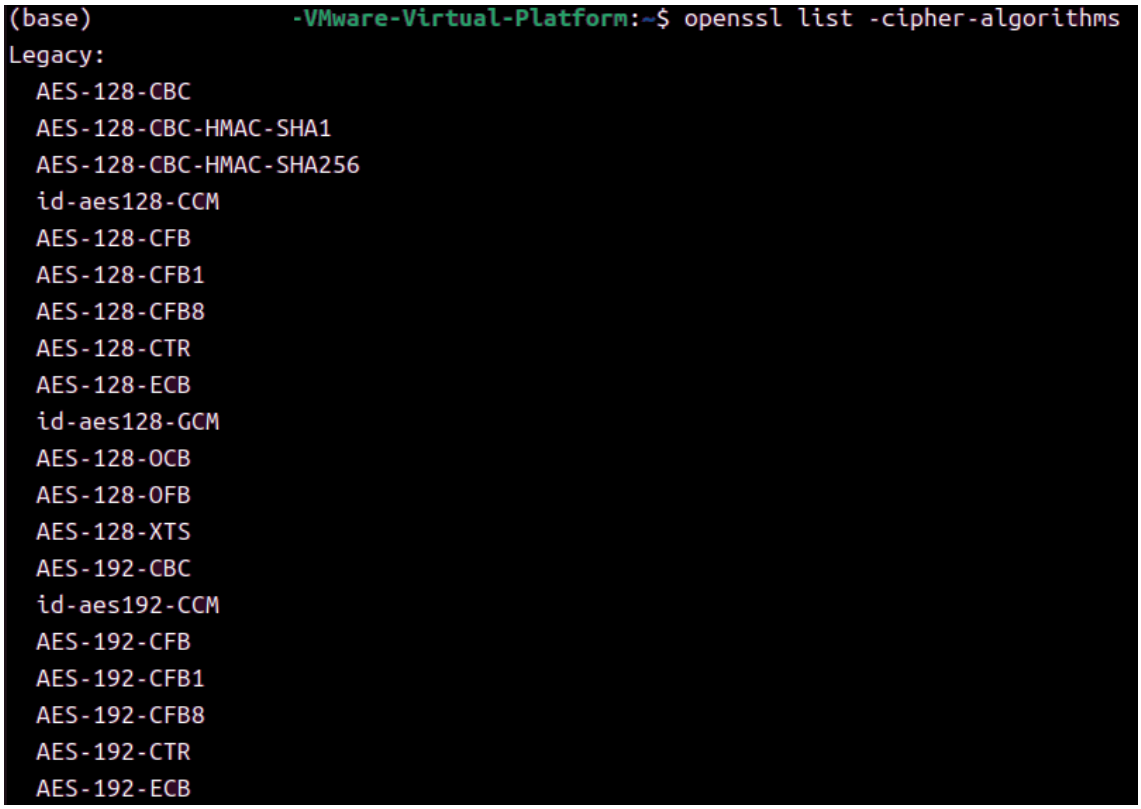

Figure 3-9 그림 제목

2.2.3 판정근거

Table 3-12 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 3-13 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

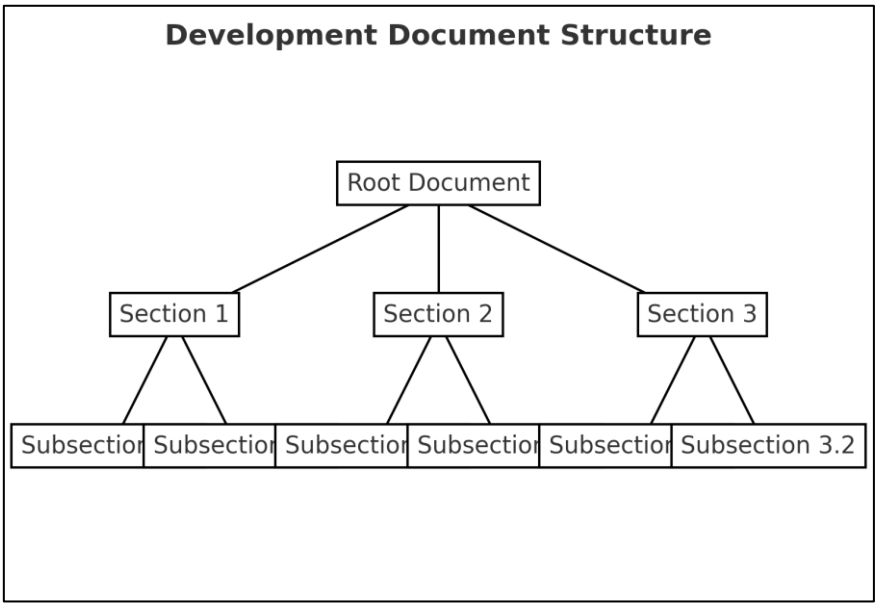

Figure 3-10 그림 제목

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			

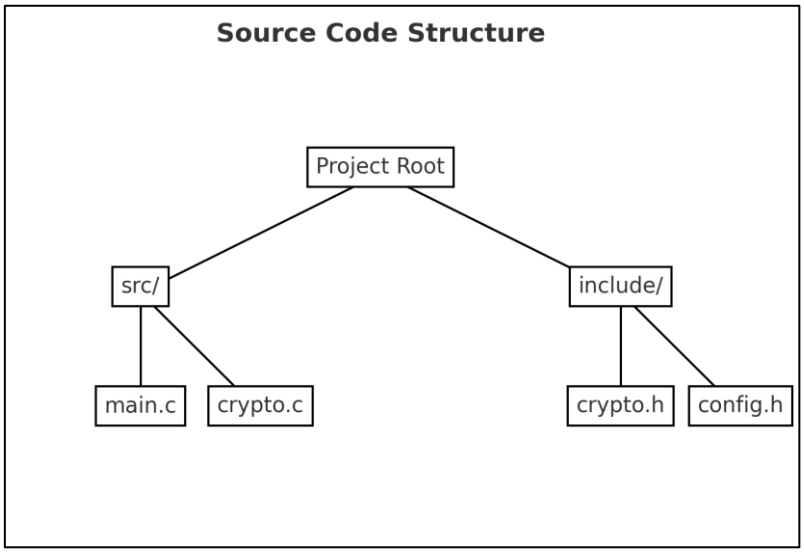

Figure 3-11 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-12 그림 제목

2.3.3 판정근거

Table 3-16 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 3-17 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

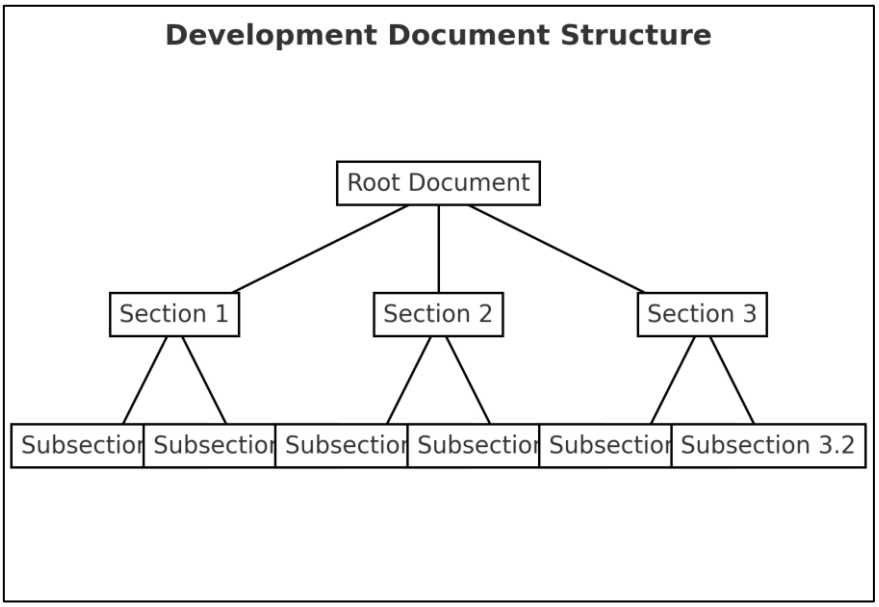

Figure 3-13 그림 제목

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			

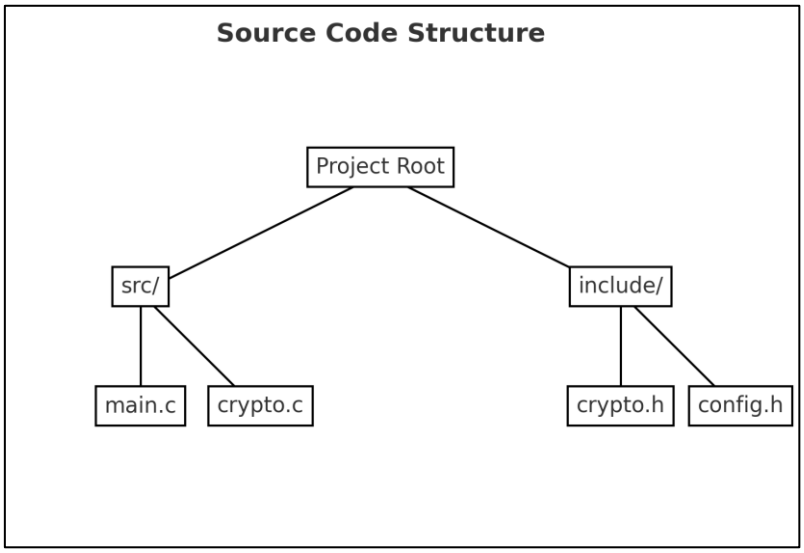

Figure 3-14 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-15 그림 제목

2.4.3 판정근거

Table 3-20 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	개발 문서 명세와 실제 설계된 암호모듈 일치성	소스코드 검토, 암호모듈 검사

2.5.2 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			

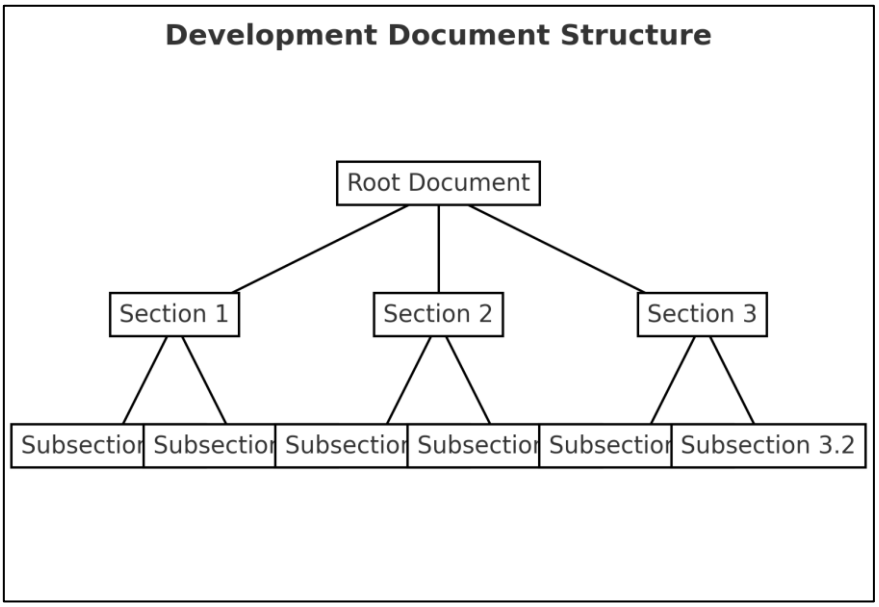

Figure 3-16 그림 제목

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			

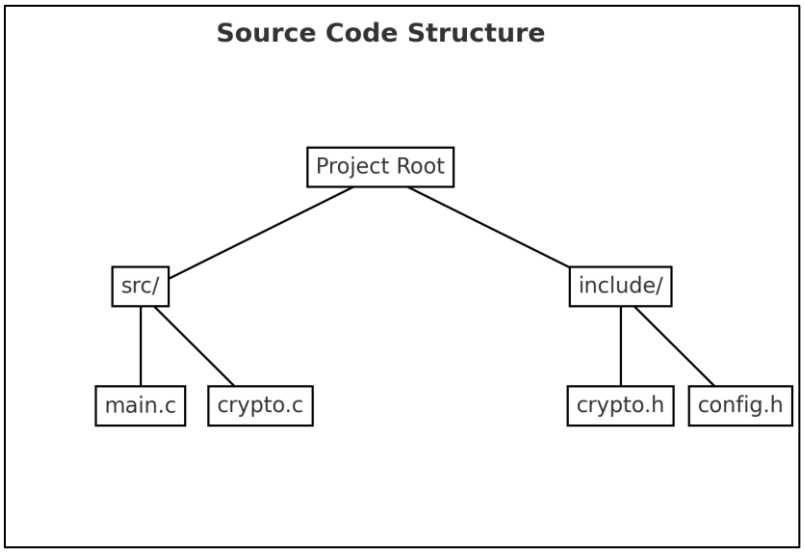

Figure 3-17 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-18 그림 제목

2.5.3 판정근거

Table 3-24 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	명세된 5개의 논리적 인터페이스 서술 여부 (데이터 입력, 데이터 출력, 제어 입력, 제어 출력, 상태 출력)	개발문서 검토

2.6.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-25 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

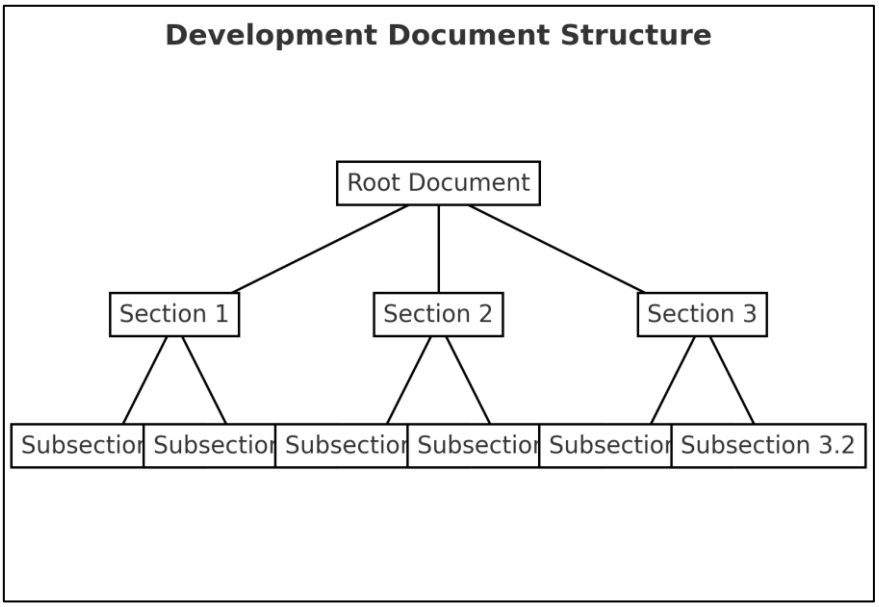

Figure 3-19 그림 제목

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			

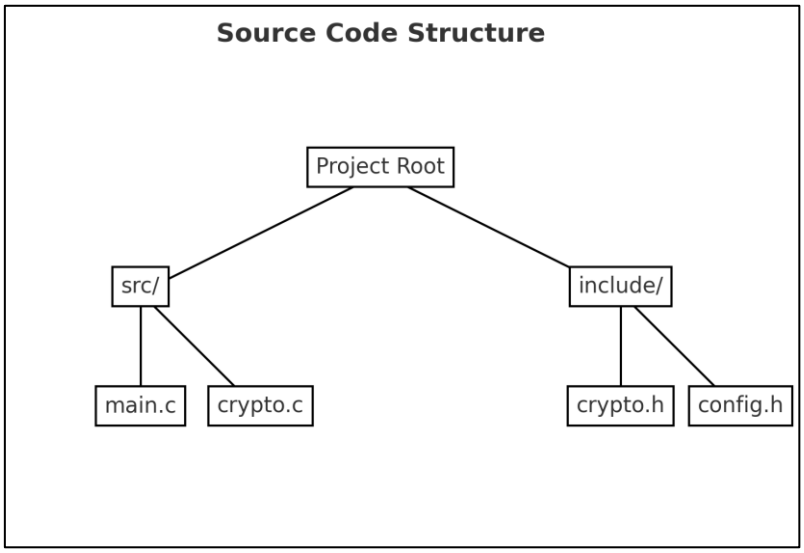

Figure 3-20 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-21 그림 제목

2.6.3 판정근거

Table 3-28 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	명세된 5개의 논리적 인터페이스 서술 여부 (데이터 입력, 데이터 출력, 제어 입력, 제어 출력, 상태 출력)	소스코드 검토, 암호모듈 검사

2.7.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-29 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

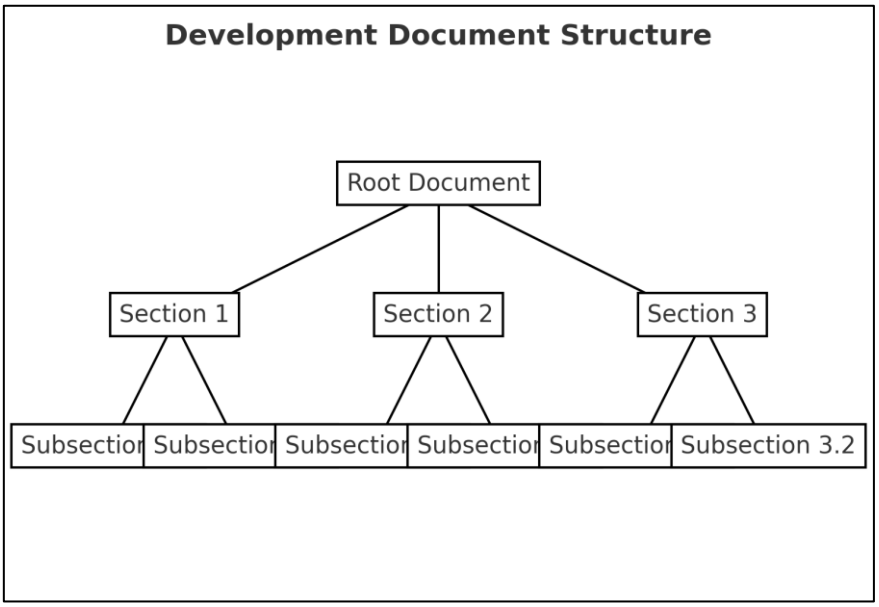

Figure 3-22 그림 제목

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			

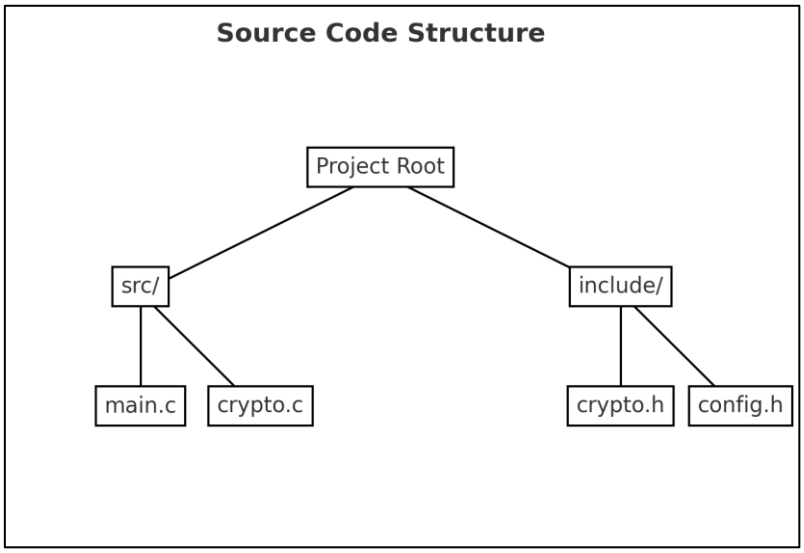

Figure 3-23 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-24 그림 제목

2.7.3 판정근거

Table 3-32 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	처리/출력되는 모든 데이터가 데이터 출력 인터페이스를 통해 출력되는지 여부	소스코드 검토, 암호모듈 검사

2.8.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-33 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

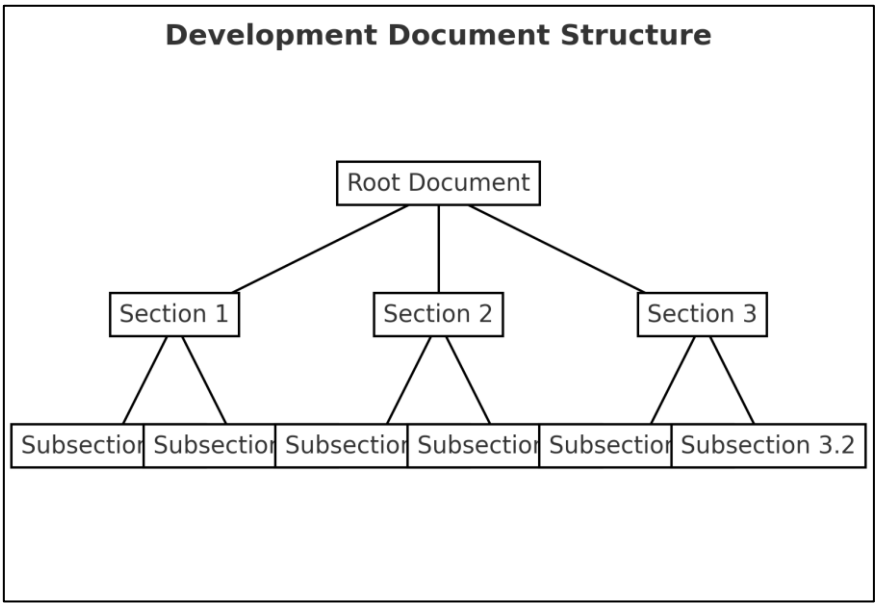

Figure 3-25 그림 제목

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			

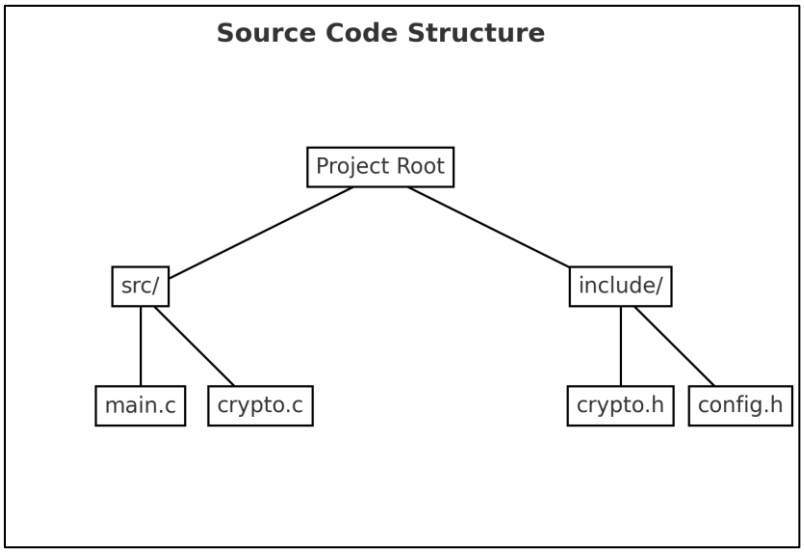

Figure 3-26 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-27 그림 제목

2.8.3 판정근거

Table 3-36 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 TE03.08.01

2.9.1 시험 요구사항

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

2.9.2 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			

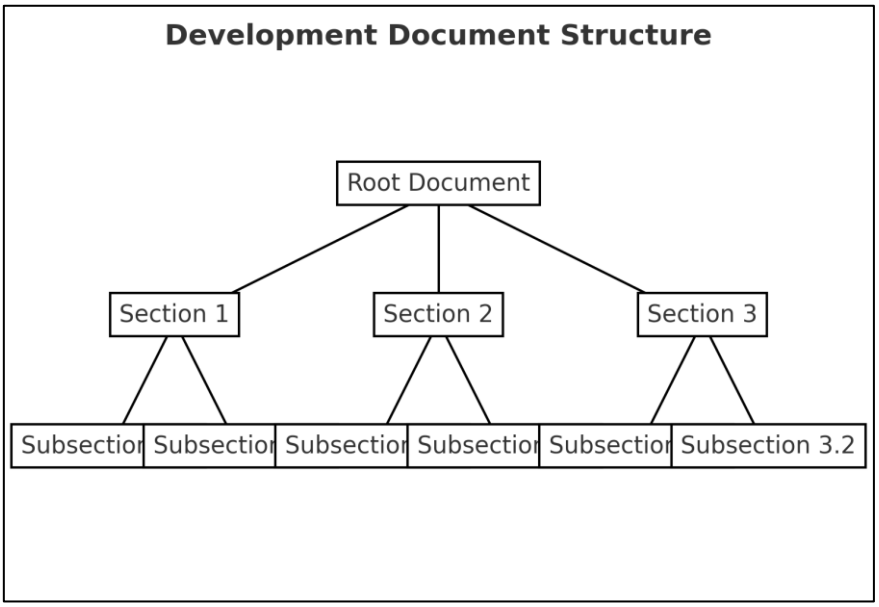

Figure 3-28 그림 제목

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			

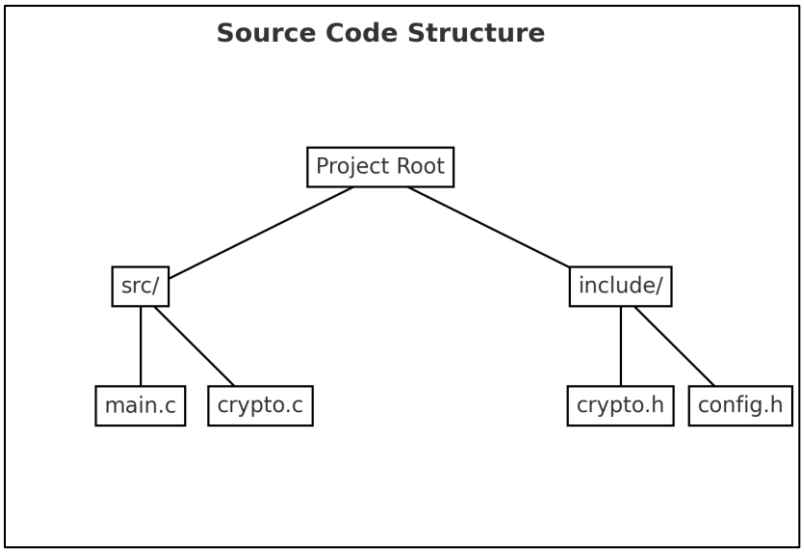

Figure 3-29 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-30 그림 제목

2.9.3 판정근거

Table 3-40 TE03.08.01 시험결과 판정근거

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

2.9.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.10 TE03.09.01

2.10.1 시험 요구사항

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

2.10.2 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			

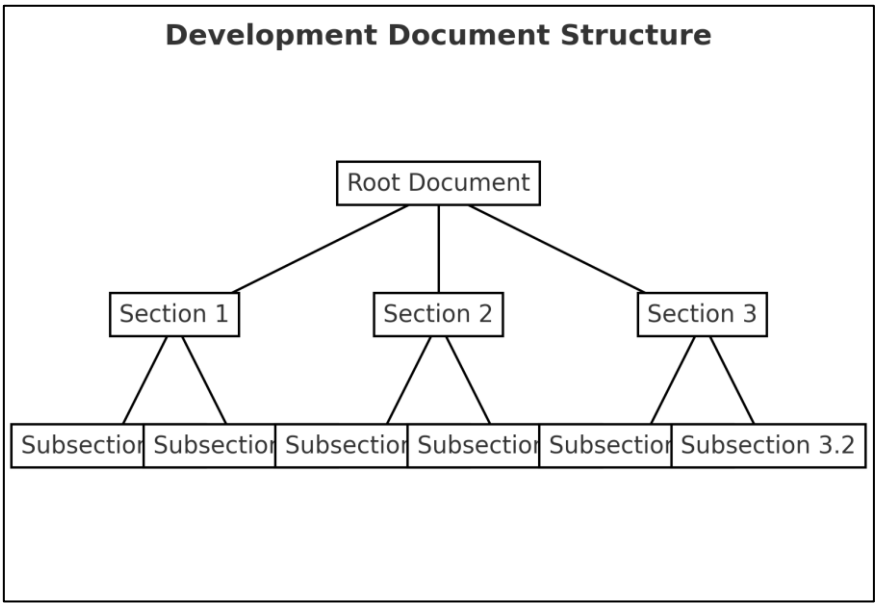

Figure 3-31 그림 제목

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			

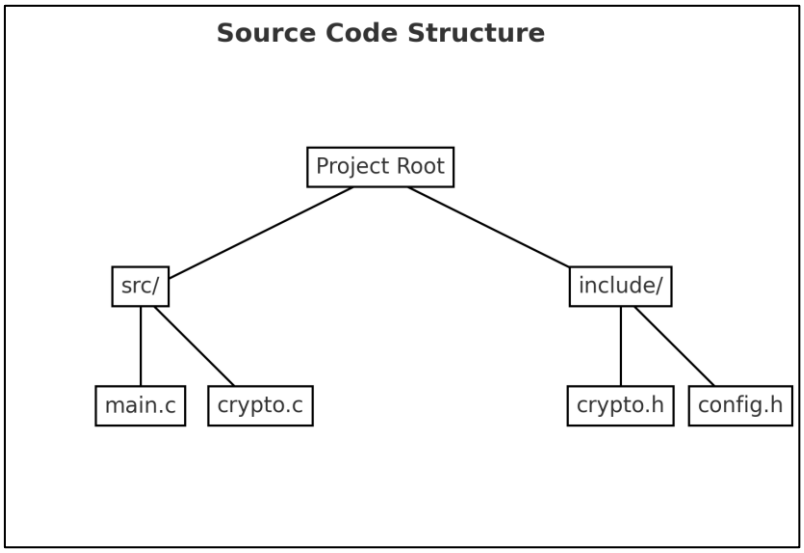

Figure 3-32 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-33 그림 제목

2.10.3 판정근거

Table 3-44 TE03.09.01 시험결과 판정근거

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

2.10.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.11 TE03.09.02

2.11.1 시험 요구사항

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

2.11.2 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			

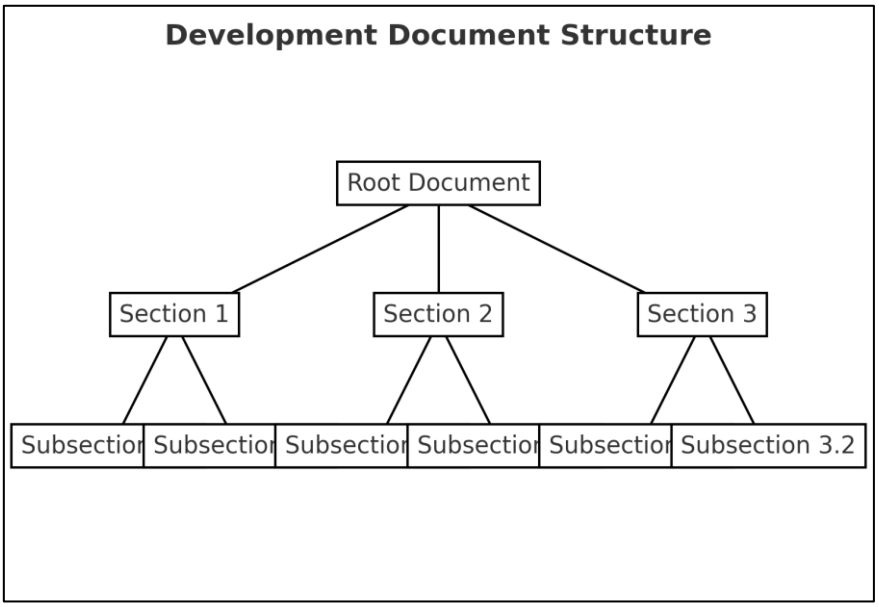

Figure 3-34 그림 제목

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			

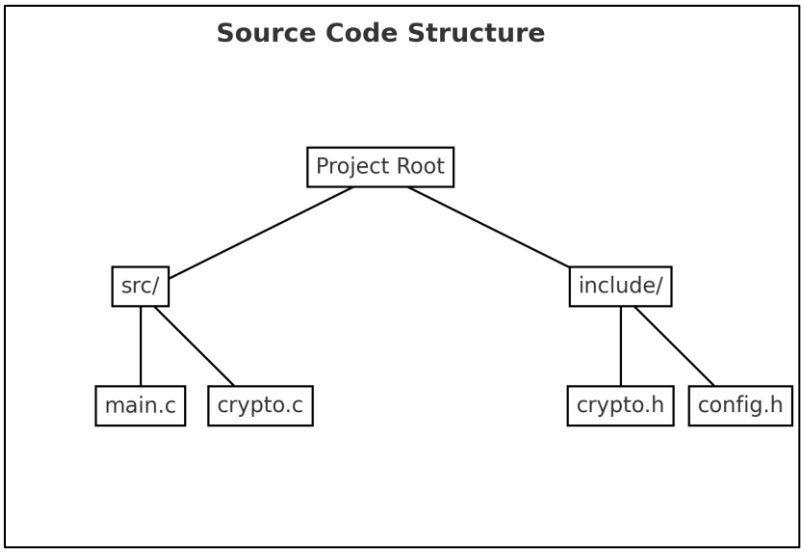

Figure 3-35 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-36 그림 제목

2.11.3 판정근거

Table 3-48 TE03.09.02 시험결과 판정근거

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

2.11.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.12 TE03.10.01

2.12.1 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

2.12.2 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			

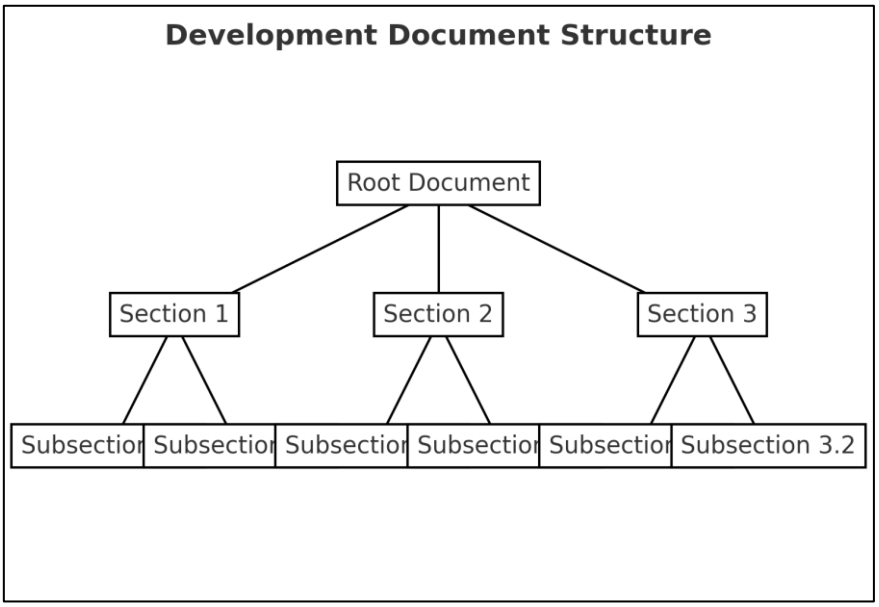

Figure 3-37 그림 제목

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			

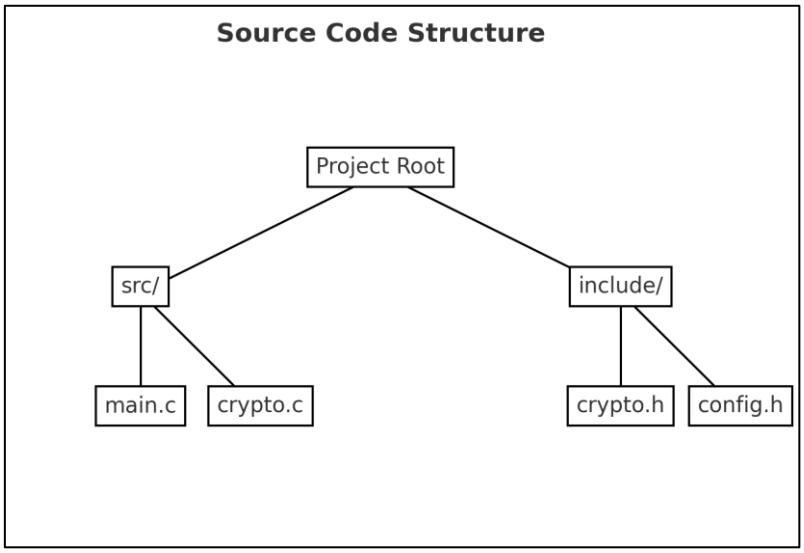

Figure 3-38 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-39 그림 제목

2.12.3 판정근거

Table 3-52 TE03.10.01 시험결과 판정근거

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

2.12.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.13 TE03.10.02

2.13.1 시험 요구사항

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

2.13.2 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			

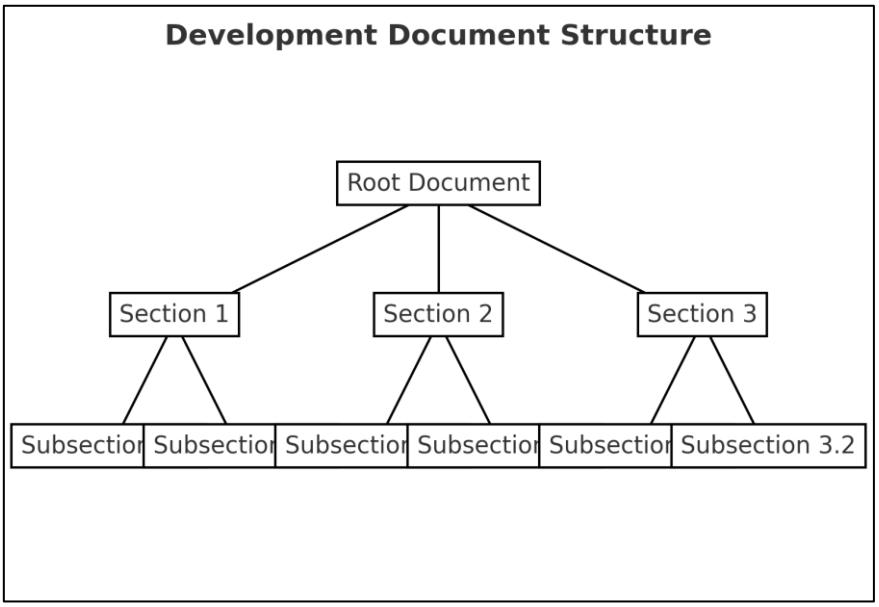

Figure 3-40 그림 제목

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			

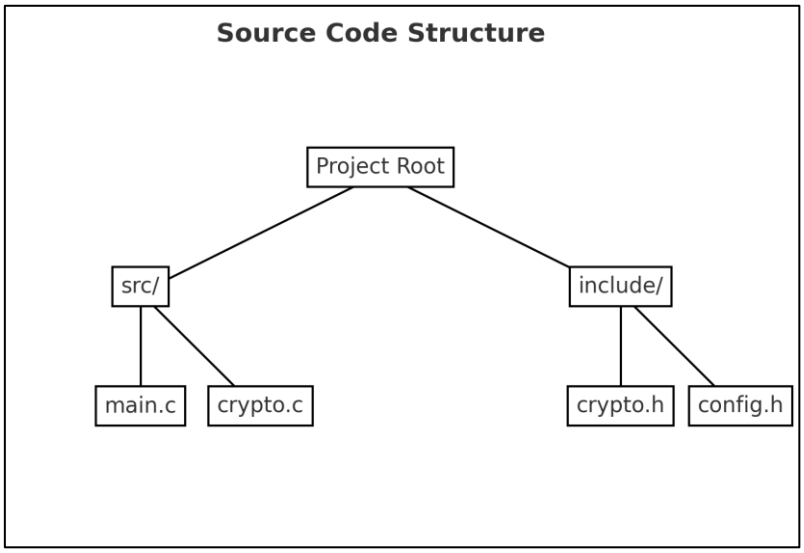

Figure 3-41 그림 제목

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			

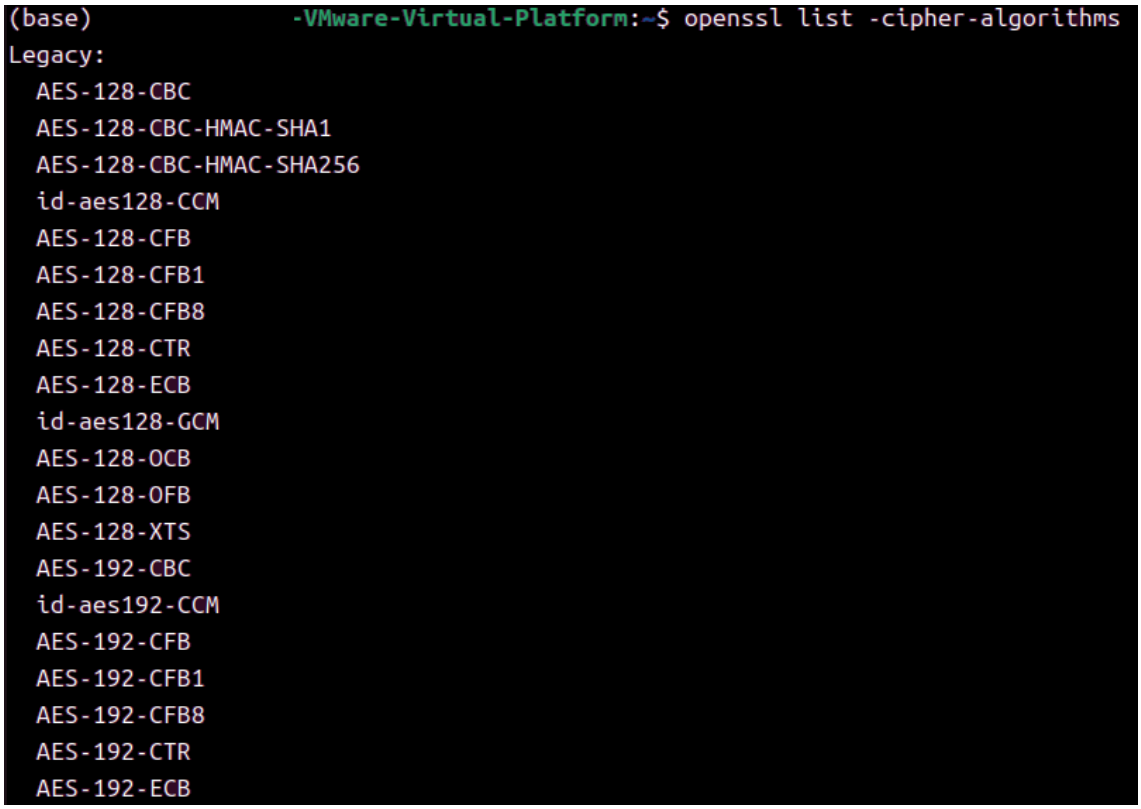

Figure 3-42 그림 제목

2.13.3 판정근거

Table 3-56 TE03.10.02 시험결과 판정근거

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

2.13.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.14 TE03.10.03

2.14.1 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

2.14.2 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			

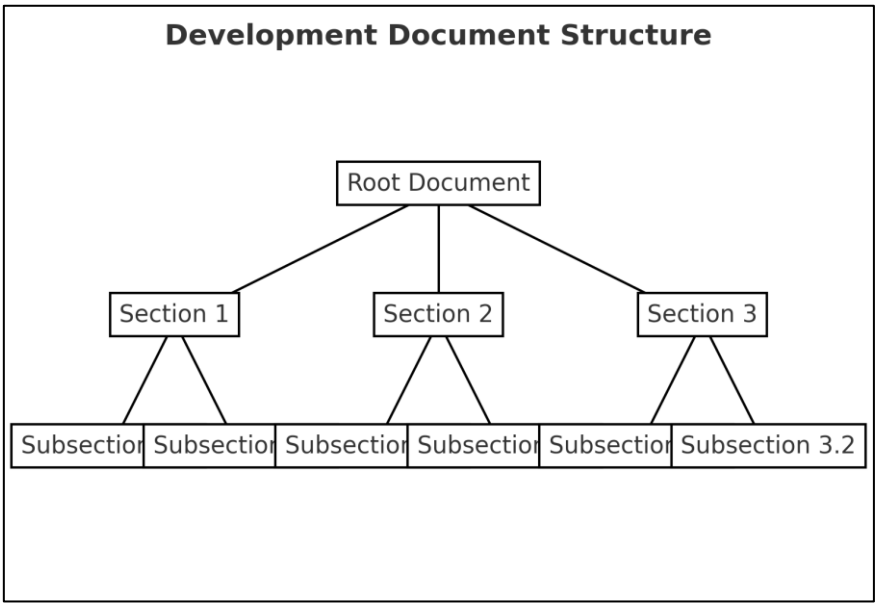

Figure 3-43 그림 제목

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			

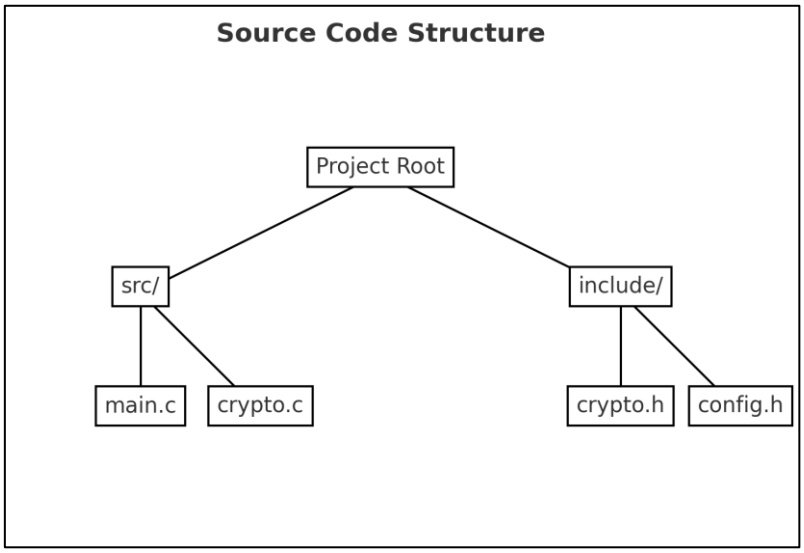

Figure 3-44 그림 제목

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			

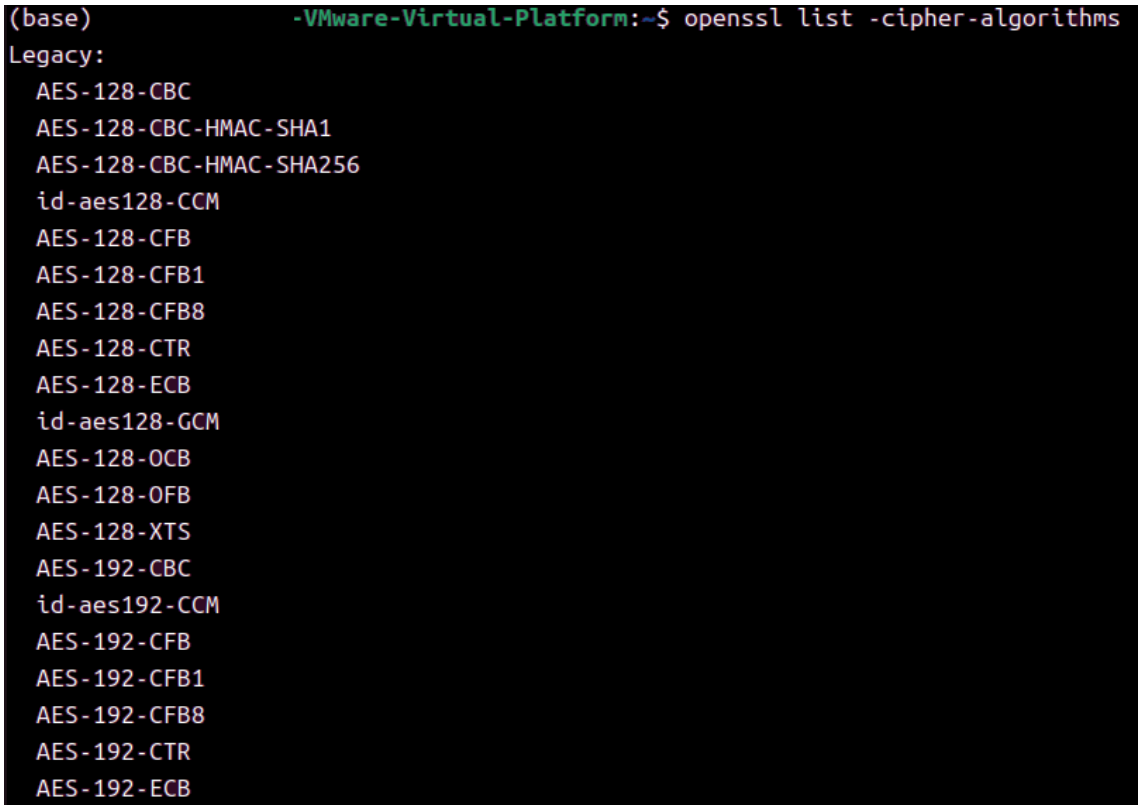

Figure 3-45 그림 제목

2.14.3 판정근거

Table 3-60 TE03.10.03 시험결과 판정근거

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

2.14.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.15 TE03.10.04

2.15.1 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

2.15.2 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			

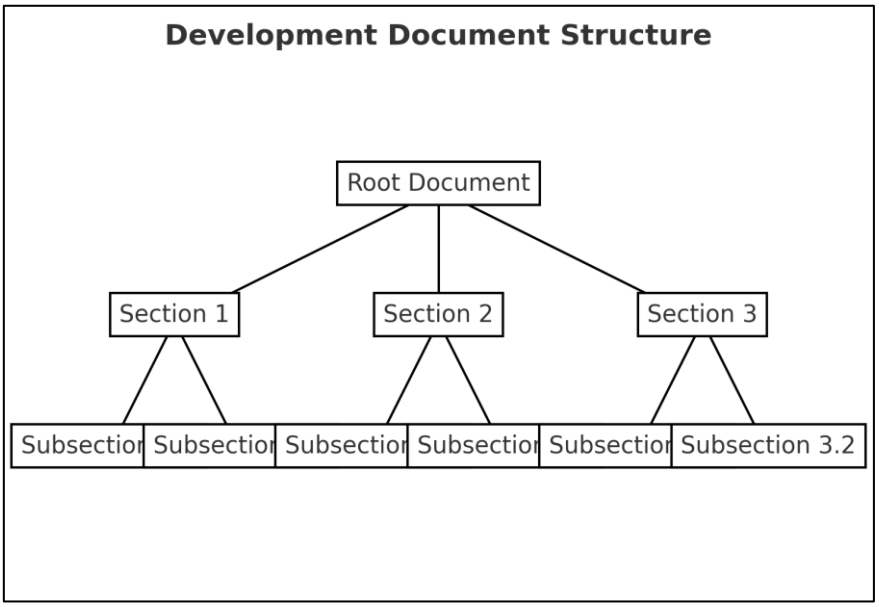

Figure 3-46 그림 제목

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			

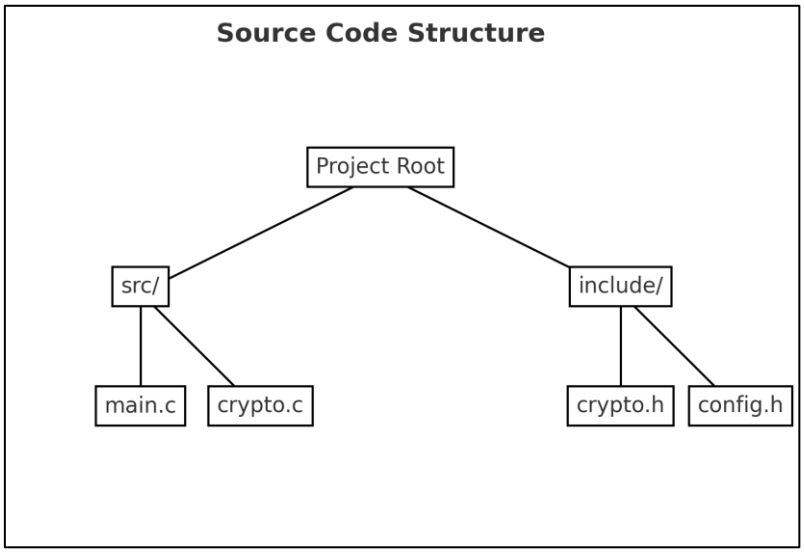

Figure 3-47 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-48 그림 제목

2.15.3 판정근거

Table 3-64 TE03.10.04 시험결과 판정근거

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

2.15.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.16 TE03.10.05

2.16.1 시험 요구사항

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

2.16.2 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			

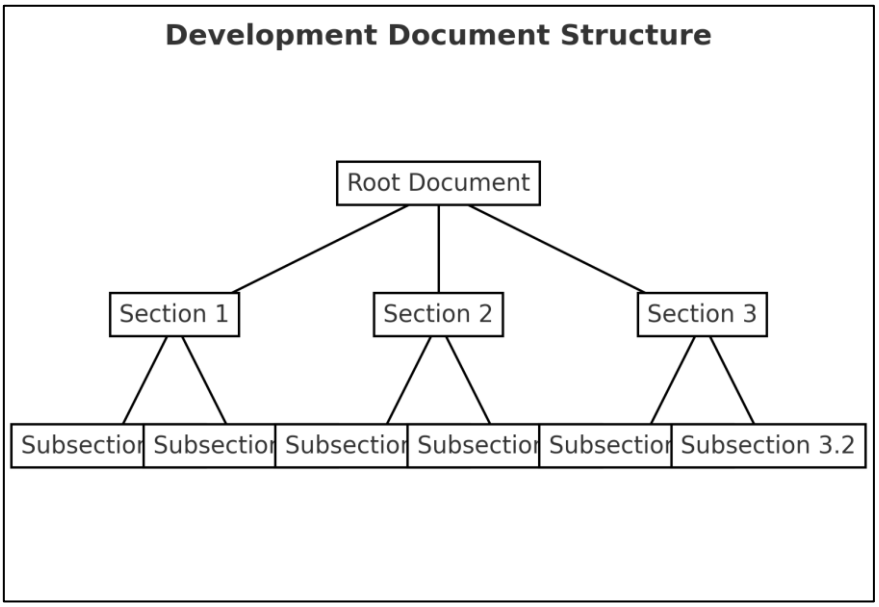

Figure 3-49 그림 제목

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			

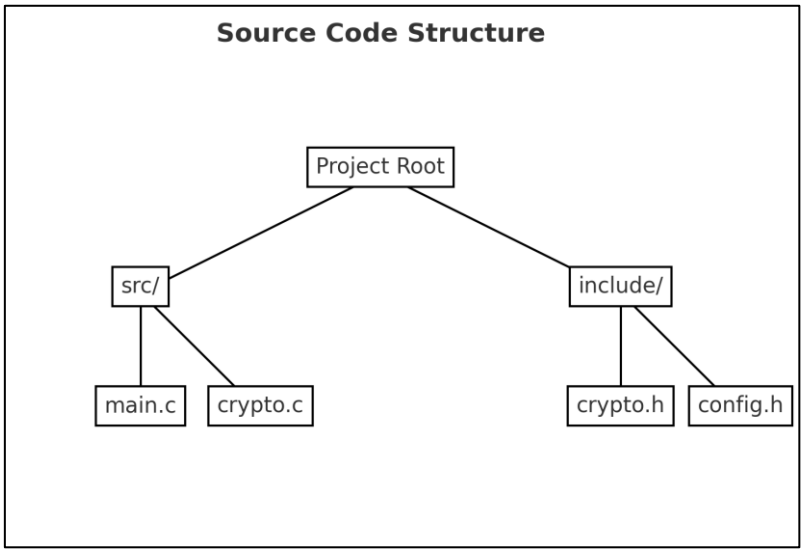

Figure 3-50 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-51 그림 제목

2.16.3 판정근거

Table 3-68 TE03.10.05 시험결과 판정근거

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

2.16.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.17 TE03.11.01

2.17.1 시험 요구사항

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

2.17.2 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			

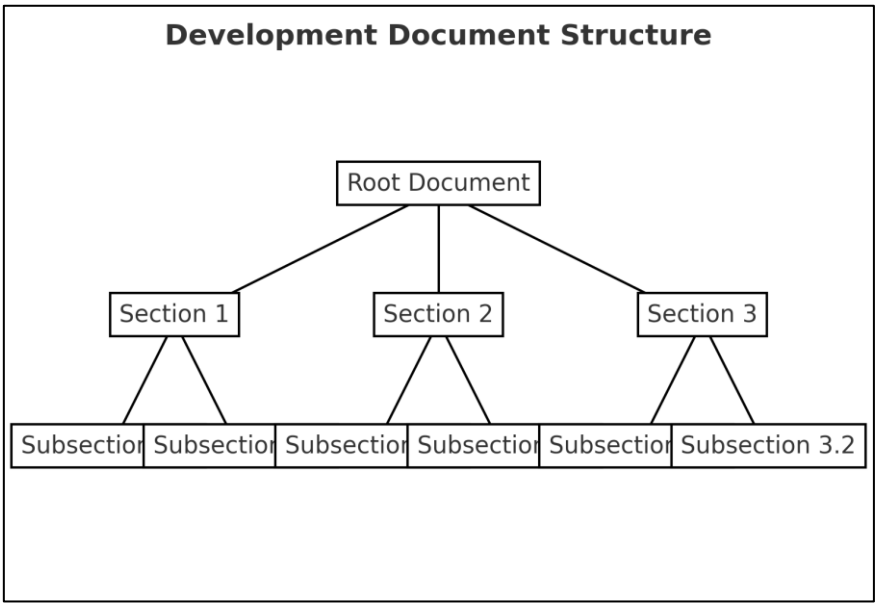

Figure 3-52 그림 제목

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			

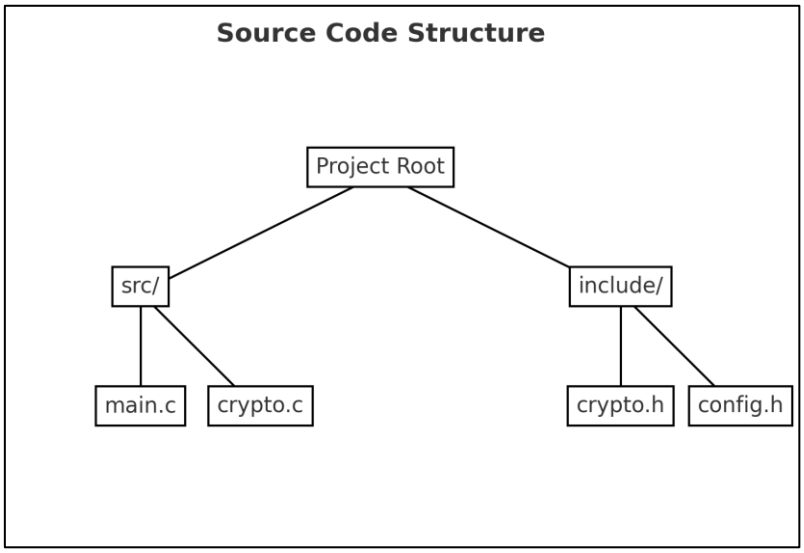

Figure 3-53 그림 제목

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			

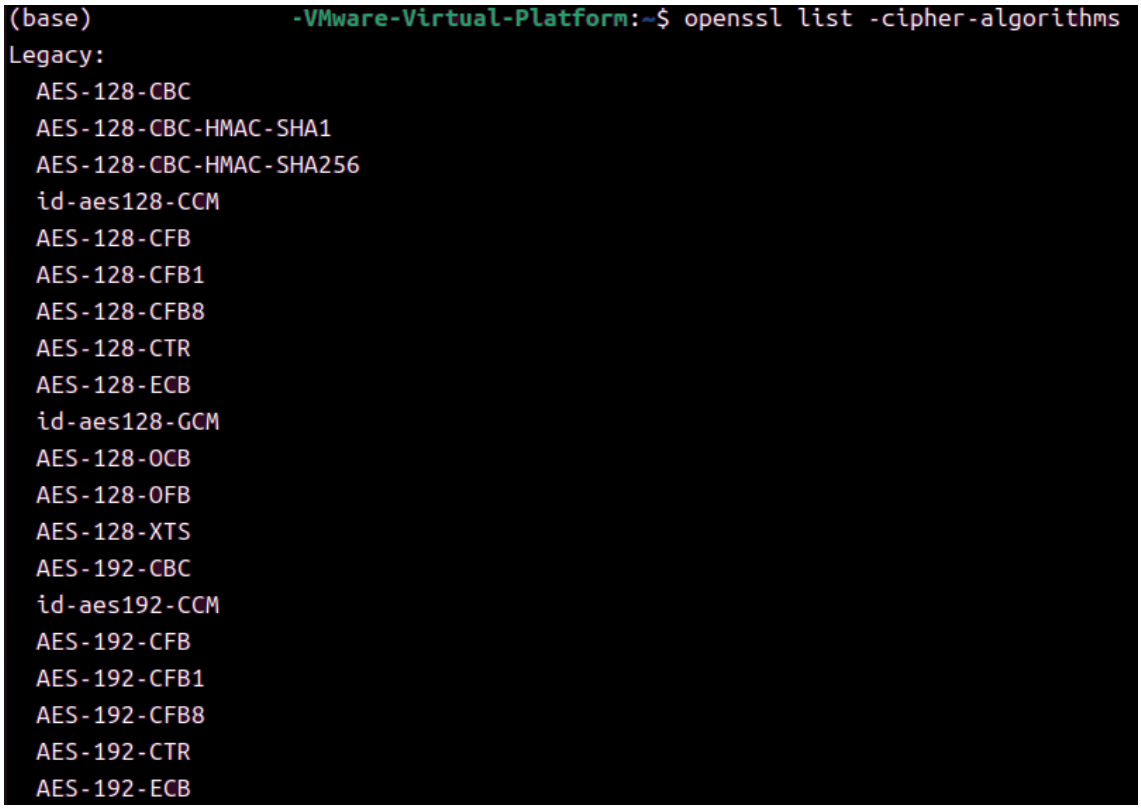

Figure 3-54 그림 제목

2.17.3 판정근거

Table 3-72 TE03.11.01 시험결과 판정근거

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

2.17.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.18 TE03.11.02

2.18.1 시험 요구사항

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

2.18.2 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			

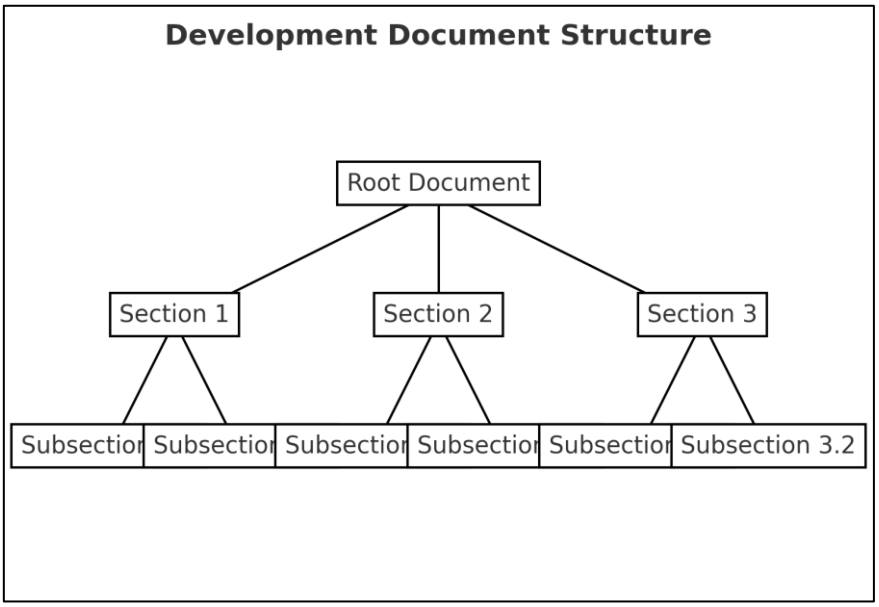

Figure 3-55 그림 제목

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			

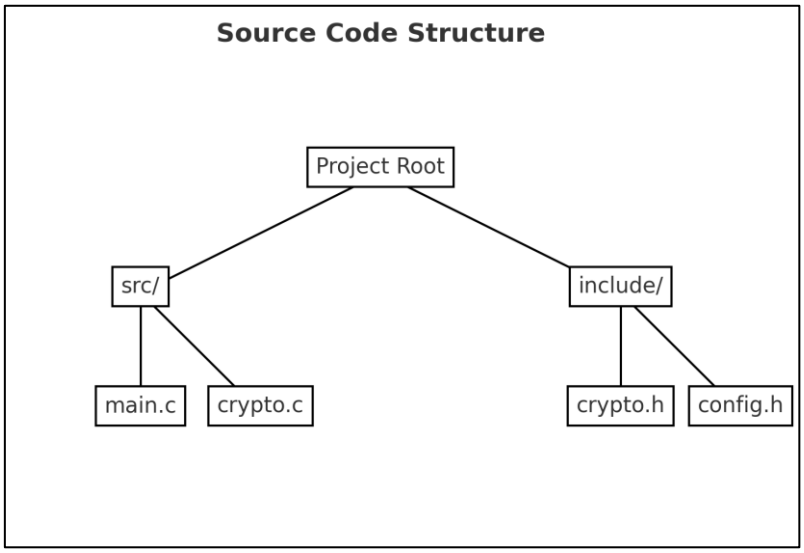

Figure 3-56 그림 제목

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			

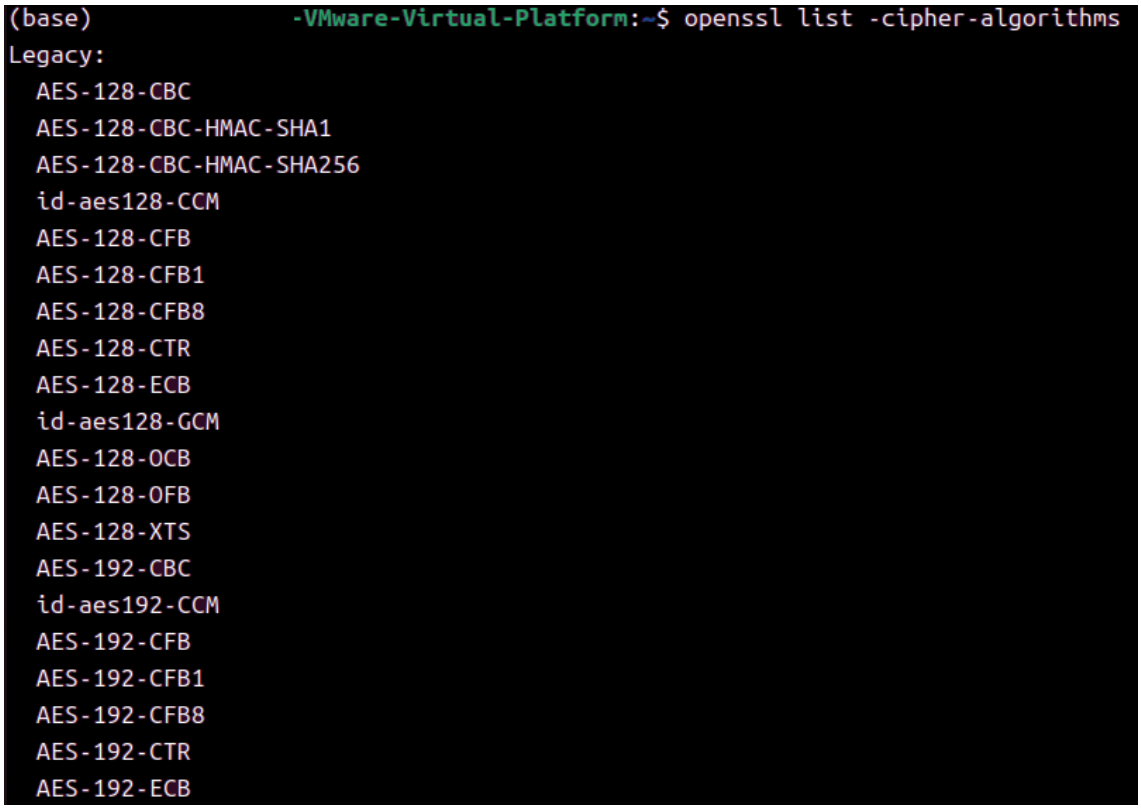

Figure 3-57 그림 제목

2.18.3 판정근거

Table 3-76 TE03.11.02 시험결과 판정근거

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

2.18.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.19 TE03.15.01

2.19.1 시험 요구사항

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

2.19.2 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			

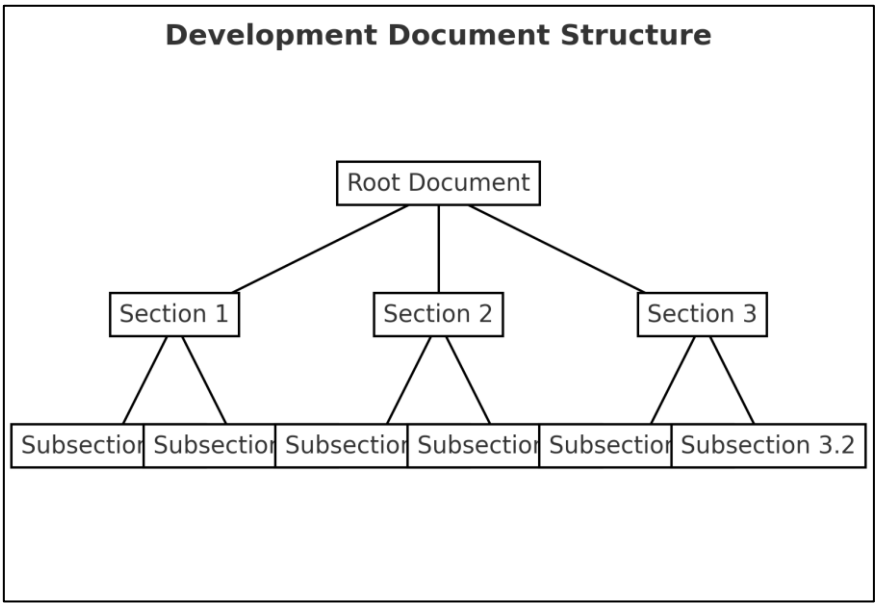

Figure 3-58 그림 제목

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			

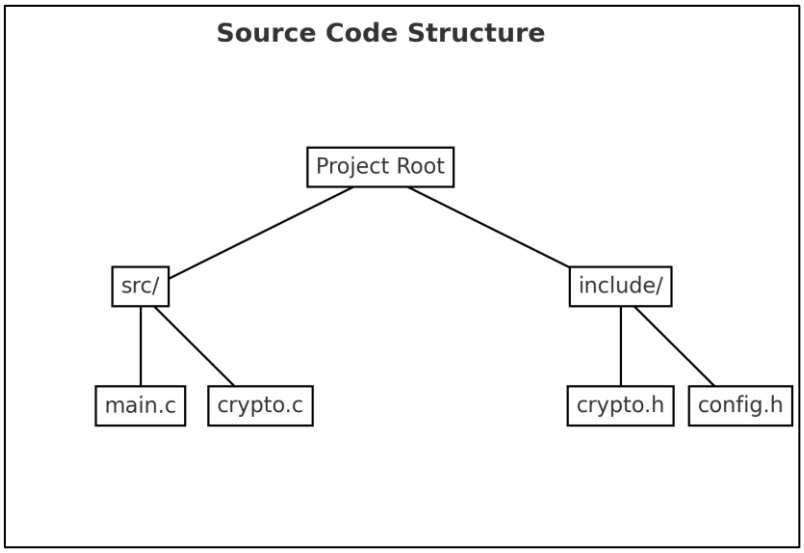

Figure 3-59 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-60 그림 제목

2.19.3 판정근거

Table 3-80 TE03.15.01 시험결과 판정근거

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

2.19.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.20 TE03.15.02

2.20.1 시험 요구사항

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

2.20.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-81 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

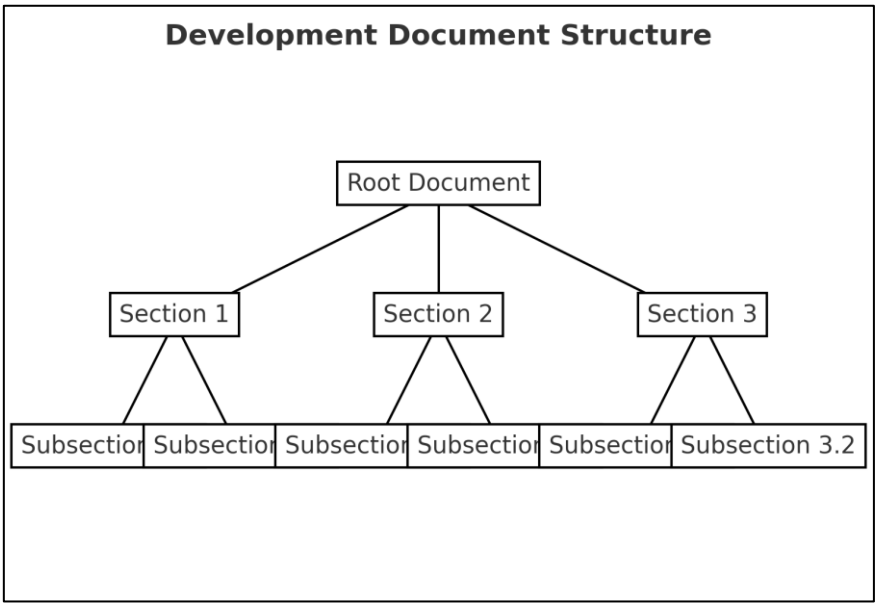

Figure 3-61 그림 제목

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			

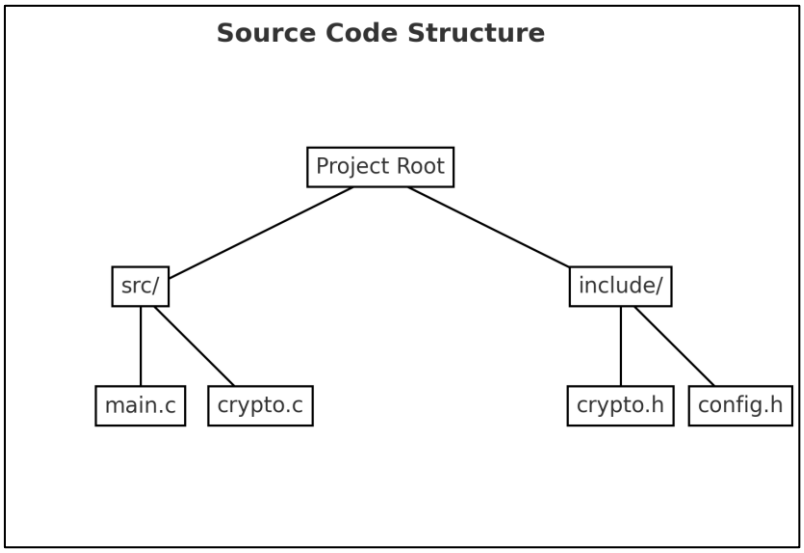

Figure 3-62 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-63 그림 제목

2.20.3 판정근거

Table 3-84 TE03.15.02 시험결과 판정근거

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

2.20.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.21 TE03.15.03

2.21.1 시험 요구사항

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

2.21.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-85 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

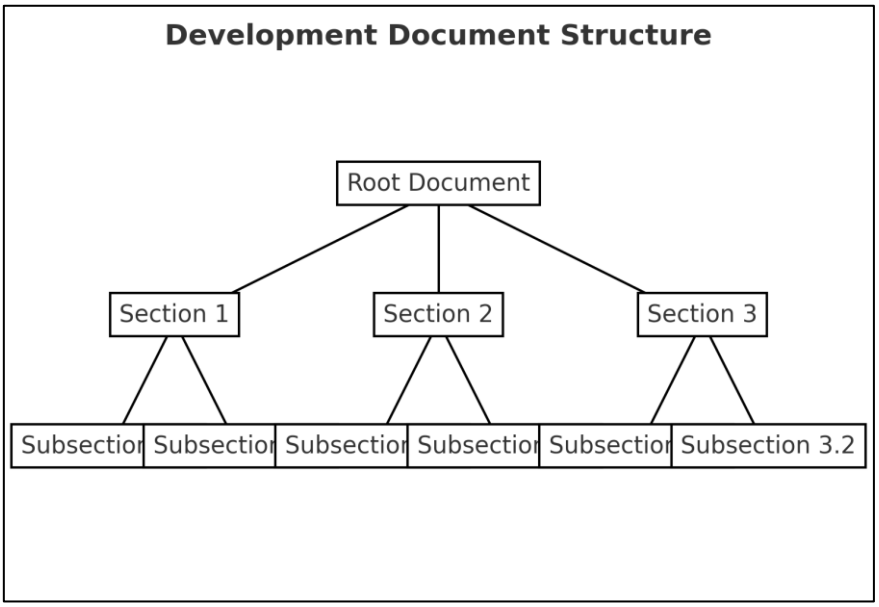

Figure 3-64 그림 제목

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			

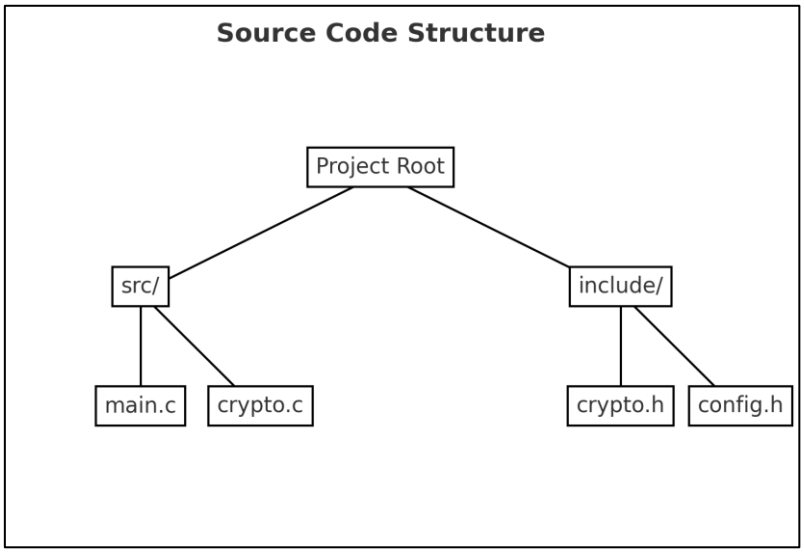

Figure 3-65 그림 제목

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			

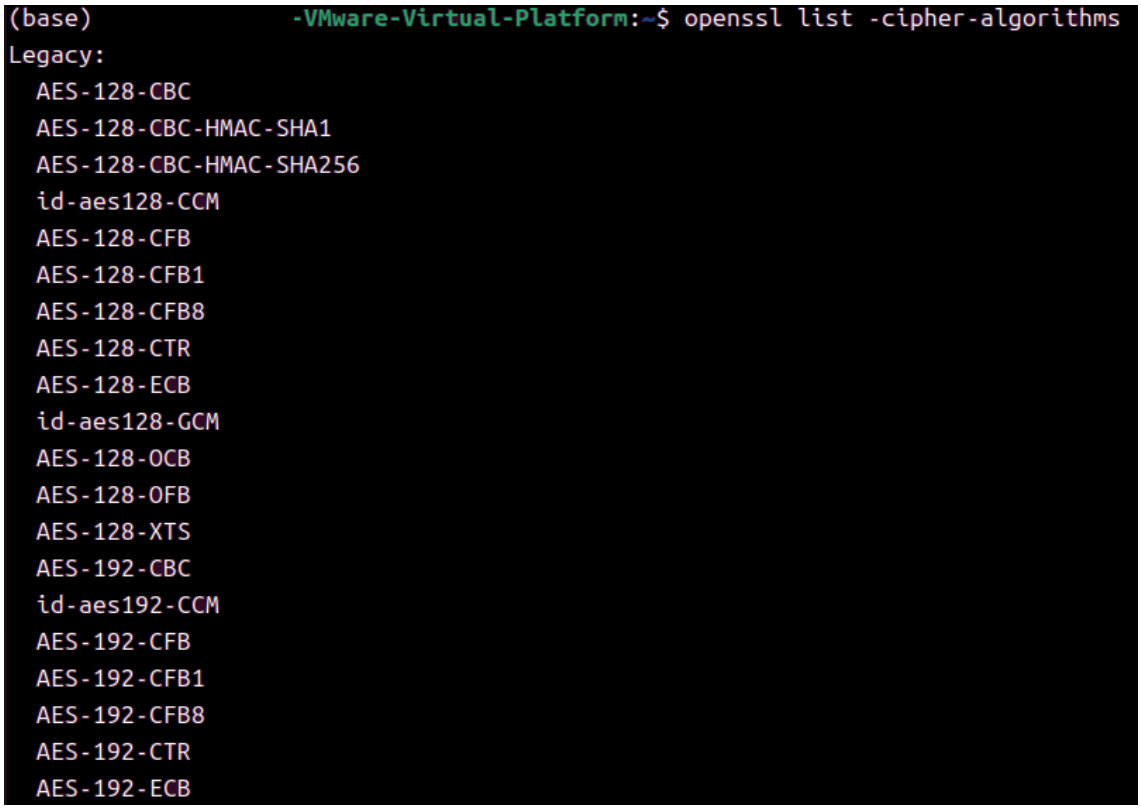

Figure 3-66 그림 제목

2.21.3 판정근거

Table 3-88 TE03.15.03 시험결과 판정근거

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

2.21.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.22 TE03.15.04

2.22.1 시험 요구사항

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

2.22.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-89 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

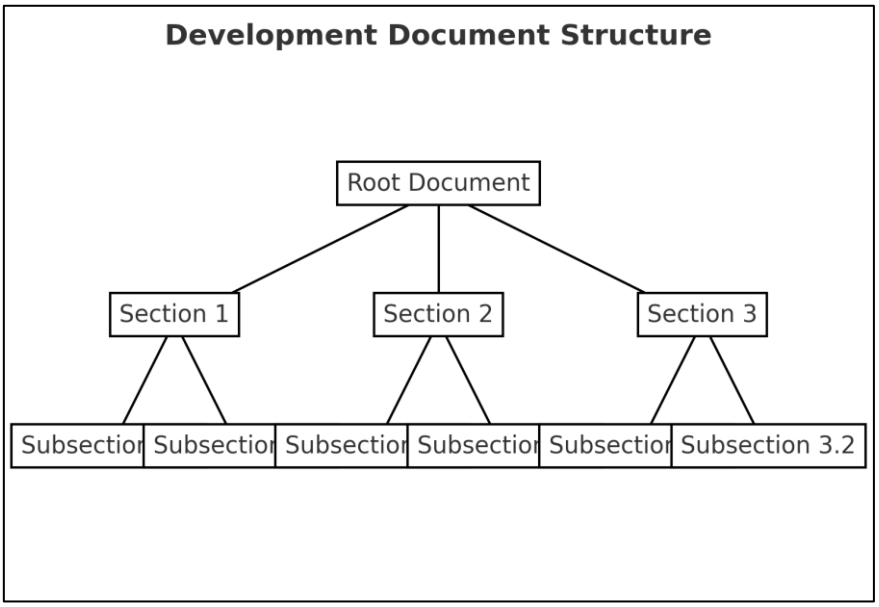

Figure 3-67 그림 제목

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			

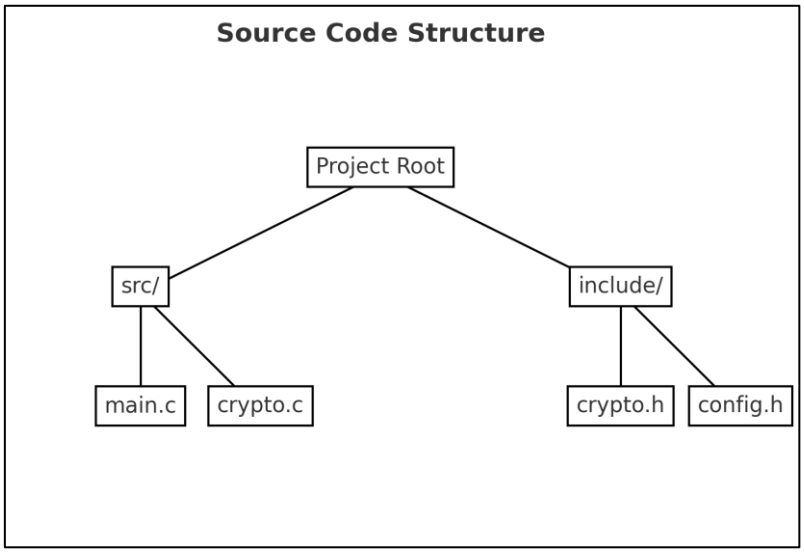

Figure 3-68 그림 제목

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			

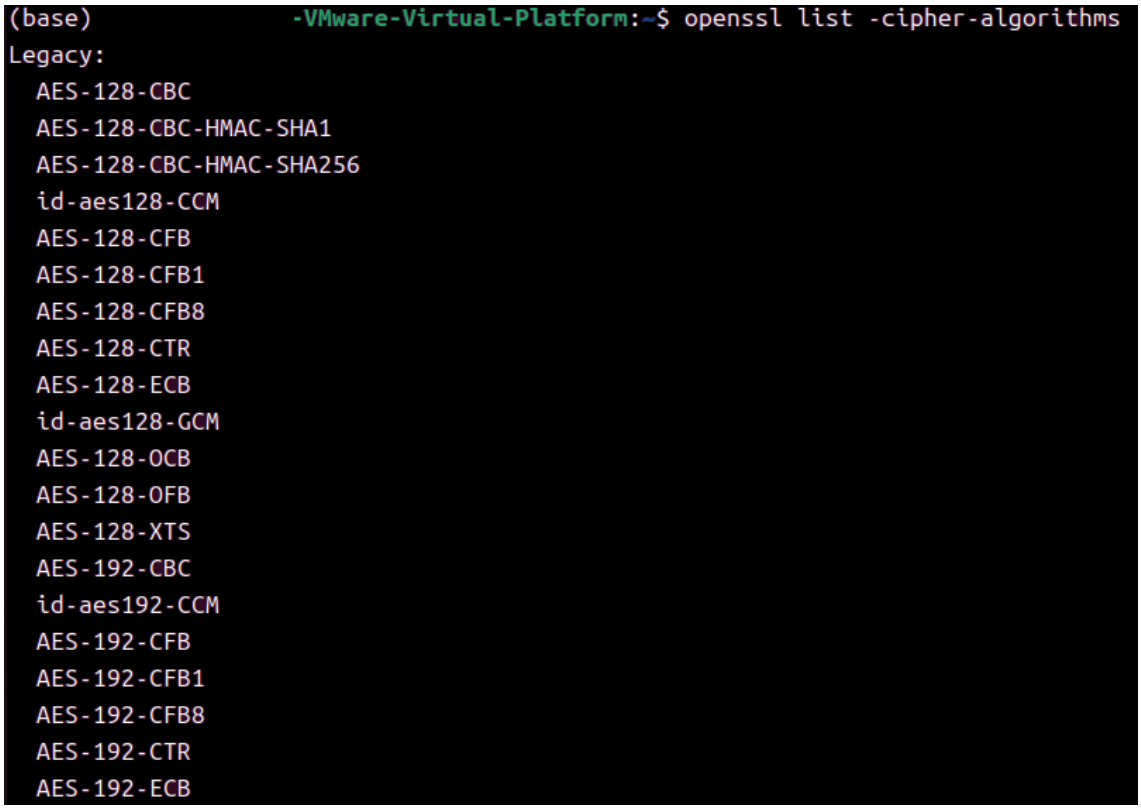

Figure 3-69 그림 제목

2.22.3 판정근거

Table 3-92 TE03.15.04 시험결과 판정근거

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

2.22.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.23 TE03.15.05

2.23.1 시험 요구사항

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

2.23.2 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			

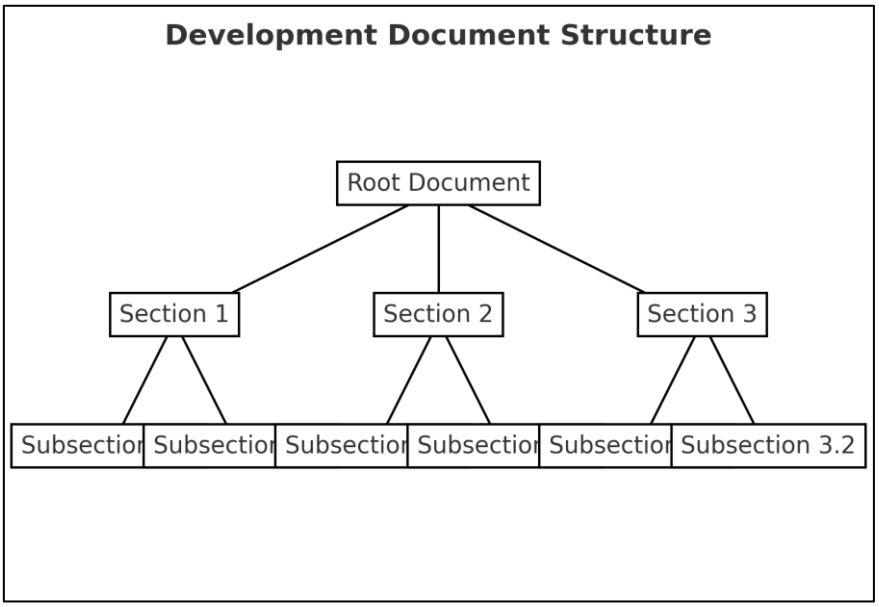

Figure 3-70 그림 제목

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			

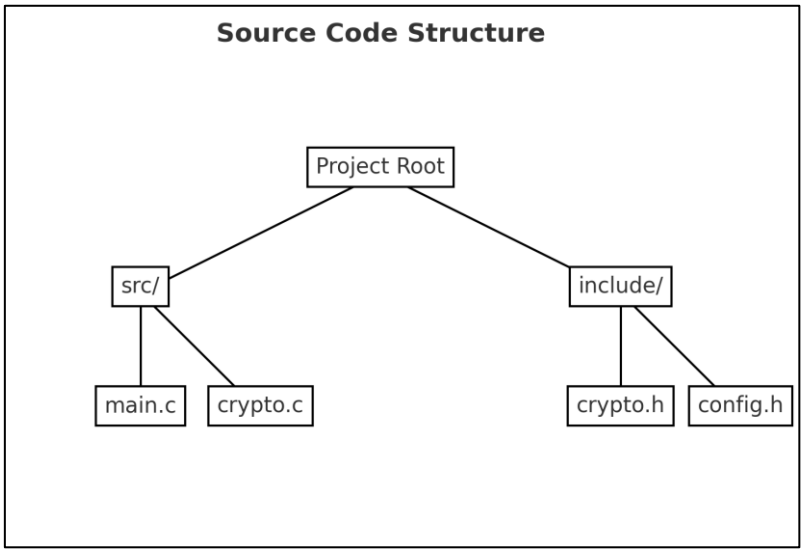

Figure 3-71 그림 제목

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			

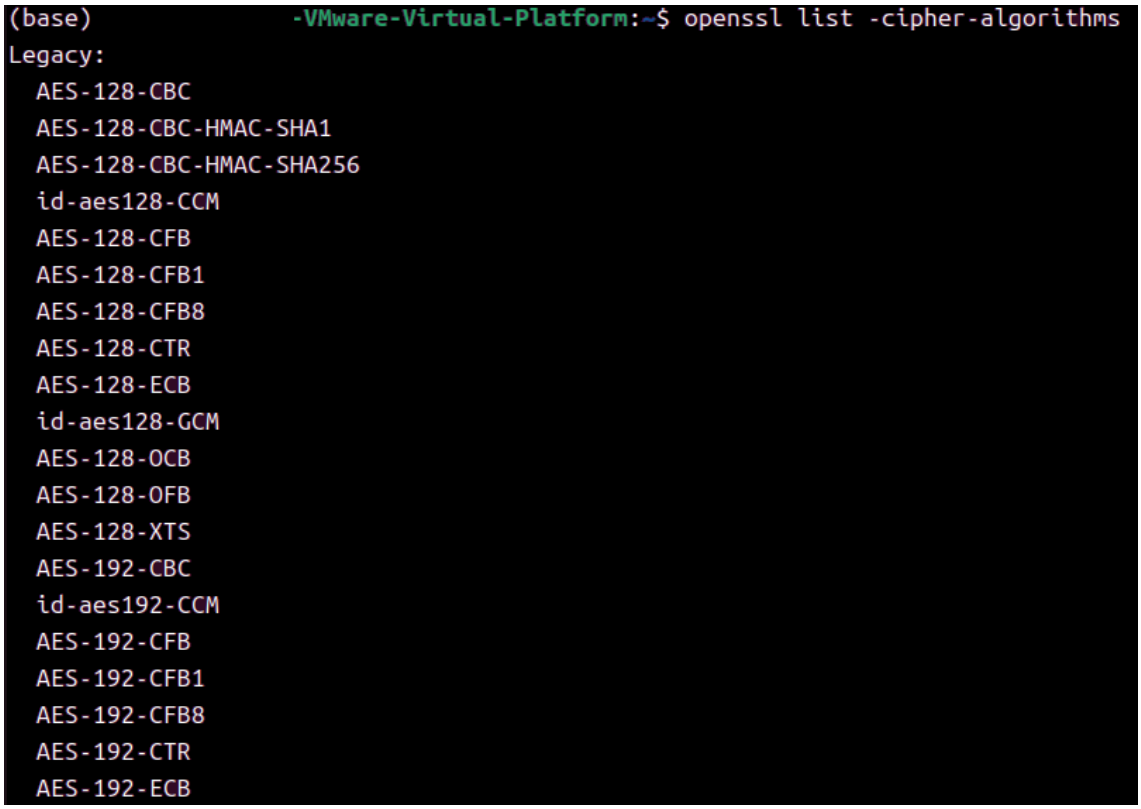

Figure 3-72 그림 제목

2.23.3 판정근거

Table 3-96 TE03.15.05 시험결과 판정근거

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

2.23.4 판정결과

- 판정: <“통과” 또는 “실패”>

2.24 TE03.15.06

2.24.1 시험 요구사항

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

2.24.2 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			

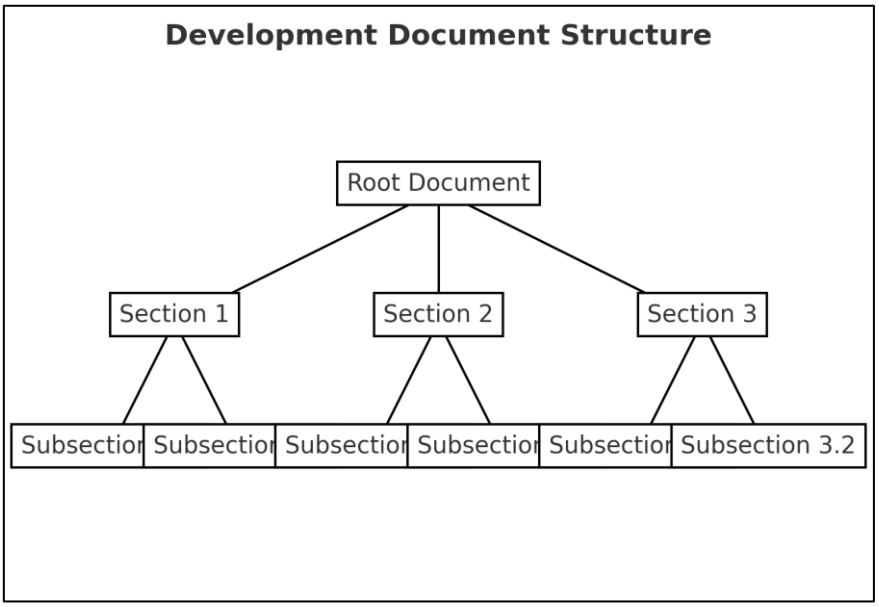

Figure 3-73 그림 제목

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			

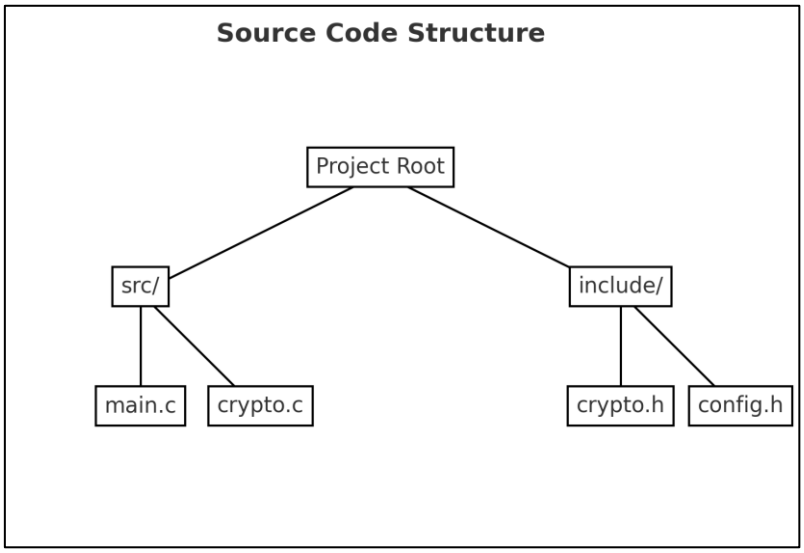

Figure 3-74 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-75 그림 제목

2.24.3 판정근거

Table 3-100 TE03.15.06 시험결과 판정근거

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

2.24.4 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 3-101 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

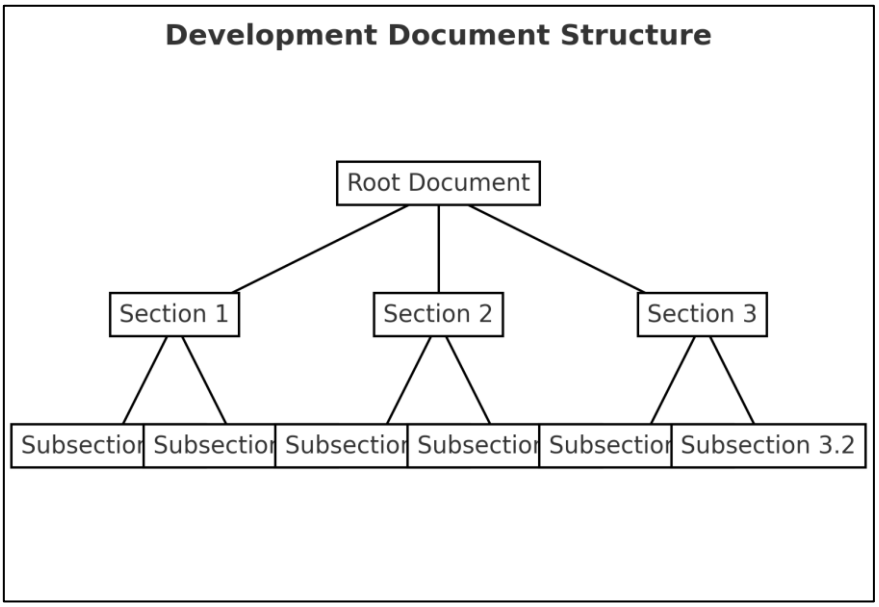

Figure 3-76 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-102 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

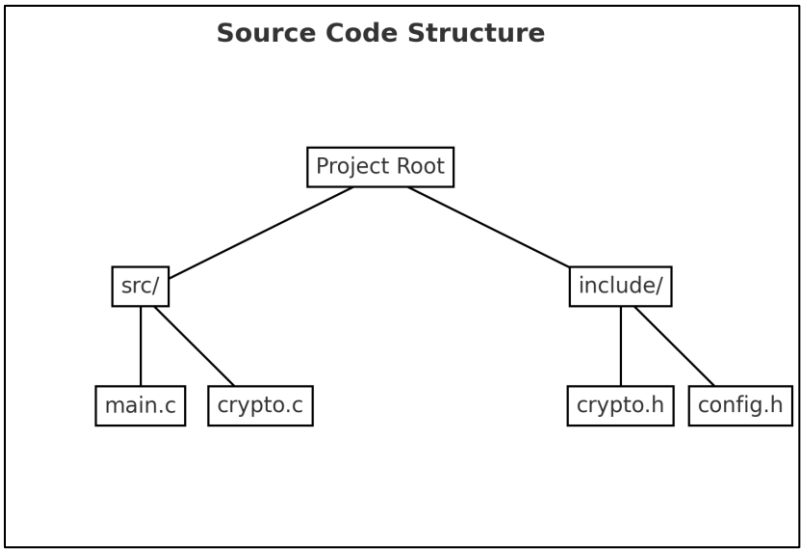

Figure 3-77 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-78 그림 제목

3.2.3 판정근거

Table 3-104 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”>

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 3-105 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

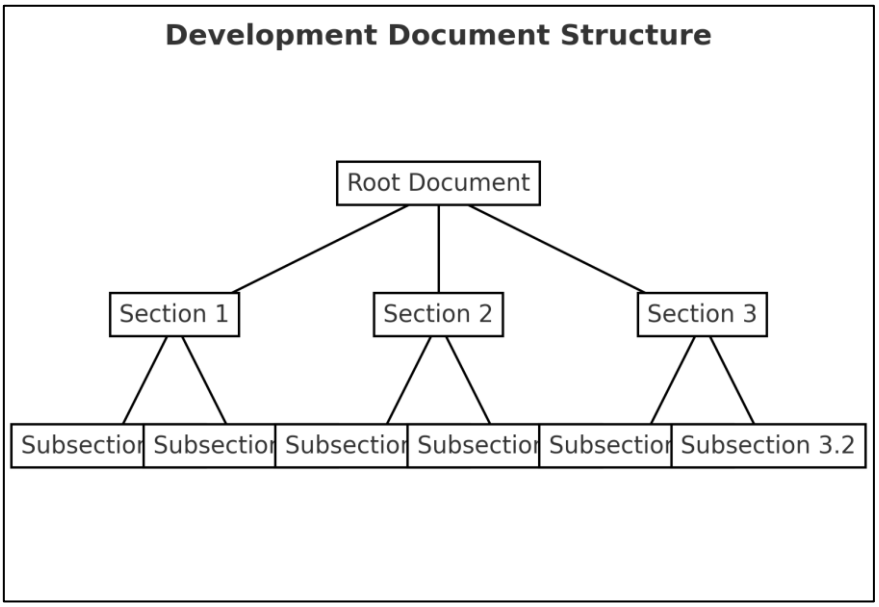

Figure 3-79 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-106 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

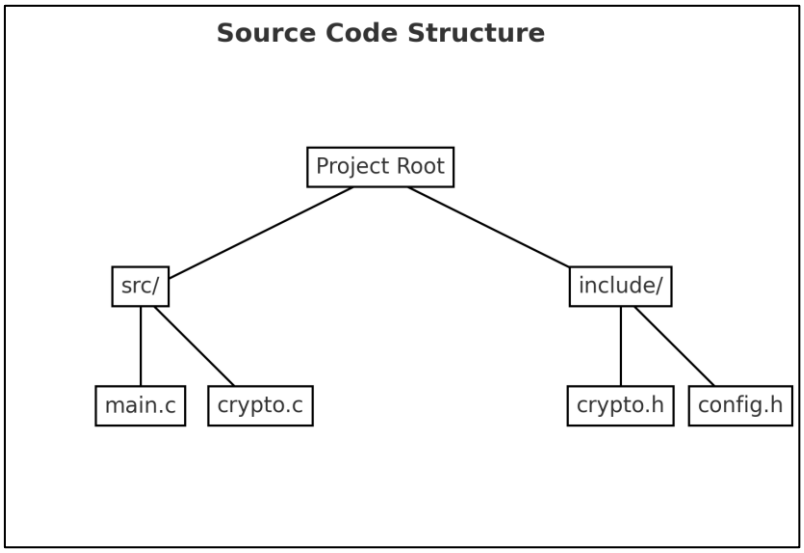

Figure 3-80 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-81 그림 제목

4.2.3 판정근거

Table 3-108 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”>

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 3-109 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

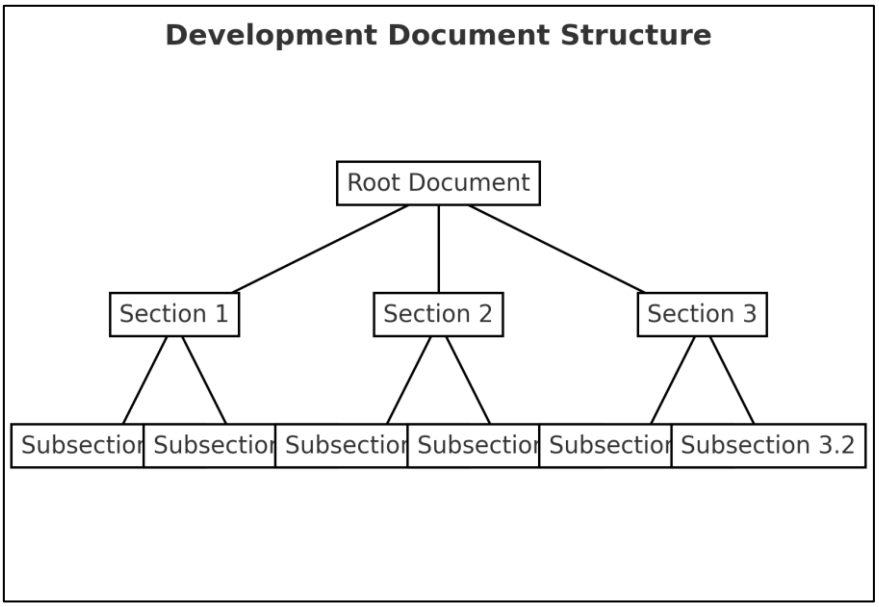

Figure 3-82 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-110 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

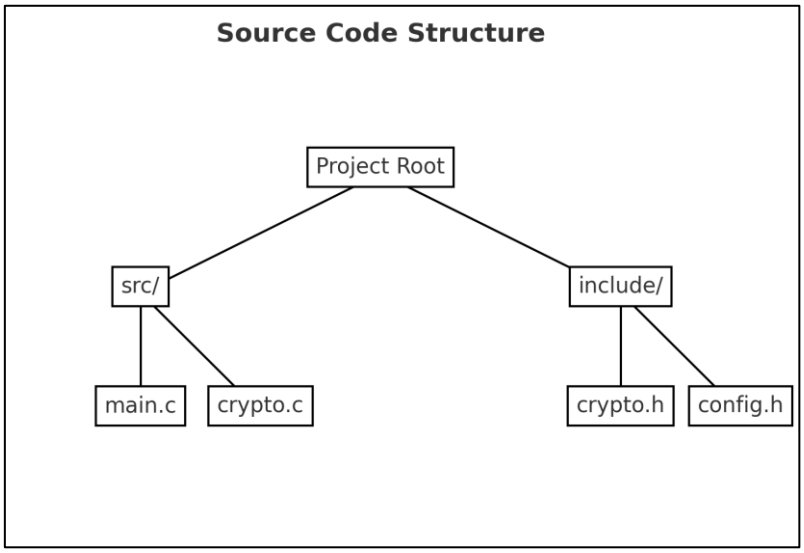

Figure 3-83 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-84 그림 제목

5.2.3 판정근거

Table 3-112 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”>

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	CSP에 대한 보호방법
AS09.02	1, 2	PSP에 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 3-113 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

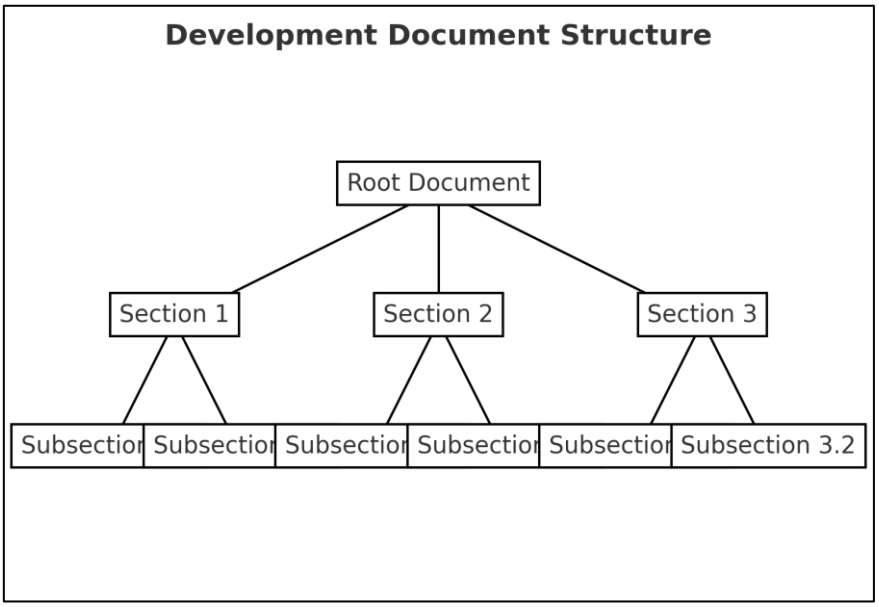

Figure 3-85 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-114 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

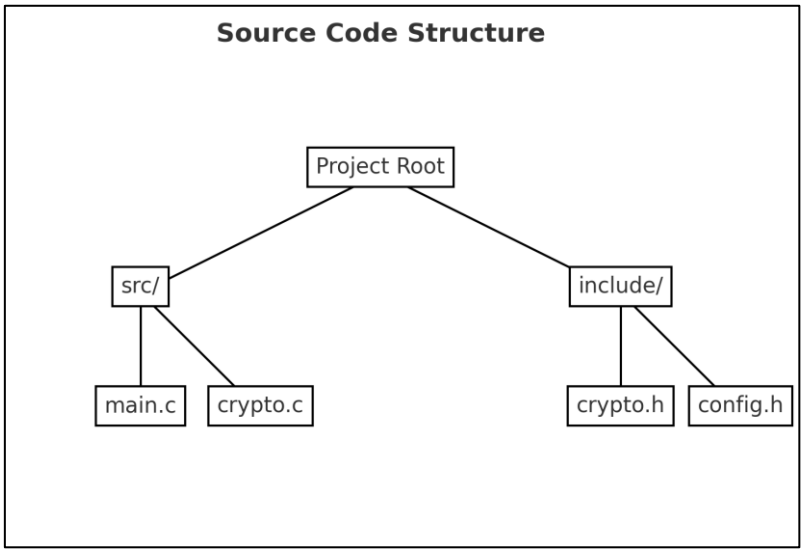

Figure 3-86 그림 제목

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			

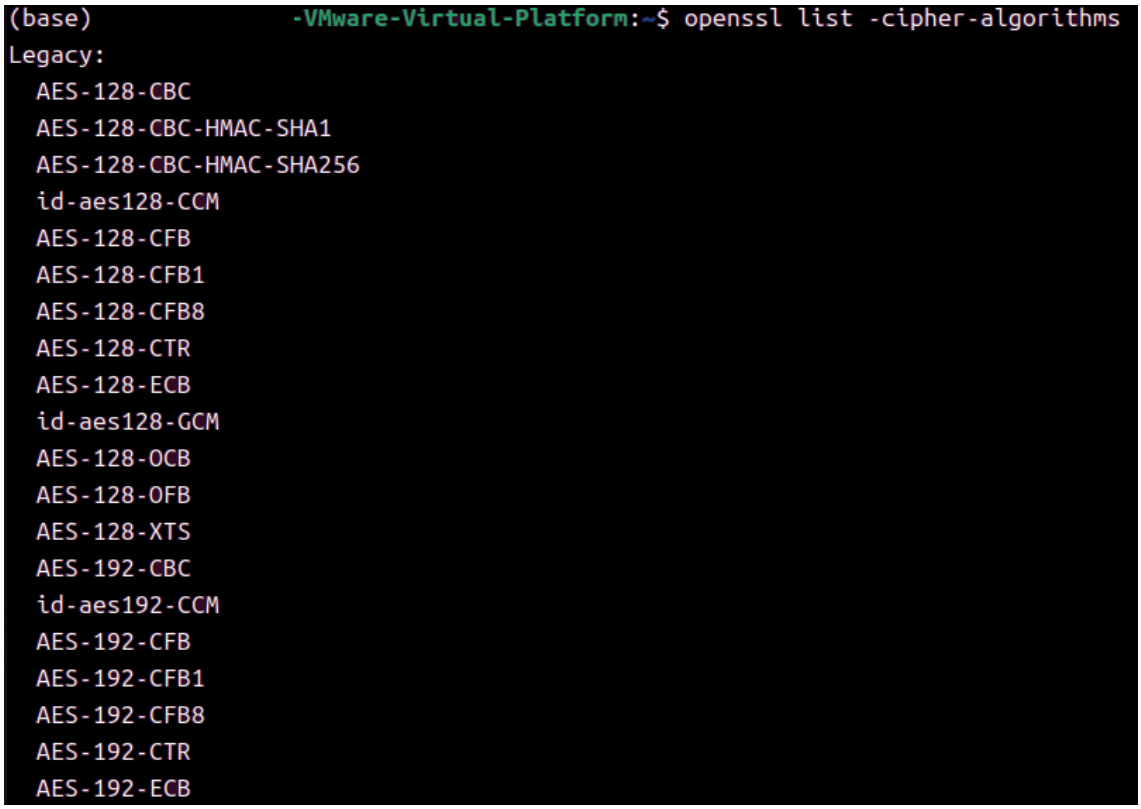

Figure 3-87 그림 제목

6.3.3 판정근거

Table 3-116 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 3-117 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

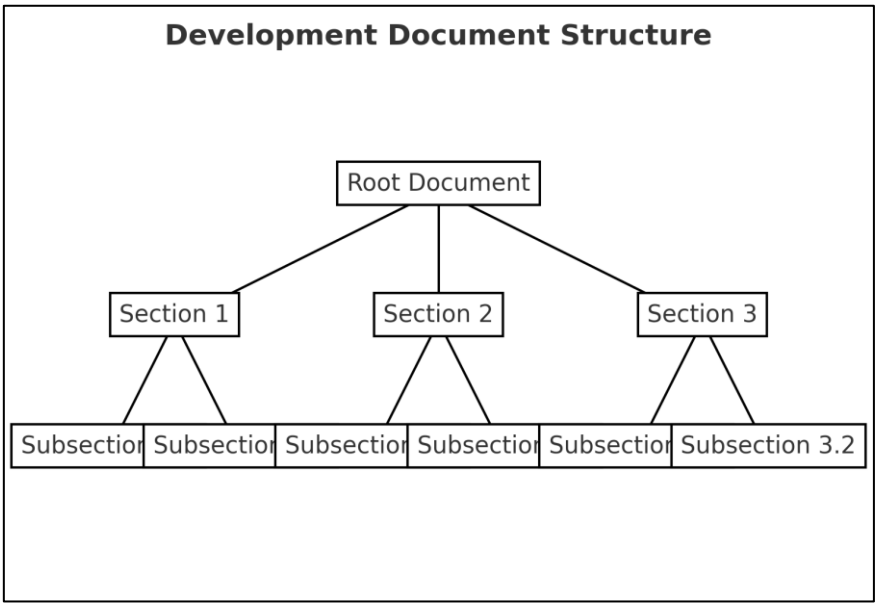

Figure 3-88 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-118 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

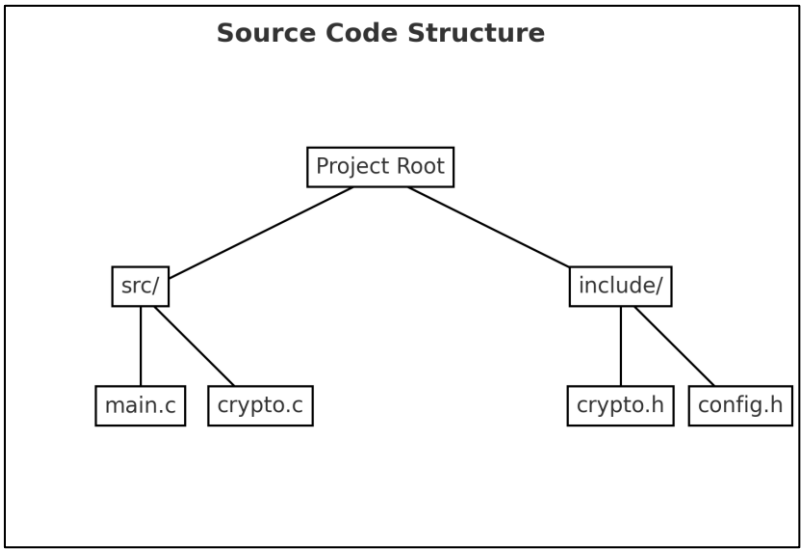

Figure 3-89 그림 제목

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			

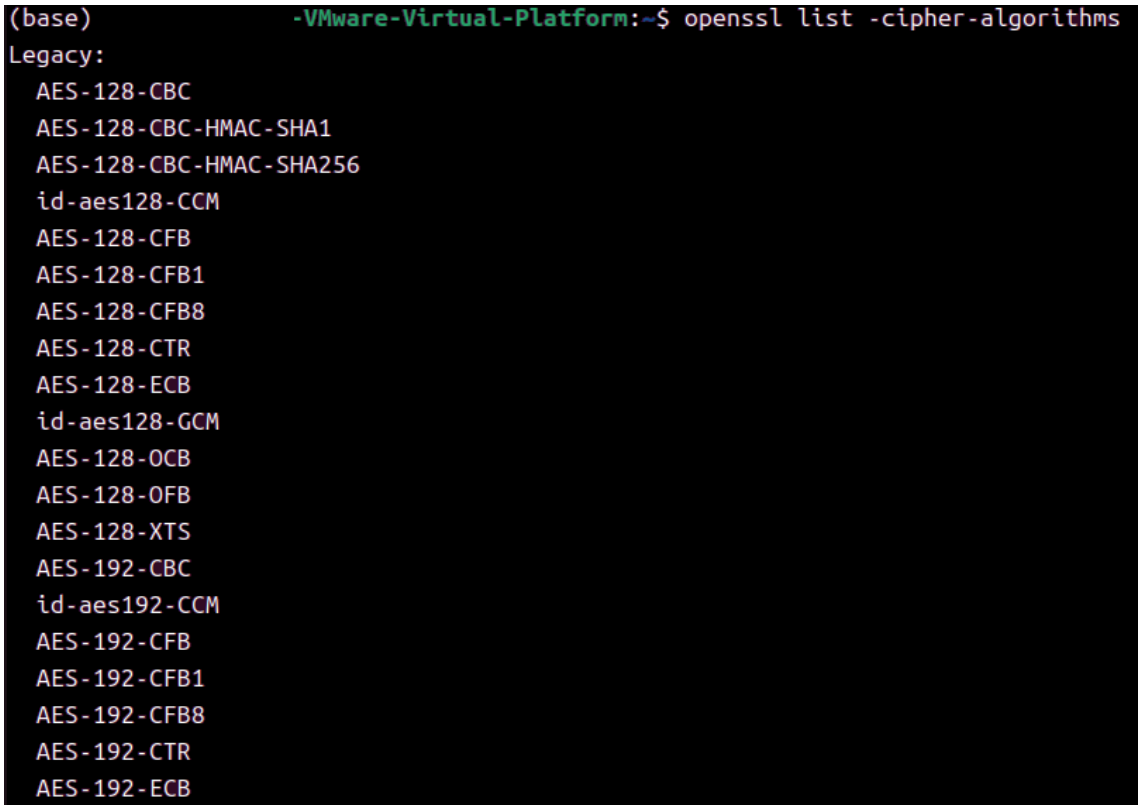

Figure 3-90 그림 제목

6.4.3 판정근거

Table 3-120 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 3-121 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

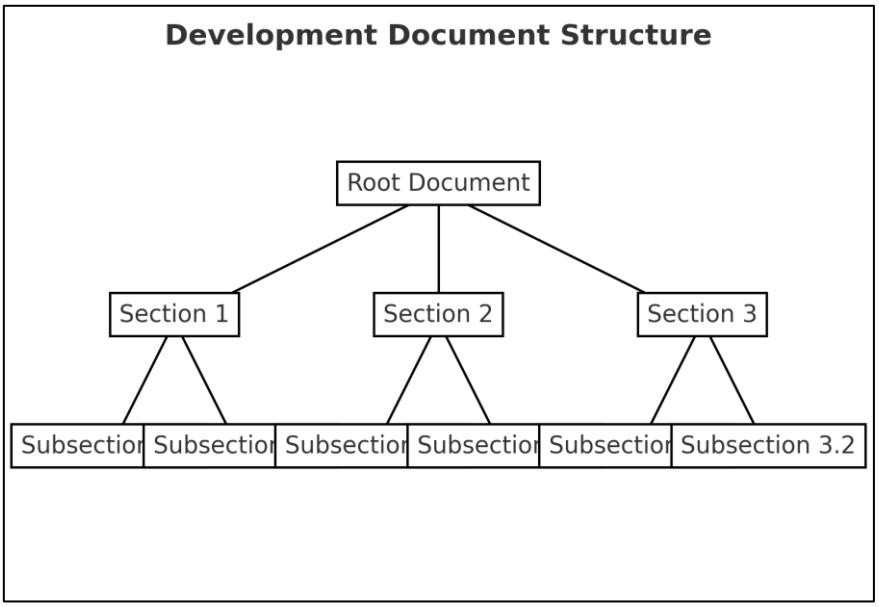

Figure 3-91 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-122 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

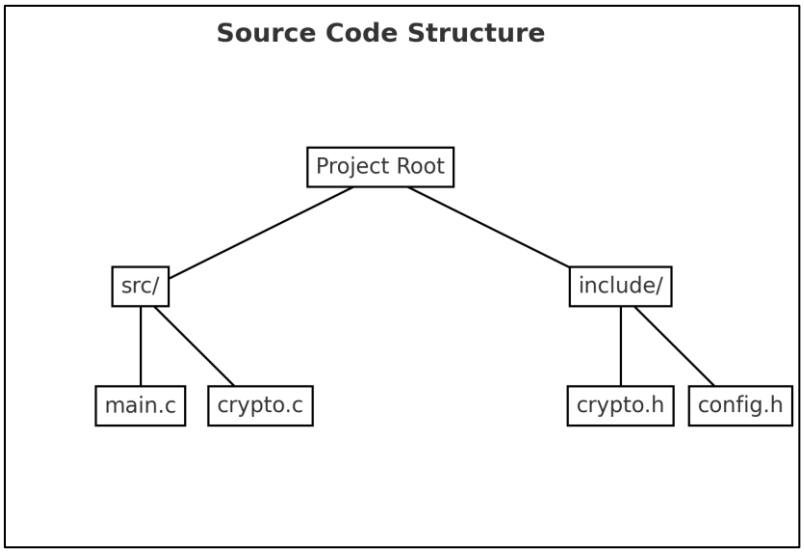

Figure 3-92 그림 제목

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			

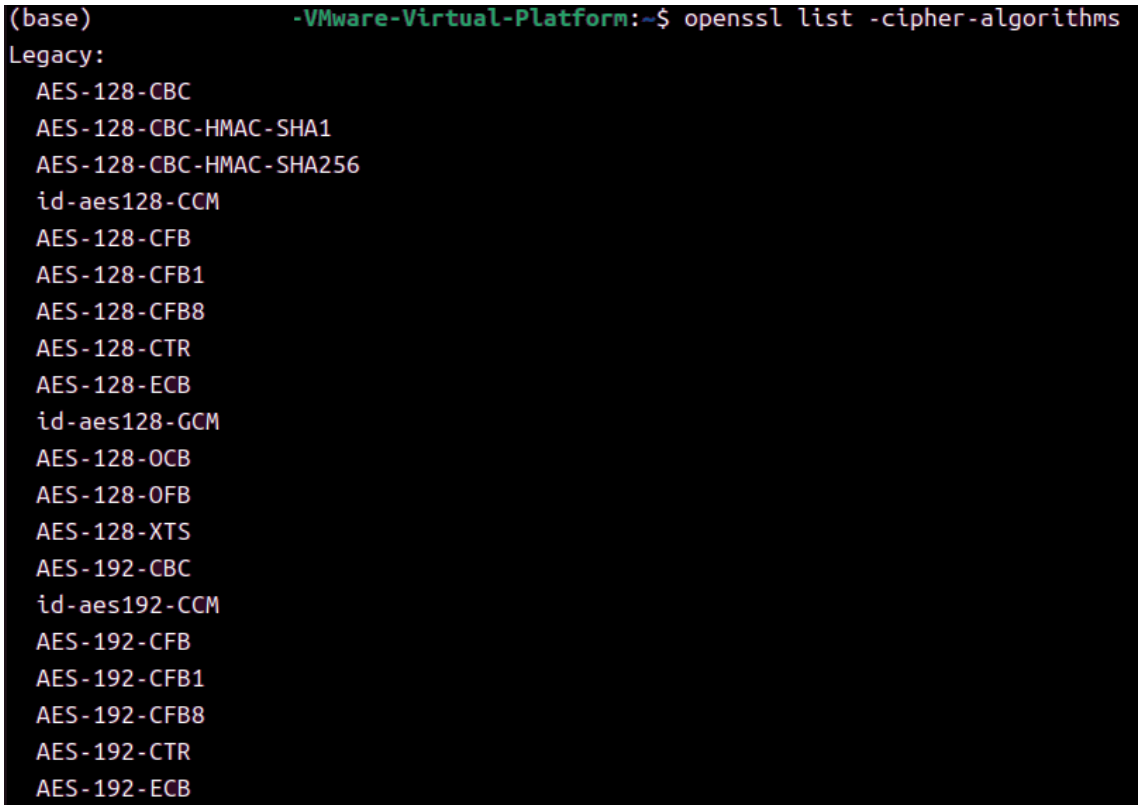

Figure 3-93 그림 제목

6.5.3 판정근거

Table 3-124 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 3-125 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

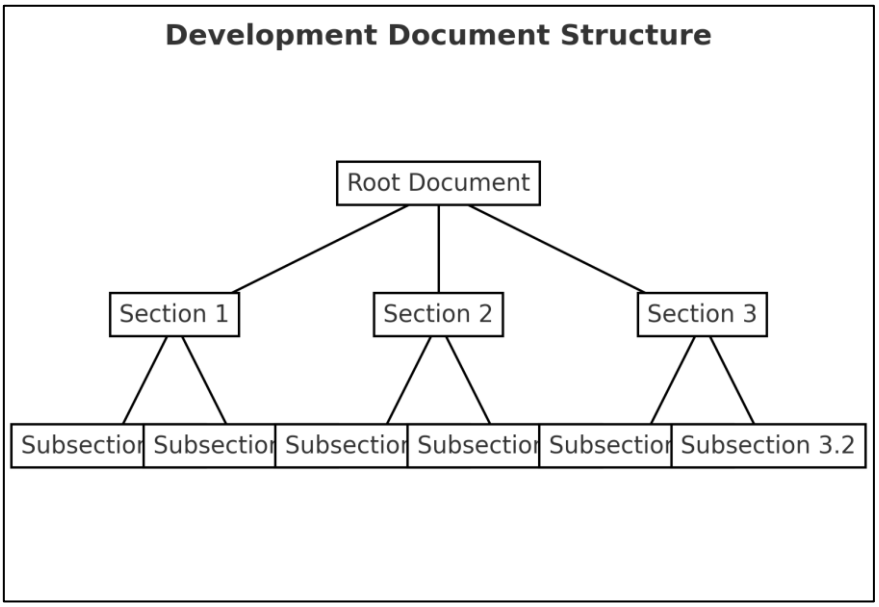

Figure 3-94 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-126 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

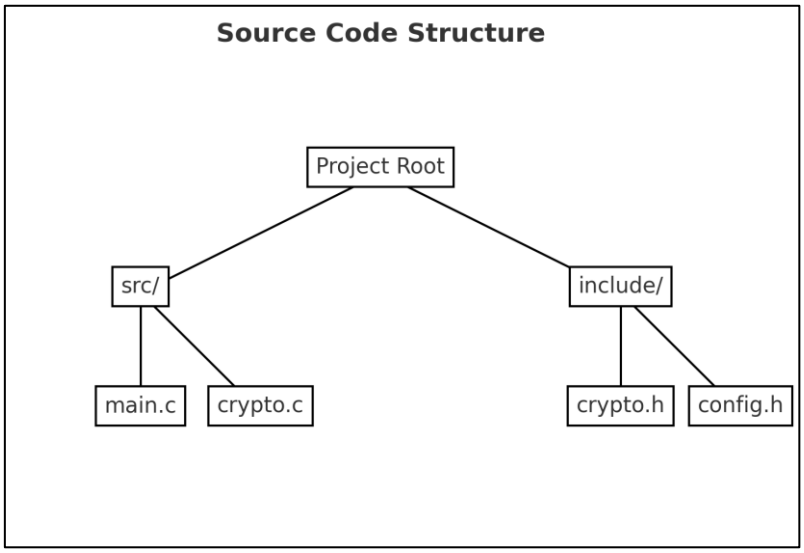

Figure 3-95 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-96 그림 제목

6.6.3 판정근거

Table 3-128 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 3-129 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

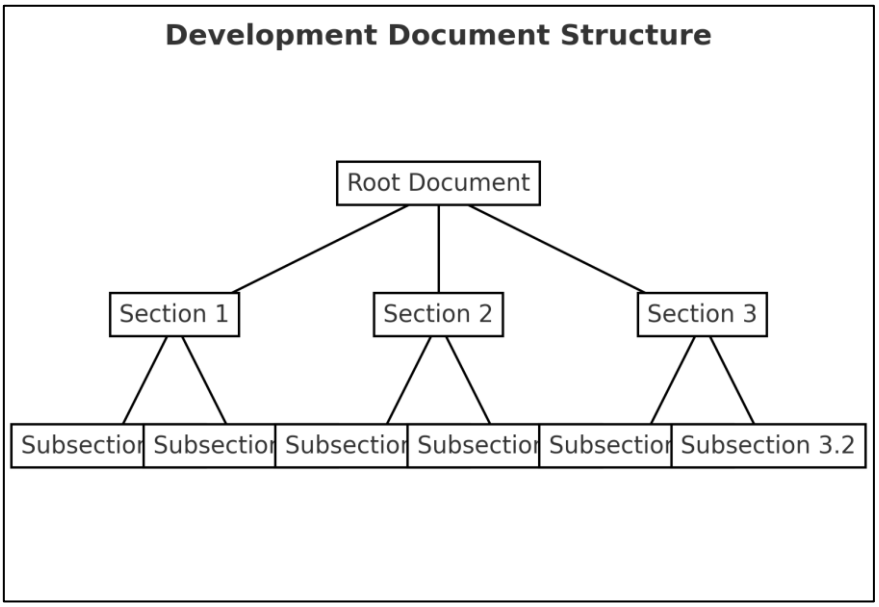

Figure 3-97 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-130 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

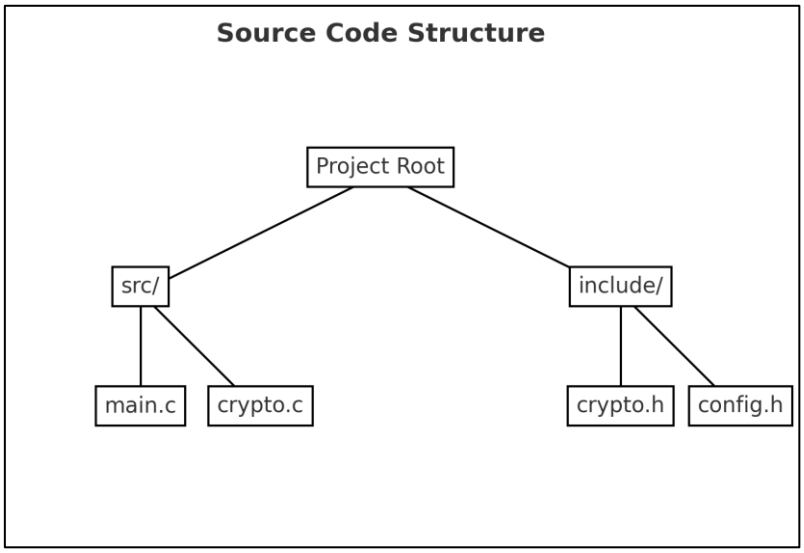

Figure 3-98 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-99 그림 제목

6.7.3 판정근거

Table 3-132 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 3-133 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	○

	CSP	시드	○	X	X	X	X	○
	PSP	공개키 파라미터(e, n)	○	X	X	X	X	○
전자서명	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	○

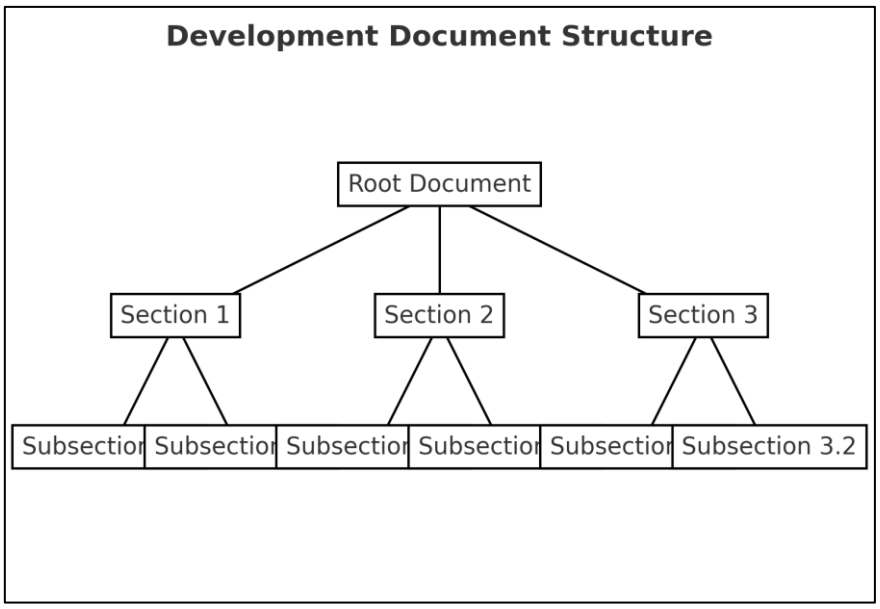

Figure 3-100 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-134 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

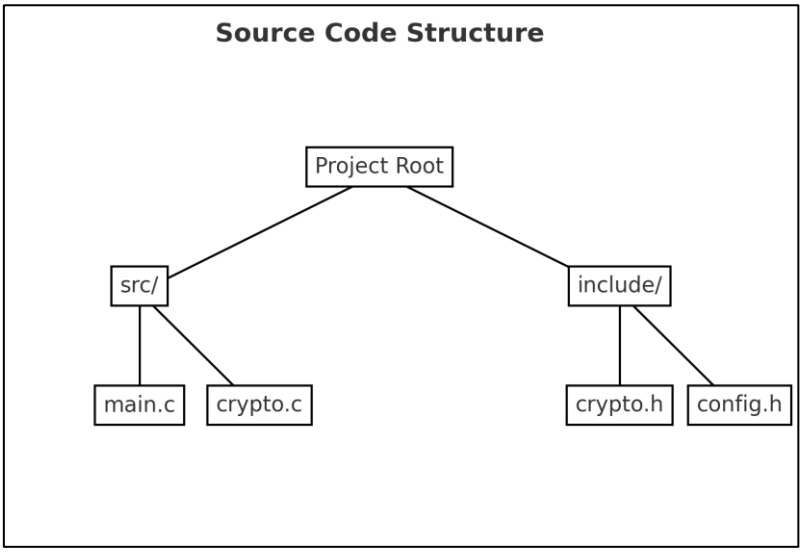

Figure 3-101 그림 제목

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			

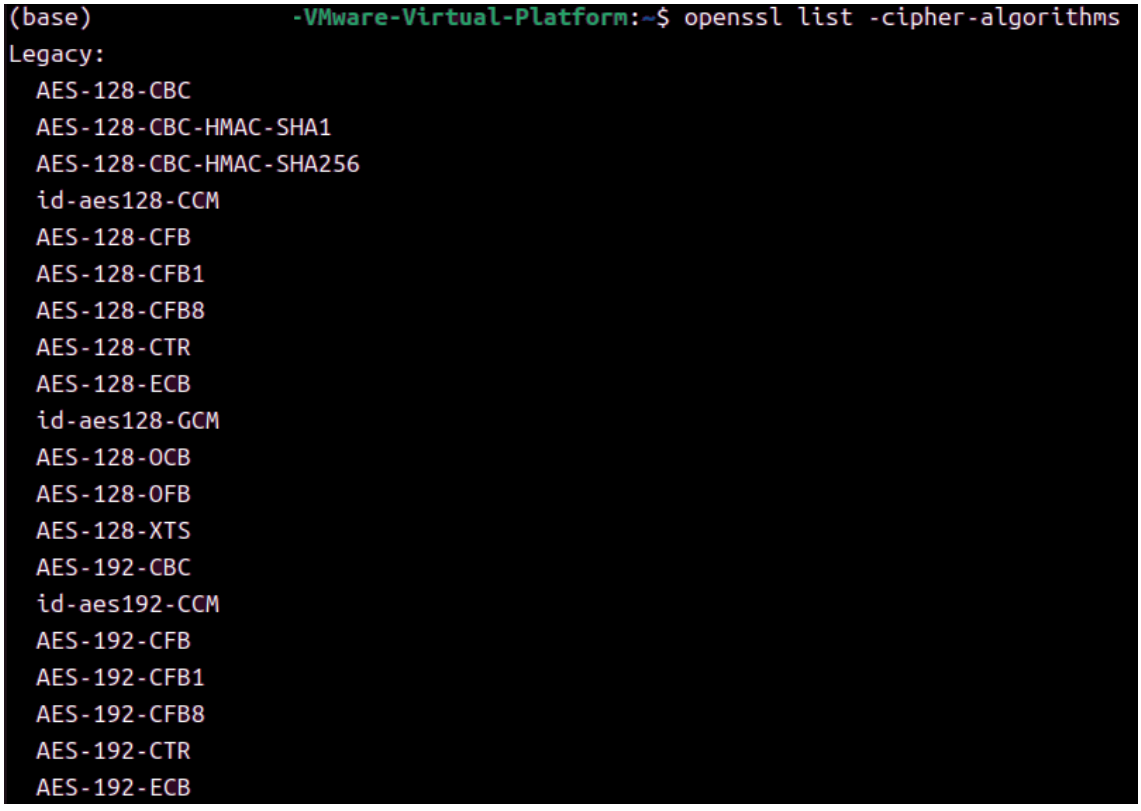

Figure 3-102 그림 제목

6.8.3 판정근거

Table 3-136 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 3-137 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

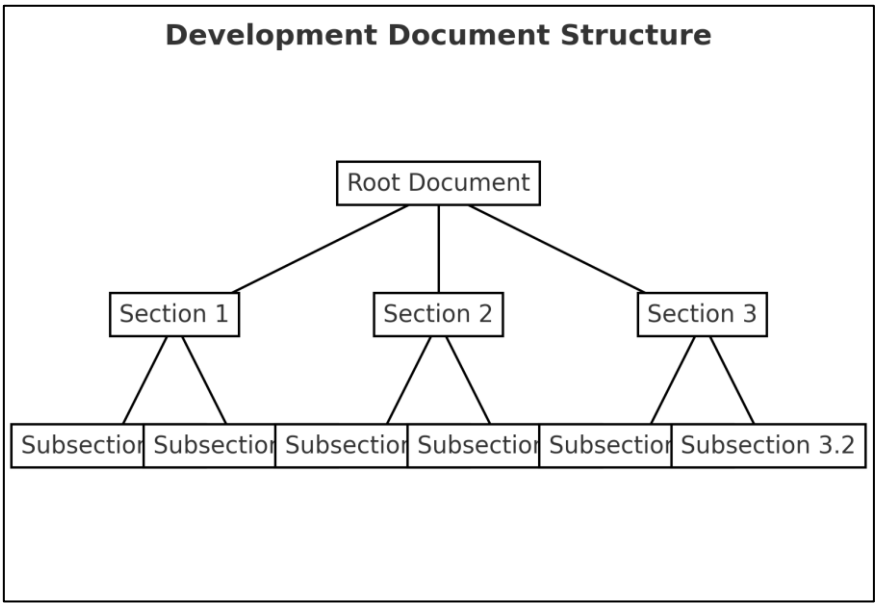

Figure 3-103 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-138 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

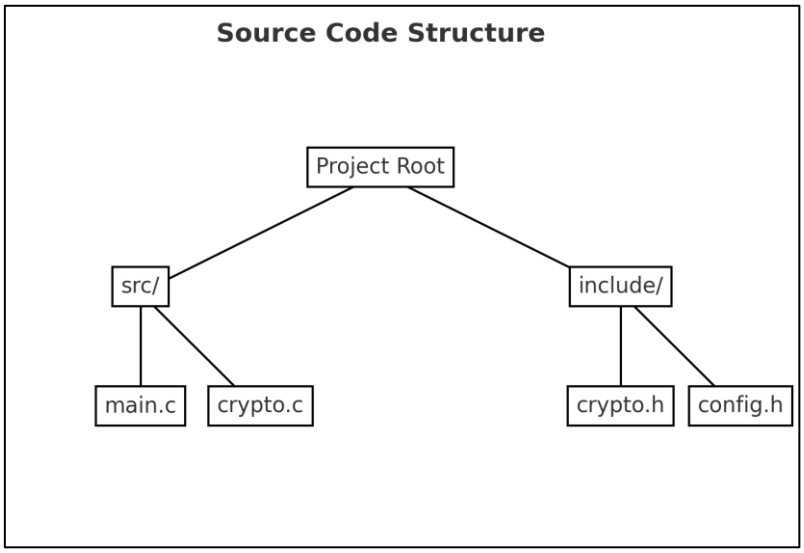

Figure 3-104 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-105 그림 제목

6.9.3 판정근거

Table 3-140 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 3-141 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

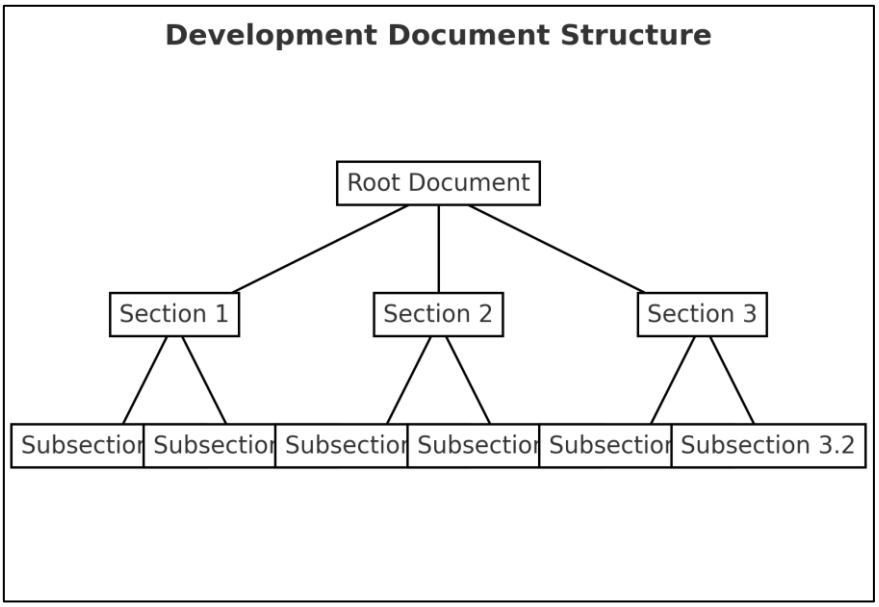

Figure 3-106 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-142 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

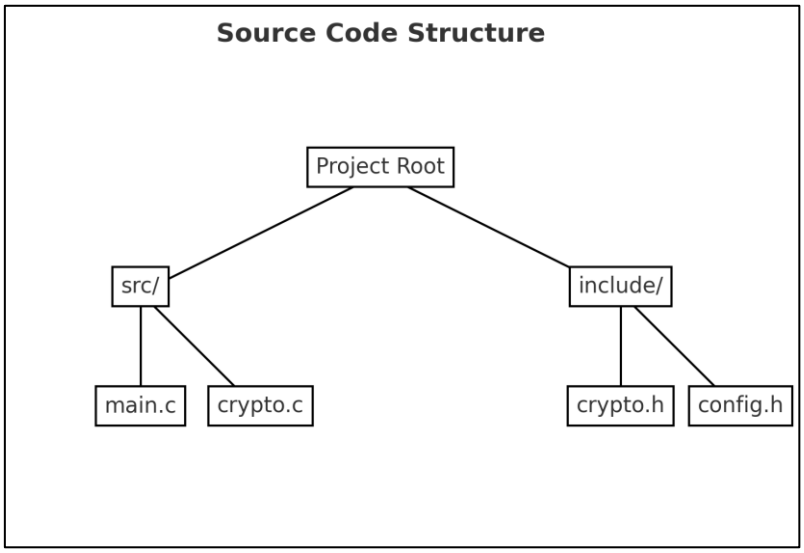

Figure 3-107 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-108 그림 제목

6.10.3 판정근거

Table 3-144 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 3-145 표 제목

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

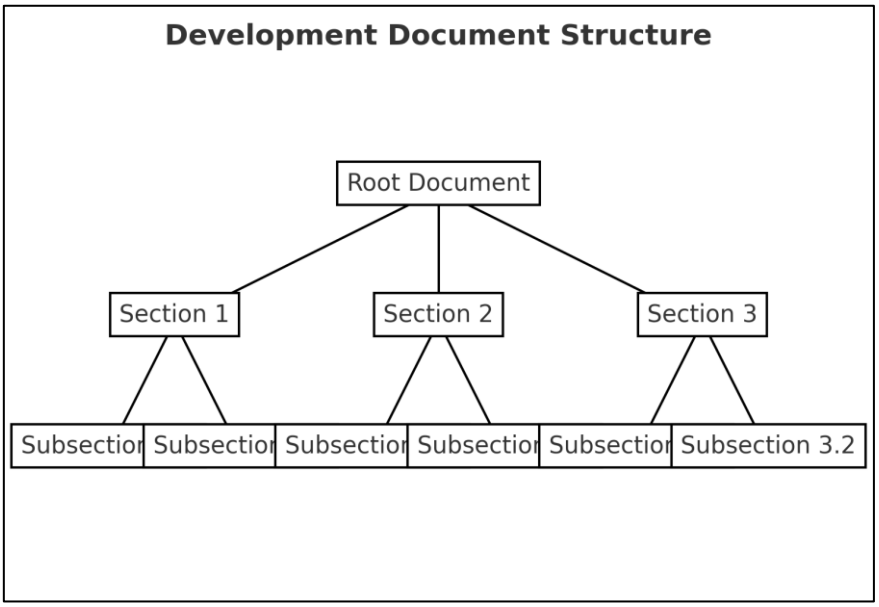

Figure 3-109 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-146 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

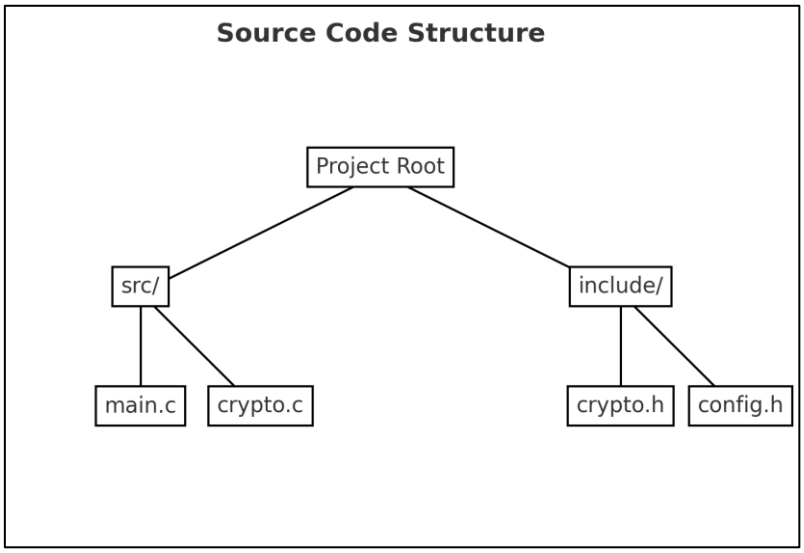

Figure 3-110 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-111 그림 제목

6.11.3 판정근거

Table 3-148 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 3-149 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

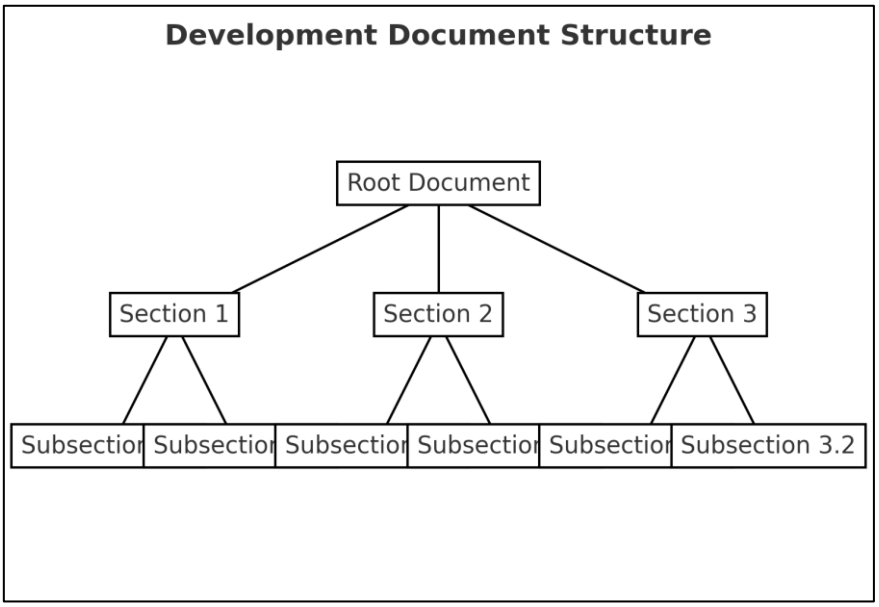

Figure 3-112 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-150 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

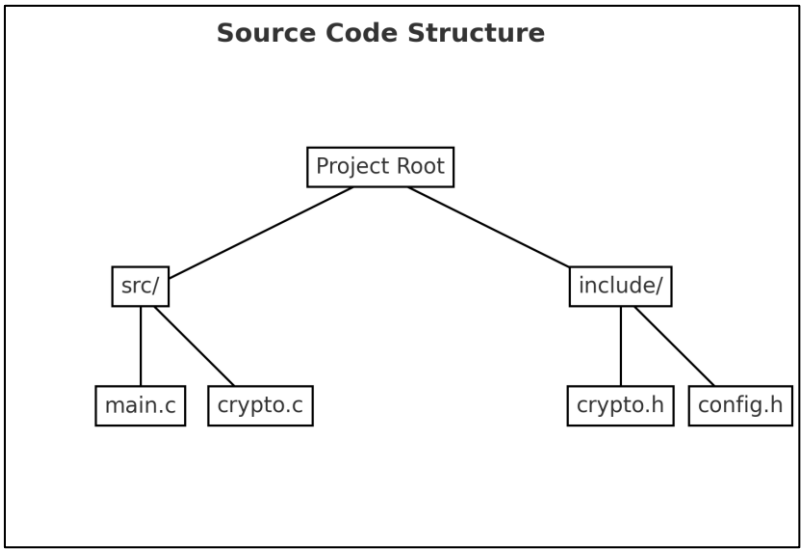

Figure 3-113 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-114 그림 제목

6.12.3 판정근거

Table 3-152 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 3-153 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

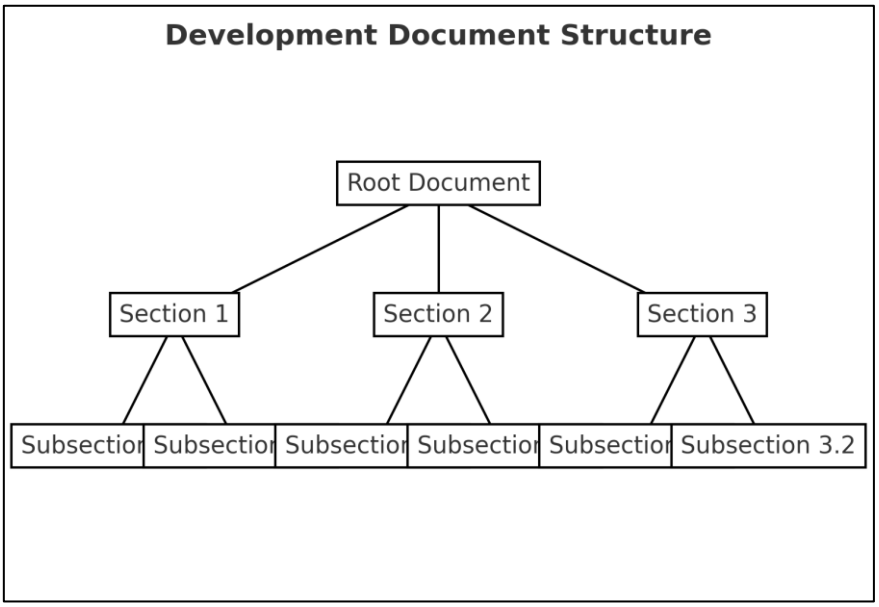

Figure 3-115 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-154 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

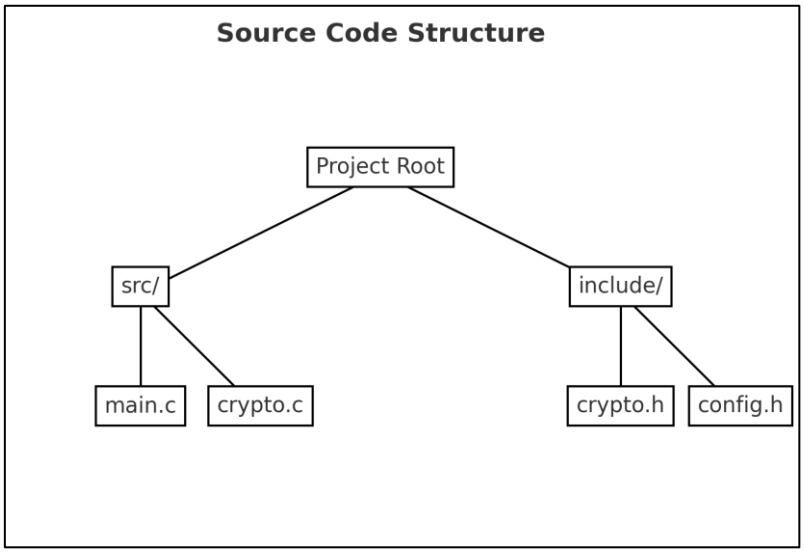

Figure 3-116 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-117 그림 제목

6.13.3 판정근거

Table 3-156 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 3-157 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

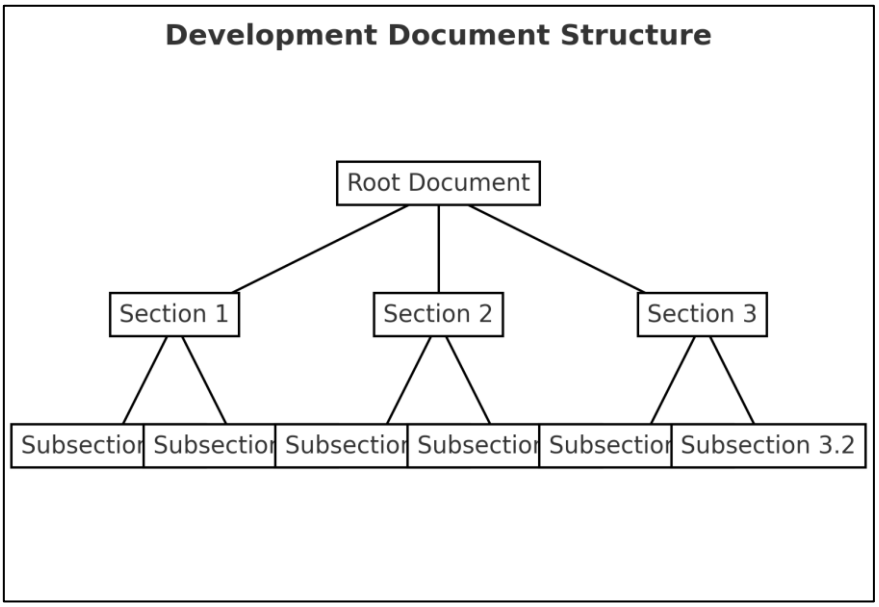

Figure 3-118 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-158 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

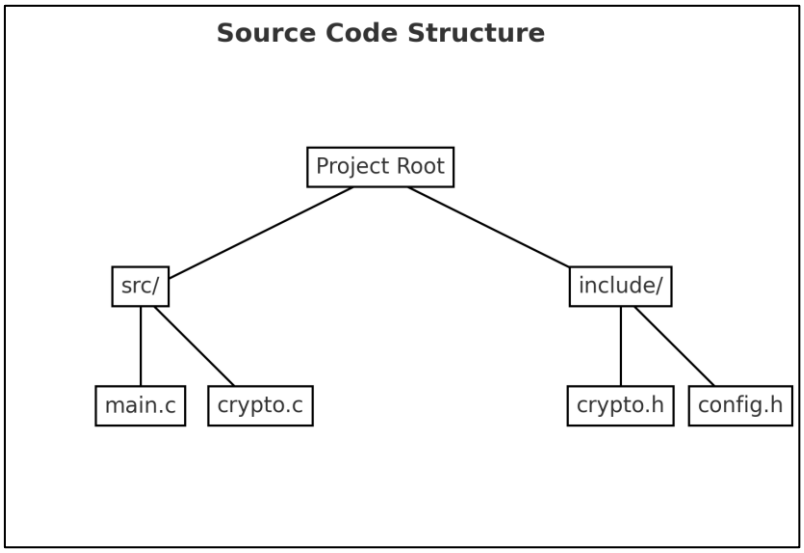

Figure 3-119 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-120 그림 제목

6.14.3 판정근거

Table 3-160 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 3-161 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

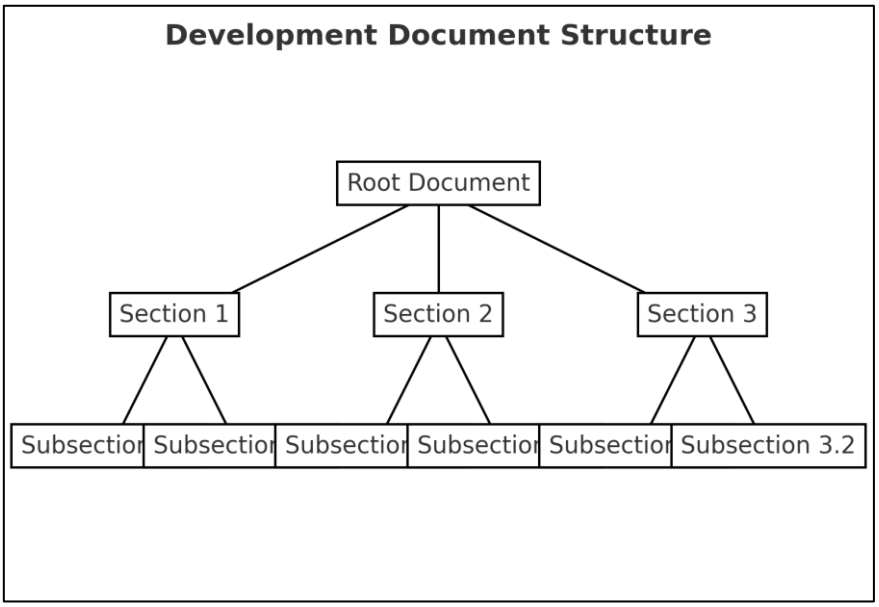

Figure 3-121 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-162 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

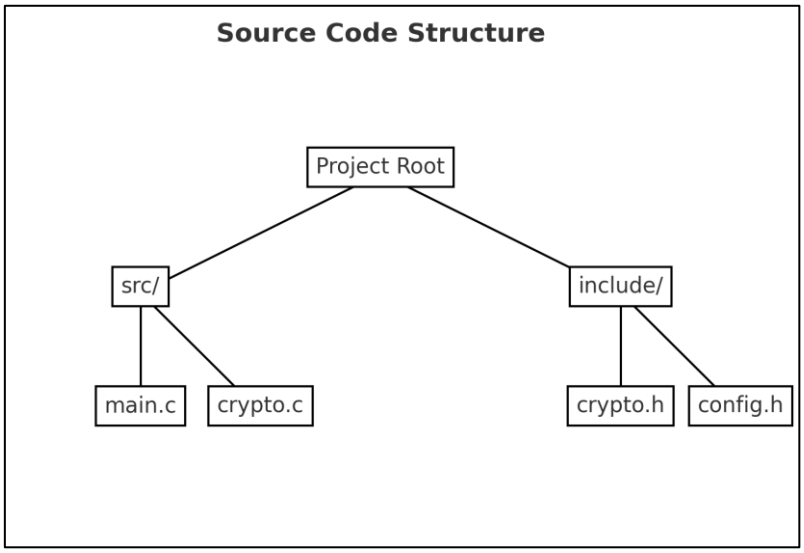

Figure 3-122 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-123 그림 제목

6.15.3 판정근거

Table 3-164 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 3-165 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

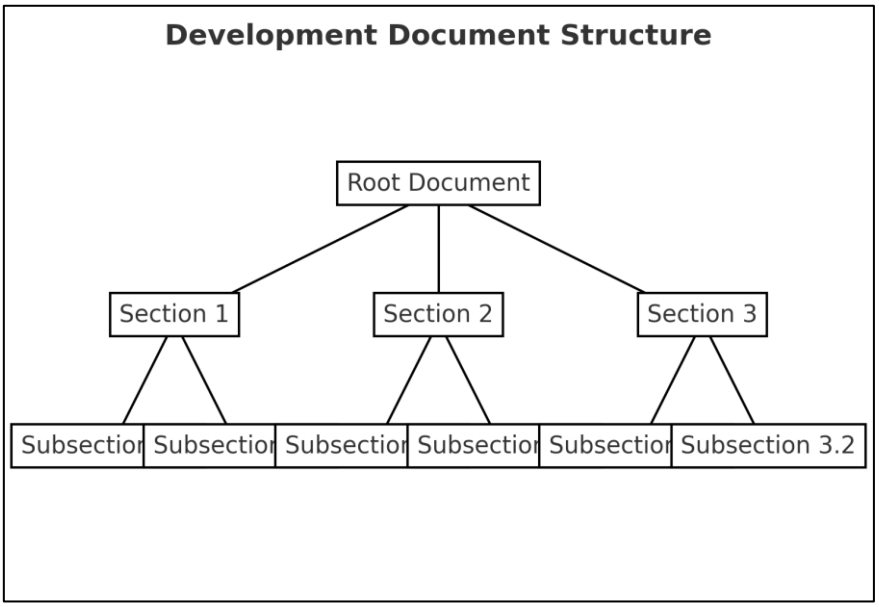

Figure 3-124 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-166 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

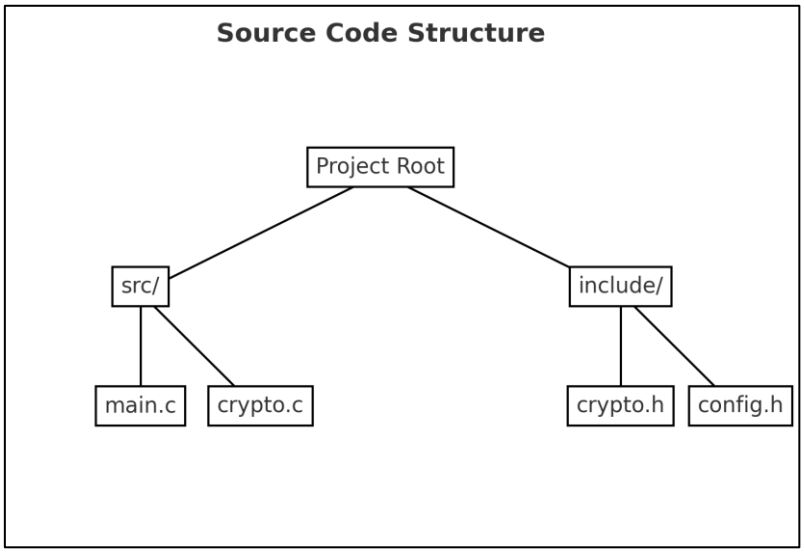

Figure 3-125 그림 제목

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			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-126 그림 제목

6.16.3 판정근거

Table 3-168 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 3-169 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

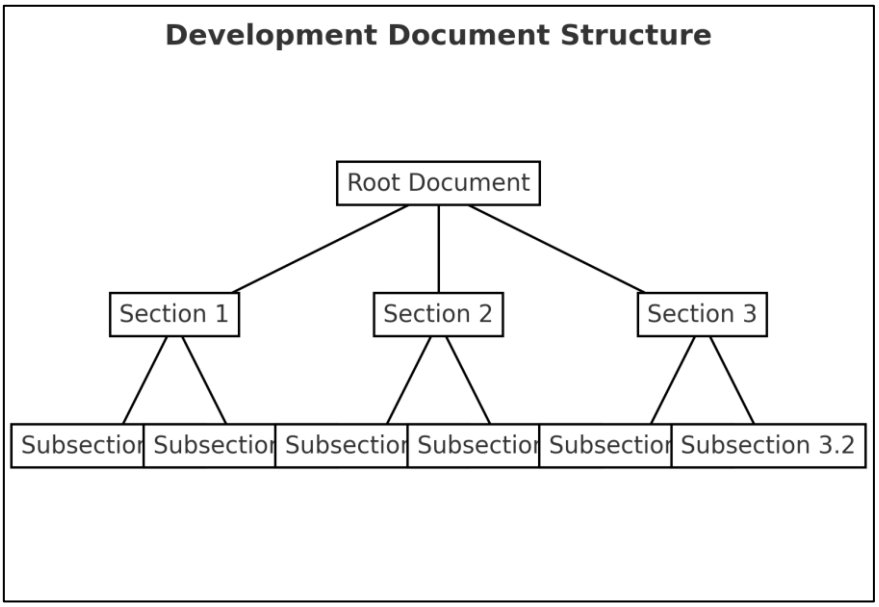

Figure 3-127 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-170 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-128 그림 제목

Table 3-171 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

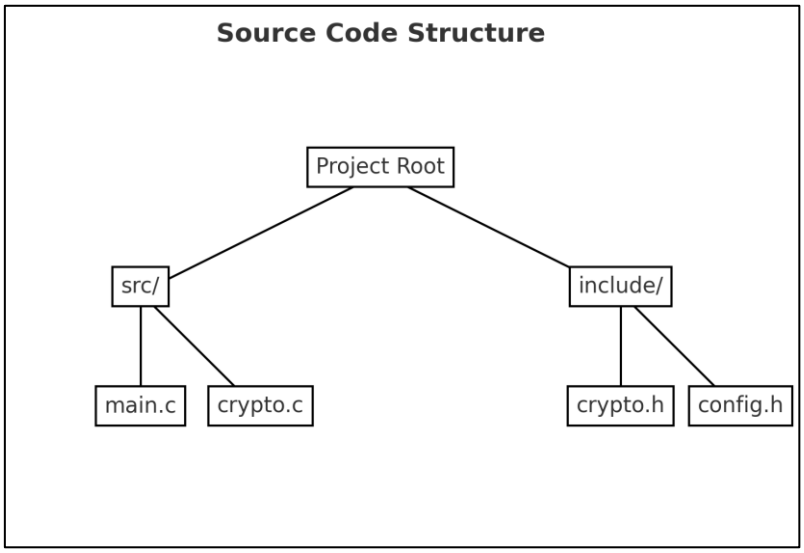

Figure 3-129 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-172 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-130 그림 제목

6.17.3 판정근거

Table 3-173 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 3-174 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

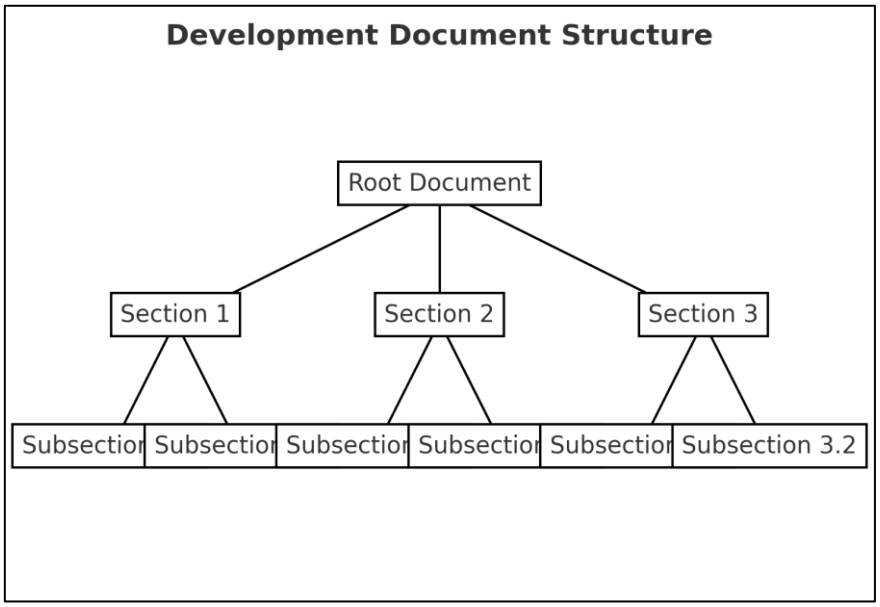

Figure 3-131 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-175 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

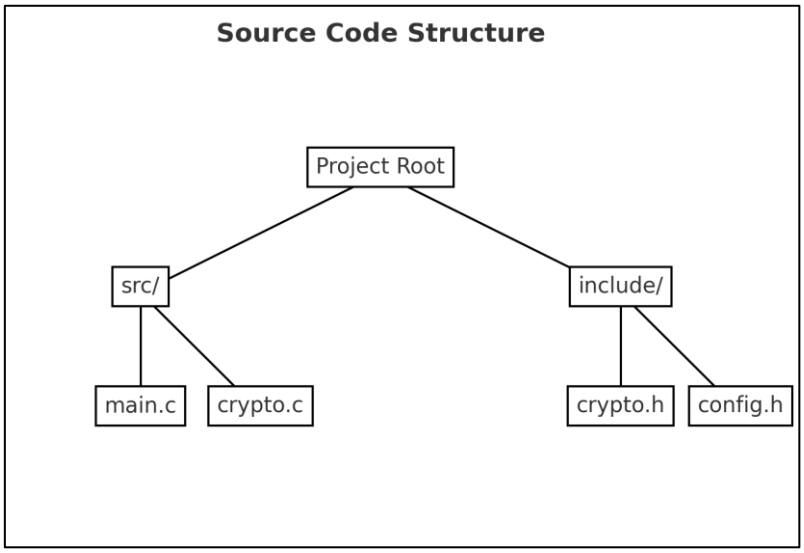

Figure 3-132 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-176 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

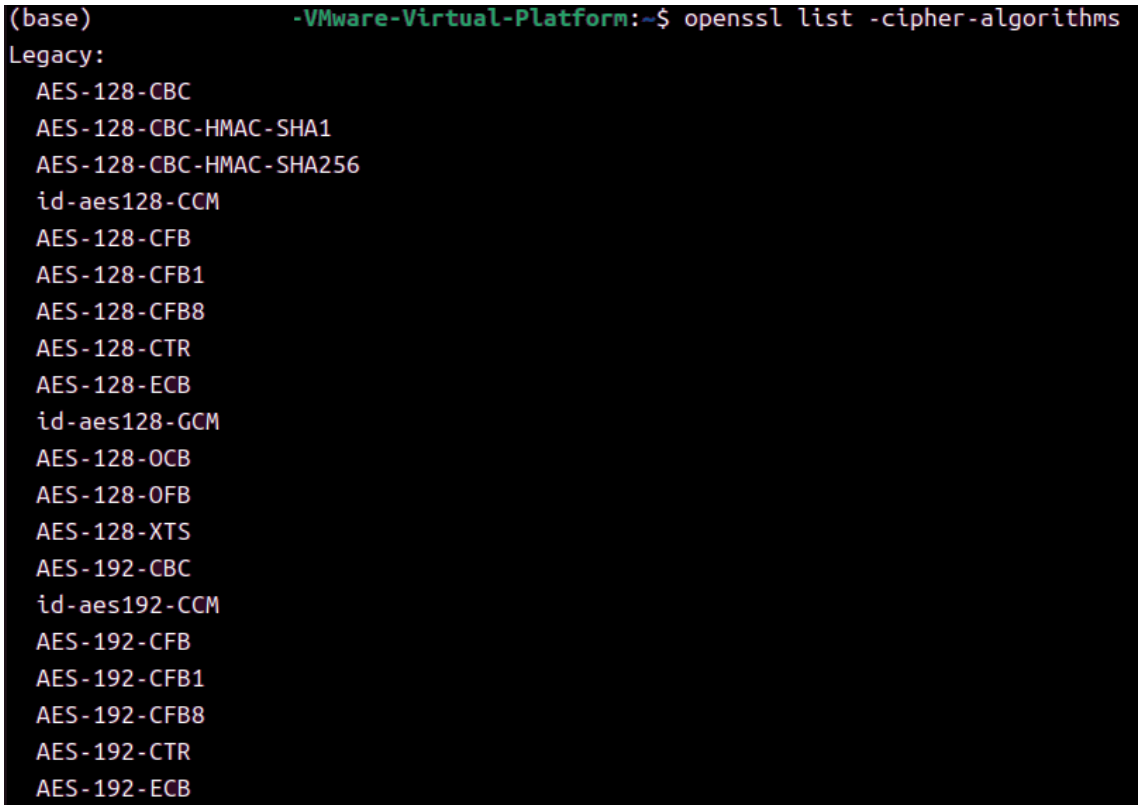

Figure 3-133 그림 제목

6.18.3 판정근거

Table 3-177 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 3-178 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

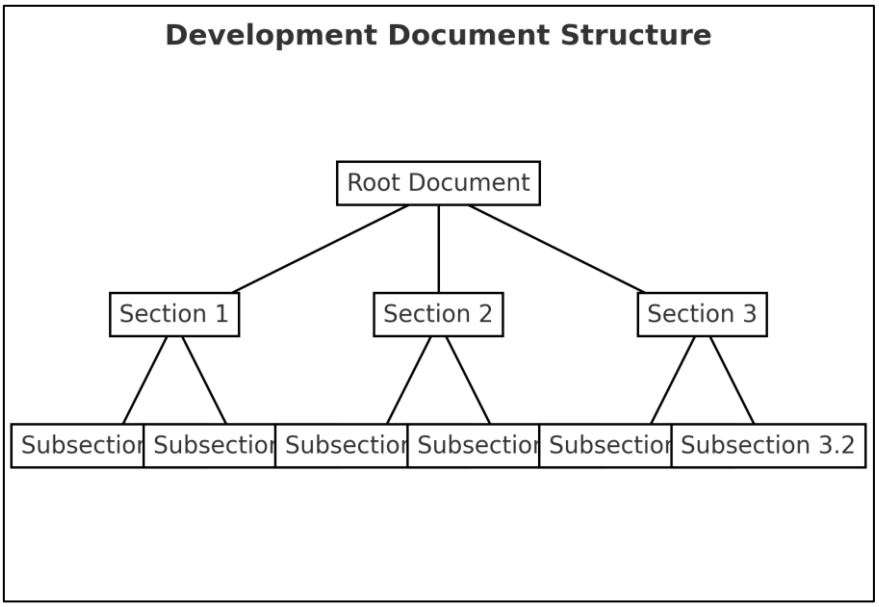

Figure 3-134 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-179 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

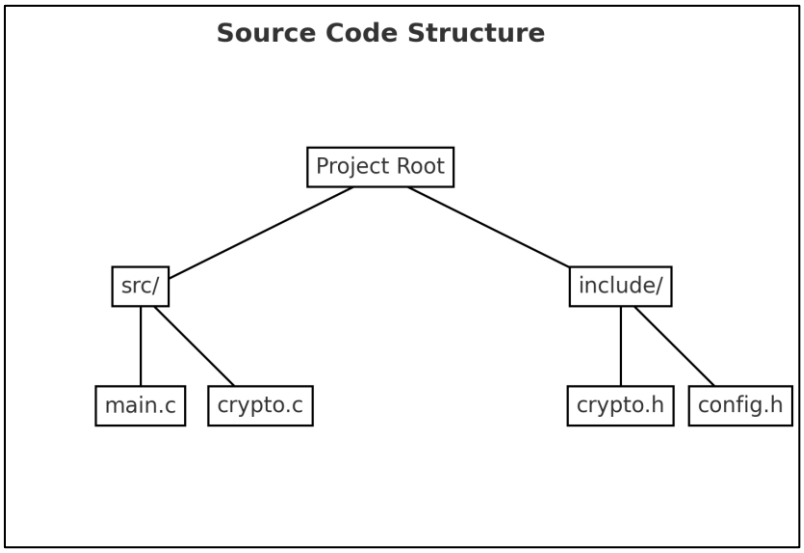

Figure 3-135 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-180 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

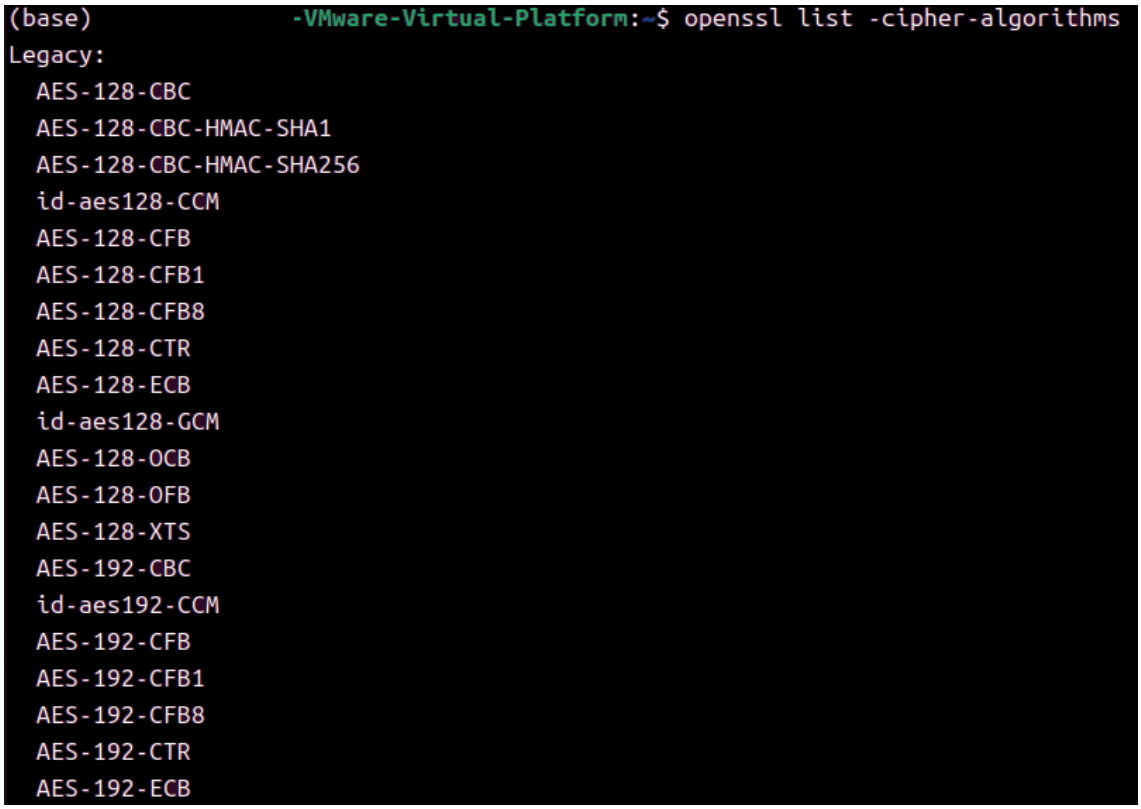

Figure 3-136 그림 제목

6.19.3 판정근거

Table 3-181 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 3-182 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

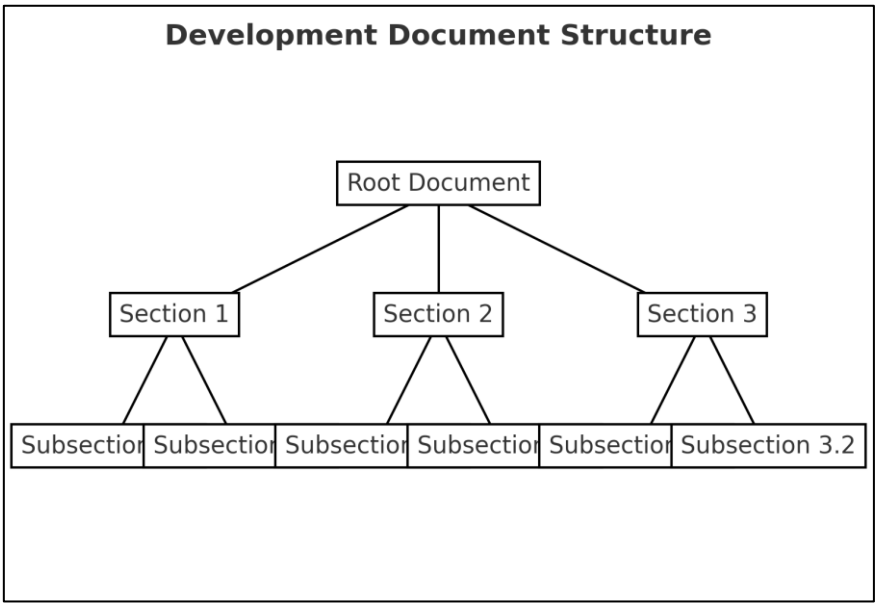

Figure 3-137 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-183 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

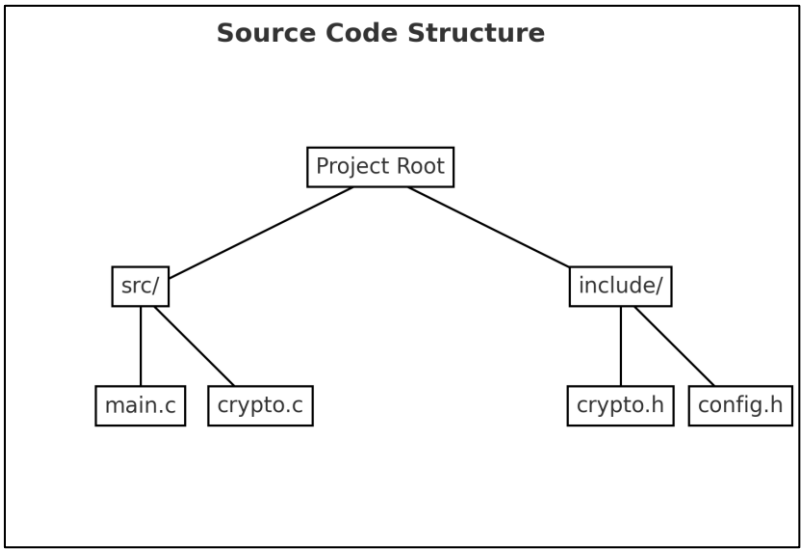

Figure 3-138 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-184 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-139 그림 제목

6.20.3 판정근거

Table 3-185 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 3-186 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

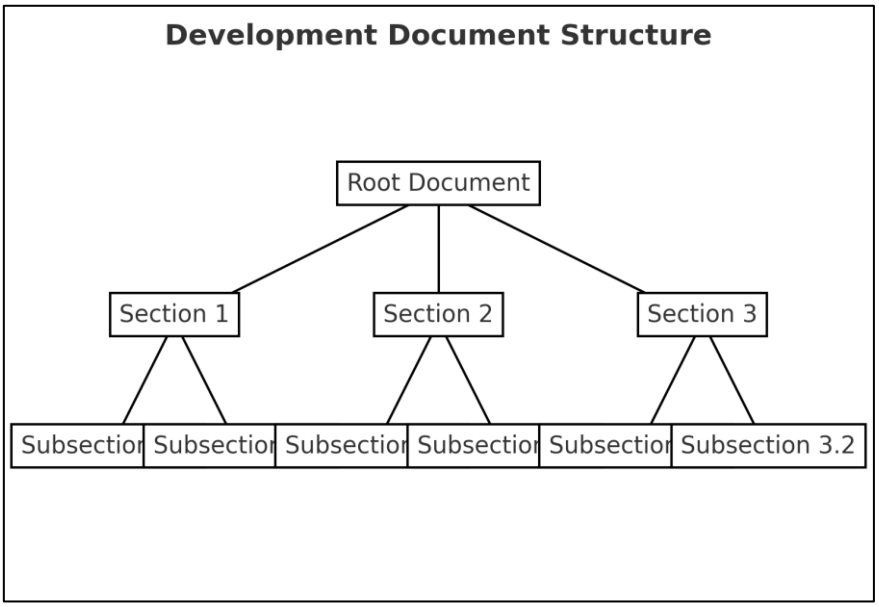

Figure 3-140 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-187 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

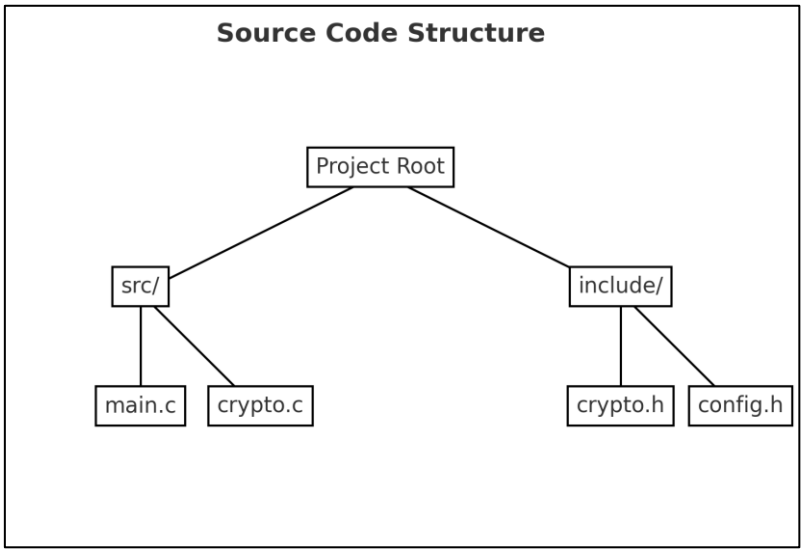

Figure 3-141 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-188 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

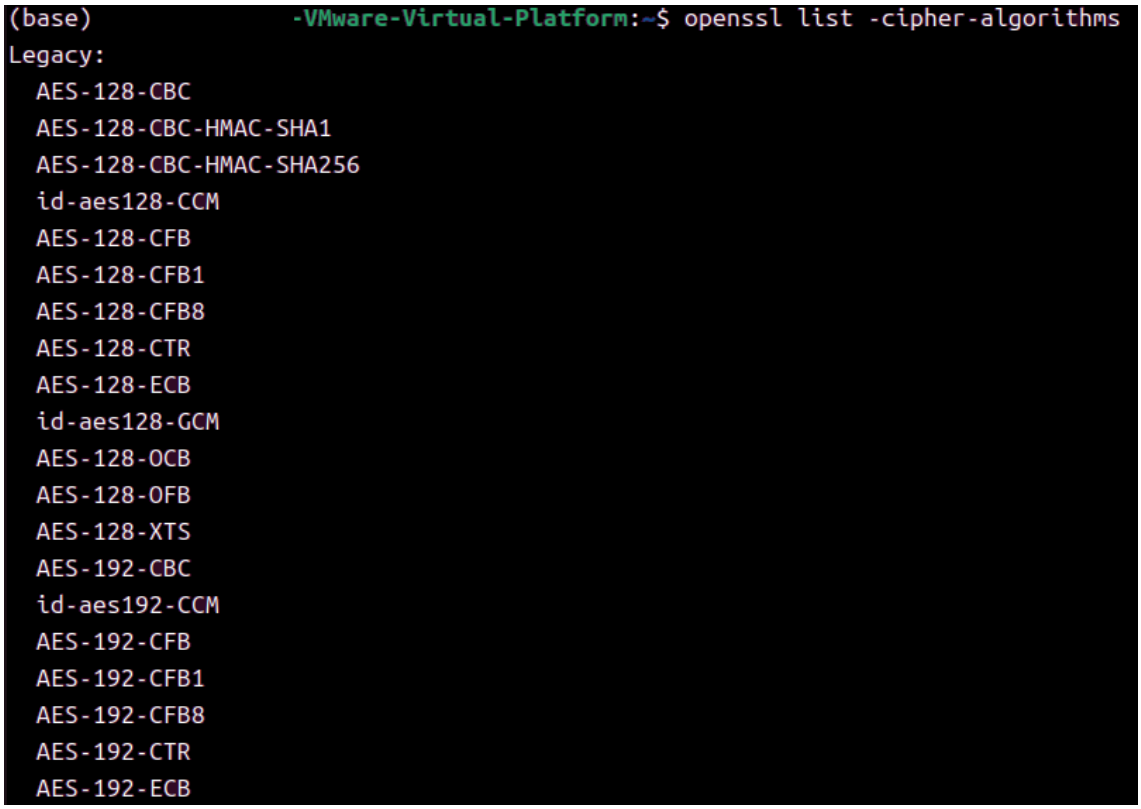

Figure 3-142 그림 제목

6.21.3 판정근거

Table 3-189 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 3-190 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

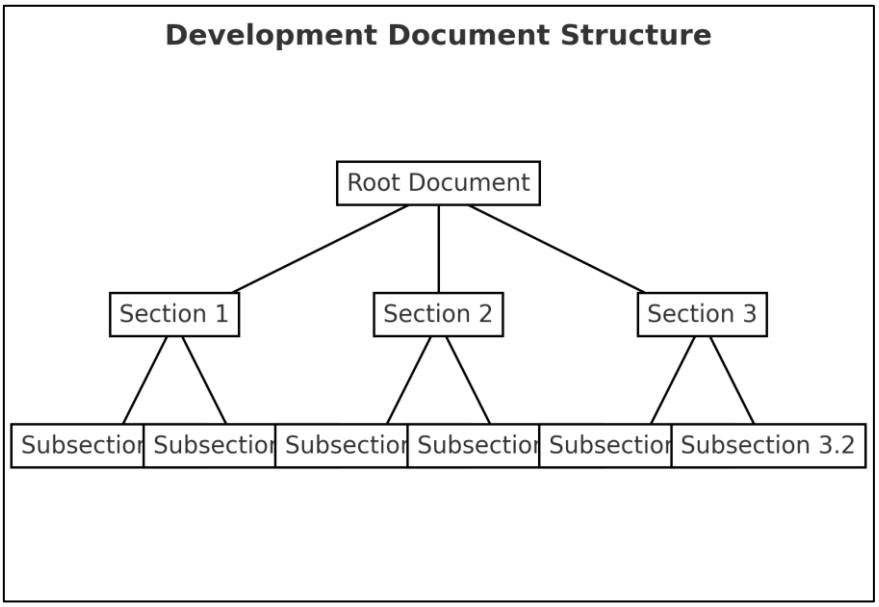

Figure 3-143 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-191 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

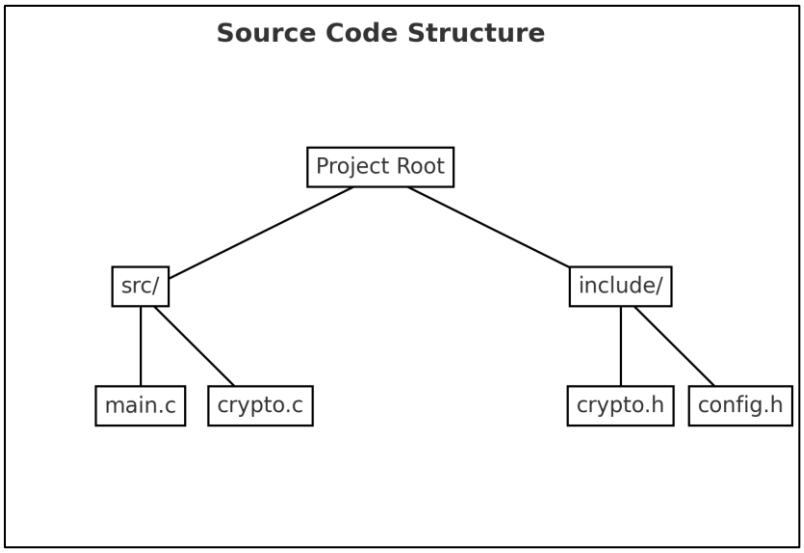

Figure 3-144 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-192 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-145 그림 제목

6.22.3 판정근거

Table 3-193 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	동작 전 및 조건부 자가시험 목록	개발문서 검토

7.2.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-194 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

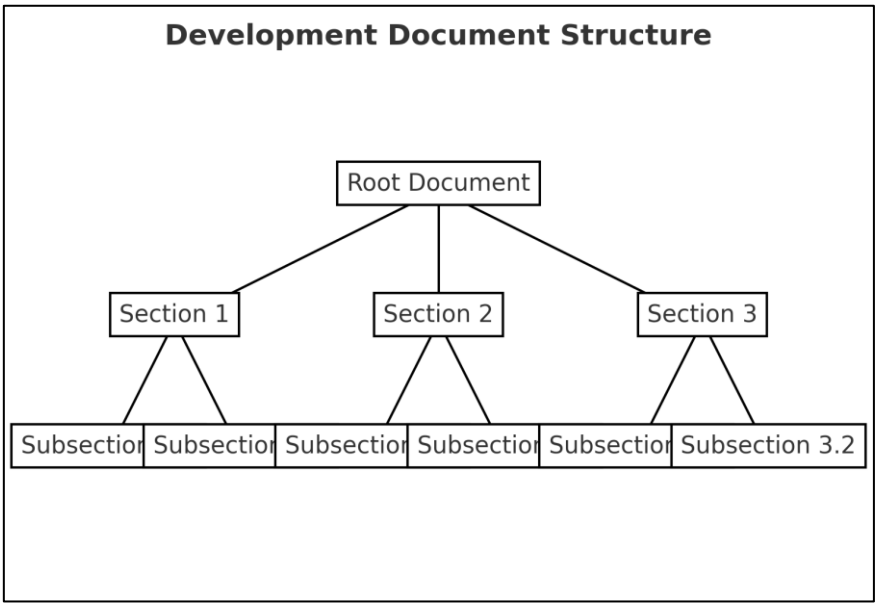

Figure 3-146 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-195 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

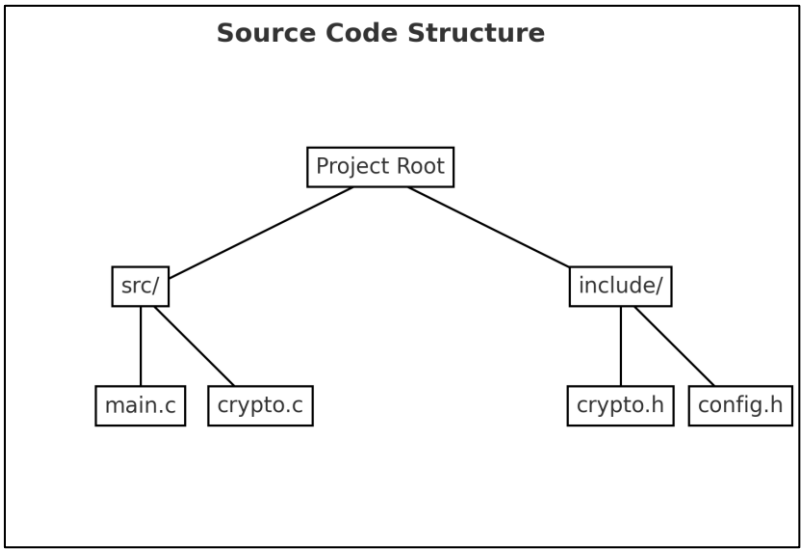

Figure 3-147 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-196 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-148 그림 제목

7.2.3 판정근거

Table 3-197 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”>

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

8.3 TE11.01.01

8.3.1 시험 요구사항

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

8.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-198 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

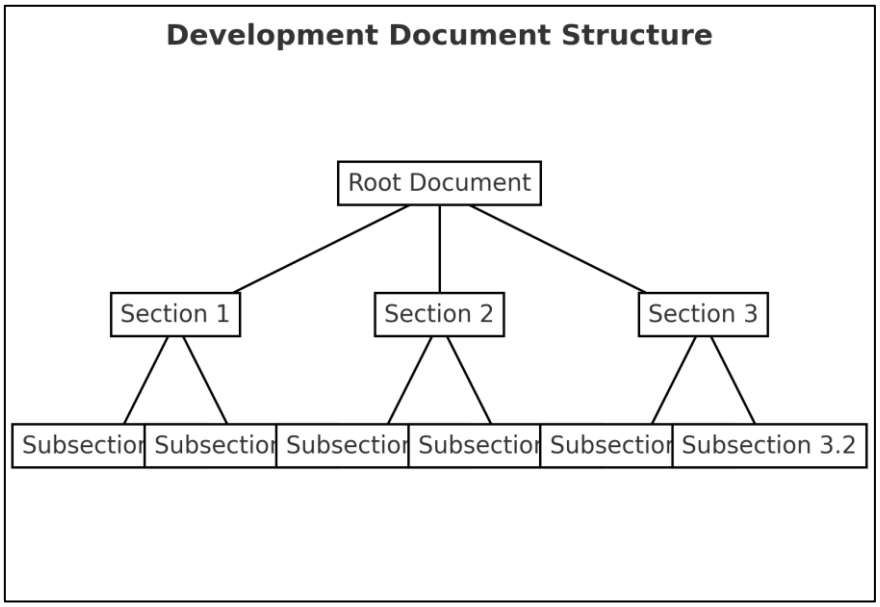

Figure 3-149 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-199 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

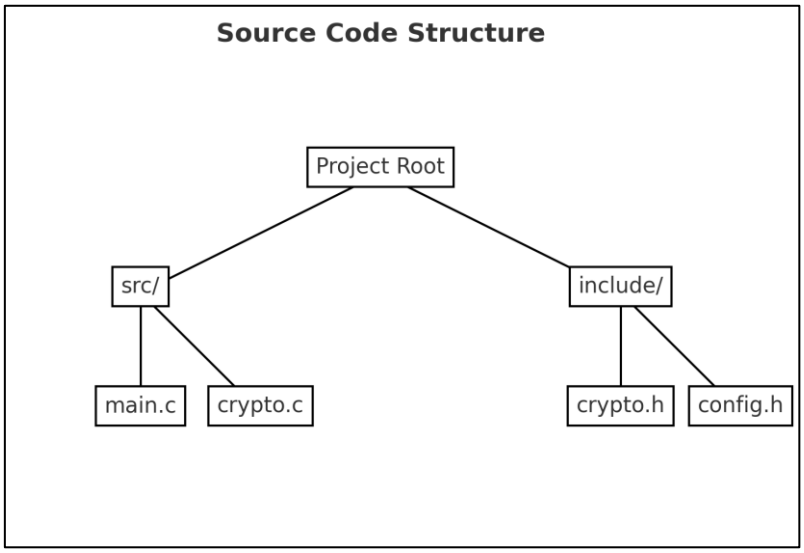

Figure 3-150 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-200 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-151 그림 제목

8.3.3 판정근거

Table 3-201 TE11.01.01 시험결과 판정근거

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

8.3.4 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

9.3 TE12.01.01

9.3.1 시험 요구사항

TE	주요 확인사항	확인방법
TE12.01.01	개발문서의 요구사항 명세 만족	개발문서 검토

9.3.2 시험내용

1) 개발문서 검토

가) 개발문서명

- <개발문서명>

나) 개발문서 검토내용

- <개발문서 검토내용 설명>

다) 증빙자료

- <증빙자료 내용 설명>

Table 3-202 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

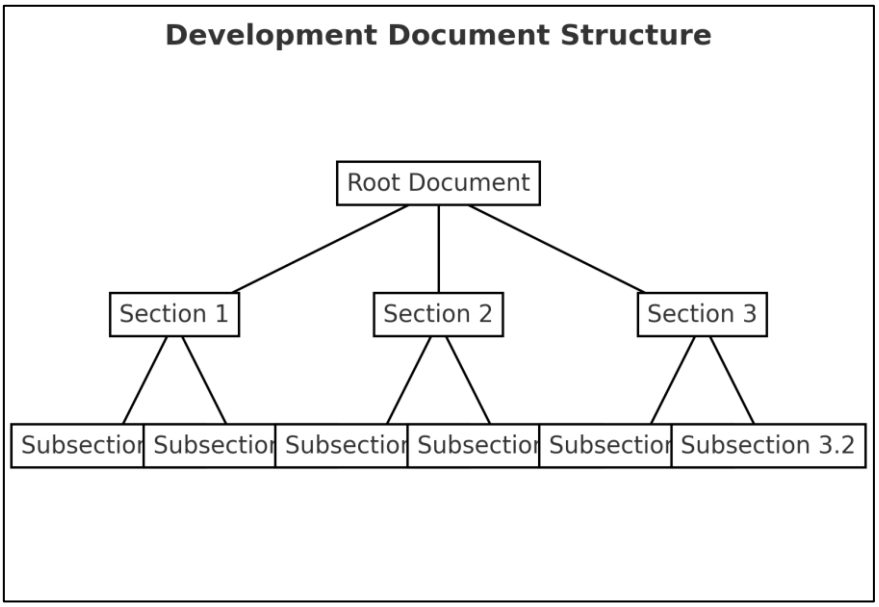

Figure 3-152 그림 제목

2) 소스코드 검토

라) 소스코드명

- <소스코드명>

마) 소스코드 검토내용

- <개발문서 검토내용 설명>

바) 증빙자료

- <증빙자료 내용 설명>

Table 3-203 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

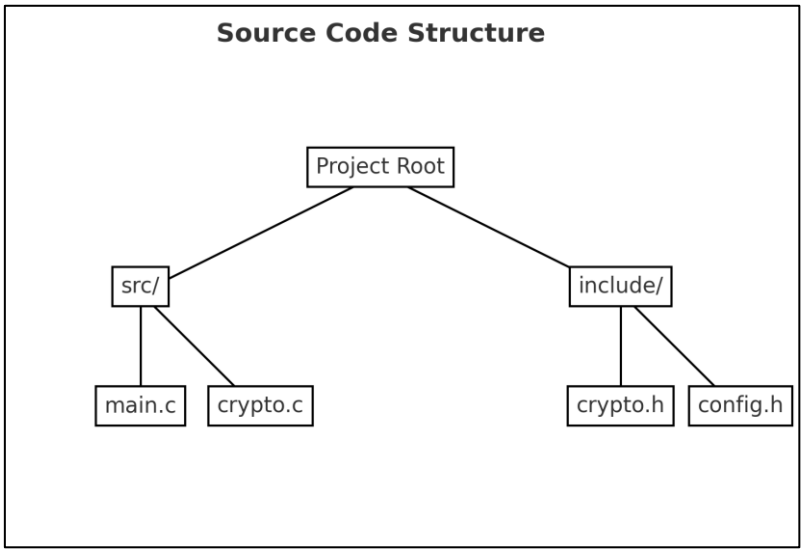

Figure 3-153 그림 제목

사) 암호모듈 시험명

- <암호모듈 시험명칭>

아) 암호모듈 시험내용

- <암호모듈 시험내용 설명>

자) 증빙자료

- <증빙자료 내용 설명>

Table 3-204 표 제목

No	대분류	중분류	내용
1			
2			
3			
4			
5			
6			
7			

```
(base)              -VMware-Virtual-Platform:~$ openssl list -cipher-algorithms
Legacy:
  AES-128-CBC
  AES-128-CBC-HMAC-SHA1
  AES-128-CBC-HMAC-SHA256
  id-aes128-CCM
  AES-128-CFB
  AES-128-CFB1
  AES-128-CFB8
  AES-128-CTR
  AES-128-ECB
  id-aes128-GCM
  AES-128-OCB
  AES-128-OFB
  AES-128-XTS
  AES-192-CBC
  id-aes192-CCM
  AES-192-CFB
  AES-192-CFB1
  AES-192-CFB8
  AES-192-CTR
  AES-192-ECB
```

Figure 3-154 그림 제목

9.3.3 판정근거

Table 3-205 TE12.01.01 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 '\[첨부4] VS시험결과\ABC V1.0 CAVP 시험결과.pdf'

제 5 장 결론

1. 시험결과

□이 암호모듈은 보안수준 1을 만족하도록 신청된 소프트웨어 암호모듈로 「KS X ISO/IEC 19790:2015, 24759:2015를 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
	동작모드	AS02.19	만족
		AS02.20	만족
		AS02.21	만족
		AS02.22	만족
		AS02.24	만족
암호모듈 인터페이스	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

		AS04.06	만족
	서비스	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
자가시험	자가시험 일반 요구사항	AS10.07	만족
		AS10.08	만족
		AS10.09	만족
		AS10.10	만족
		AS10.11	만족
	동작 전 자가시험	AS10.15	만족
		AS10.17	만족
		AS10.20	만족
		AS10.24	만족
	조건부 자가시험	AS10.25	만족
		AS10.27	만족
		AS10.28	만족
		AS10.29	만족
		AS10.33	만족
		AS10.34	만족
		AS10.35	만족
		AS10.53	만족
생명주기 보증	생명주기 보증 일반 요구사항	AS11.01	만족
	형상 관리	AS11.03	만족
		AS11.04	만족

		AS11.05	만족
	유한상태모델	AS11.08	만족
		AS11.11	만족
	개발	AS11.13	만족
		AS11.15	만족
		AS11.16	만족
		AS11.19	만족
	벤더 시험	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 1을 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

[별첨1] 소스목록 및 소스 해시 값
[별첨2] 보안정책서

[첨부1] 소스코드
[첨부2] 암호모듈
[첨부3] 개발문서
[첨부4] VS시험결과
[첨부5] 테스트프로그램