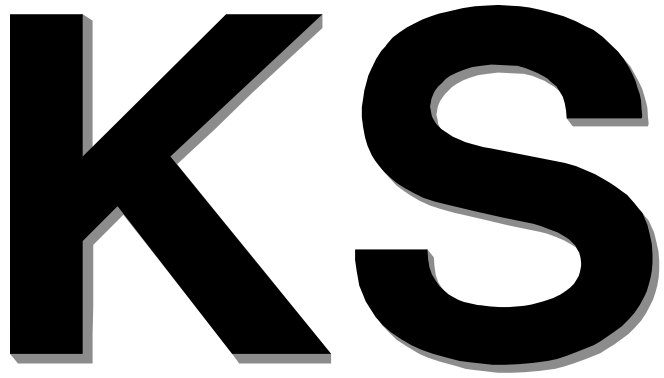
KSKSKSKS
KSKSKSK
KSKSKS
KSKSK
KSKS
KSK
KS

KS X ISO/IEC 24759



정보기술 — 보안기술 — 암호모듈 시험 요구사항

KS X ISO/IEC 24759:2015

산업통상자원부 국가기술표준원

2015년 8월 4일 개정

http://www.kats.go.kr

심 의 : 정보기술 기술심의회

	성 명	근 무 처	직 위
(회 장)	김 형 준	한국전자통신연구원	센 터 장
(위 원)	강 현 국	고려대학교	교 수
	김 재 성	한국인터넷진흥원	수 석
	류 관 희	충북대학교	교 수
	박 춘 식	서울여자대학교	교 수
	박 호 진	한국전자통신연구원	책 임
	오 경 희	TCA 서비스	대 표
	전 진 옥	비트컴퓨터	대 표
	정 혁	한국전자통신연구원	책 임
	정 혜 정	평택대학교	교 수
(간 사)	배 승 호	국가기술표준원 표준정책국 전기전자표준과	

개정 작성 : 암호모듈 연구위원회

	성 명	근 무 처	직 위
(위원장)	최 희 봉	국가보안기술연구소	책임연구원
(위 원)	이 훈 재	동서대학교	교 수
	이 옥 연	국민대학교	교 수
	홍 석 희	고려대학교	교 수
	최 명 길	중앙대학교	교 수
	염 용 진	국민대학교	교 수
	한 상 윤	국가보안기술연구소	선임연구원
(간 사)	배 승 호	국가기술표준원	연 구 사

표준열람 : 국가표준종합정보센터 (http://www.standard.go.kr)

제 정 자 : 산업통상자원부 국가기술표준원장　　제　　정 : 2007년 12월 26일
개　　정 : 2015년 8월 4일　　국가기술표준원 고시　제 2015-0342 호
심　　의 : 산업표준심의회 정보기술 기술심의회
원안작성협력 : 암호모듈 연구위원회

목 차

개 요

이 표준은 2014년 제2판으로 발행된 ISO/IEC 24759, Information technology -- Security techniques -- Test requirements for cryptographic modules를 기초로 기술적 내용 및 대응국제표준의 구성을 변경하지 않고 작성한 한국산업표준이다.

한국산업표준

KS X ISO/IEC 24759:2015

정보기술 — 보안기술 — 암호모듈 시험 요구사항

Information technology — Security techniques — Test requirements for cryptographic modules

1 적용범위

이 표준은 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항에 적합한지 여부를 시험하기 위해서 시험기관이 사용하는 시험방법을 명세하고 있다. 이 방법은 시험을 수행하는 동안 객관성과 일관성을 보증하기 위하여 개발되었다.

또한 이 표준은 벤더가 시험기관에 제출해야 하는 정보의 요구사항을 명세하고 있다. 이 정보의 요구사항은 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항에 적합함을 설명하는 증거들이다.

벤더는 시험기관에 암호모듈 시험을 신청하기 전에 암호모듈이 KS X ISO/IEC 19790에 명세된 요구사항을 충족하는지 여부를 검증할 때 이 표준을 사용할 수 있다.

2 인용표준

다음의 인용표준은 이 표준의 적용을 위해 필수적이다. 발행연도가 표기된 인용표준은 인용된 판만을 적용한다. 발행연도가 표기되지 않은 인용표준은 최신판(모든 추록을 포함)을 적용한다.

KS X ISO/IEC 19790, 정보 기술 — 보안 기술 — 암호모듈 보안 요구사항

3 용어와 정의

이 표준의 목적을 위하여 KS X ISO/IEC 19790에 정의된 용어와 정의를 적용한다.

4 약어

이 표준의 목적을 위하여 KS X ISO/IEC 19790에 정의된 약어를 적용한다.

5 문서 구조

5.1 일반사항

6.은 시험기관이 사용하는 시험방법과 벤더가 시험기관에 제출해야 하는 정보를 명세한다. **6.1** 일반사항을 제외하고, **6.**은 11개 영역의 보안 요구사항을 설명하는 11개 절과 KS X ISO/IEC 19790의 **부속서** A~F로 구성된다.

5.2 시험 항목과 보안 요구사항

6.의 각 절은 KS X ISO/IEC 19790의 보안 요구사항을 시험 항목으로 나누어 서술하고 있다(예: 암호모듈의 특정 보안수준이 해당 보안 요구사항을 충족하기 위한 서술문).

시험 항목은 다음과 같이 나타낸다.

AS<요구사항 번호>.<시험 항목 번호>

여기서 "요구사항 번호"는 해당 보안 요구사항 영역 번호(즉, 1～12, A～F)이다. "시험 항목 번호"는 절 내의 시험 항목을 위한 식별 번호이다. 각 시험 항목의 문장 끝에는 시험 항목이 적용하는 보안수준(예: 보안수준 1～4)을 괄호 안에 표시한다.

각 시험 항목 다음에는 벤더가 고려해야 하는 요구사항들이 있다. 이 요구사항은 시험자가 해당 시험 항목의 준수 여부를 검증하는 데 필요한 개발 문서나 제출물을 서술한다. 이 요구사항은 다음과 같이 나타낸다.

VE<요구사항 번호>.<시험 항목 번호>.<순서 번호>

여기서 "요구사항 번호"와 "시험 항목 번호"는 해당 보안 요구사항 영역 번호(즉, 1～12, A～F)와 시험 항목 식별 번호이고, "순서 번호"는 시험 항목 내의 벤더 요구사항 식별 번호이다.

각 시험 항목과 벤더에 부가된 요구사항 다음에는 암호모듈의 시험 절차에 대한 요구사항들이 있다. 이 요구사항은 암호모듈의 해당 시험 항목에 따라 시험하기 위해 시험자가 수행해야 할 시험 절차이다. 이 요구사항은 다음처럼 나타낸다.

TE<요구사항 번호>.<시험 항목 번호>.<순서 번호>

여기서 "요구사항 번호"와 "시험 항목 번호"는 해당 영역 식별 번호(즉, 1～12, A～F)와 시험 항목 식별 번호이고, "순서 번호"는 시험 항목 요구사항 내의 시험자 요구사항을 위한 식별 번호이다.

검증기관은 이 표준에 있는 VE, TE를 수정, 첨가, 삭제할 수 있다.

5.3 시험 항목의 상호 참조

시험 항목을 명확하게 나타내기 위하여 KS X ISO/IEC 19790이나 다른 시험 항목 번호를 상호 참조하는 내용은 괄호({ })에 서술한다.

6 보안 요구사항

6.1 일반사항

AS01.01: (명세 – 보안수준 1, 2, 3, 4)

이 장은 암호모듈이 이 표준을 준수하기 위해 충족해야 하는 보안 요구사항을 명세한다.

비고 이 절은 **6.**의 기타 절의 시험 항목과 A～F의 시험 항목들을 충족시키기 위한 일반 요구사항을 설명한다. 이 절은 자체 시험 항목이 없으며, 별도로 시험되지 않는다.

AS01.02: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 이 장에서 기술된 각 영역의 요구사항에 대해 시험되어야 한다.

비고 1 시험은 다음 방법 중 하나 또는 그 이상으로 수행될 수 있다.
a) 시험자는 시험자의 설비에서 시험을 수행한다.
b) 시험자는 벤더의 설비에서 시험을 수행한다.
c) 시험자는 벤더가 벤더의 설비에서 시험을 수행하는 것을 감독한다.
- 시험자가 직접 시험을 수행하지 못한 근거를 제시해야 한다.
- 시험자는 요구되는 시험 계획과 시험방법을 개발한다.
- 시험자는 시험 수행 과정을 직접 관찰한다.

시험 절차에 의한 시험 중 하나라도 '실패'하면 시험 항목은 실패로 판정된다.

비고 2 이 절은 **6.**의 기타 절의 시험 항목을 충족시키는 일반 요구사항을 설명한다. 이 절은 자체 시험 항목이 없으며 별도로 시험되지 않는다.

AS01.03: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 각 영역에서 독립적으로 평가되어야 한다.

비고 이 절은 **6.**의 기타 절의 시험 항목과 A~F의 시험 항목들을 충족시키기 위한 일반 요구사항을 설명한다. 이 절은 자체 시험 항목이 없으며, 별도로 시험되지 않는다.

AS01.04: (명세 – 보안수준 1, 2, 3, 4)

암호모듈을 독립적으로 검증하거나 평가하기 위해 사용자 설명서, 설치 설명서, 설계 명세와 생명주기 문서를 포함하는 개발 문서가 제출되어야 한다.

비고 이 절은 **6.**의 기타 절의 시험 항목과 A~F의 시험 항목들을 충족시키기 위한 일반 요구사항을 설명한다. 이 절은 자체 시험 항목이 없으며, 별도로 시험되지 않는다.

6.2 암호모듈 명세

6.2.1 암호모듈 명세의 일반 요구사항

AS02.01: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 모든 암호알고리즘이나 프로세서를 사용하여 최소한 한 개 이상의 암호 서비스를 구현하고 암호 경계 내에 포함된 하드웨어나 소프트웨어, 펌웨어 또는 이들의 결합 형태이어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS02.02: (명세 – 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790 **부속서**} **A.2.2**에 명세된 요구사항을 충족하는 개발 문서가 제출되어야 한다.

비고 해당 시험 항목은 **ASA.01**의 일부분으로 시험된다.

6.2.2 암호모듈 유형

AS02.03: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 다음과 같은 모듈 유형 중 한 가지로 정의되어야 한다.

- 하드웨어 모듈은 하드웨어 경계를 이용하여 암호 경계가 구분될 수 있도록 명세화된 모듈이다. 하드웨어 암호 경계 안에 펌웨어 또는 소프트웨어를 포함할 수 있으며, 이때 펌웨어 또는 소프트웨어는 운영체제도 포함할 수 있다.
- 소프트웨어 모듈은 변경 가능한 운영환경에서 실행하는 소프트웨어 구성 요소(한 개 또는 여러 개의 구성 요소)들이며, 암호 경계는 소프트웨어 경계를 이용하여 구분될 수 있도록 명세화된 모듈이다. 소프트웨어 구성 요소가 실행되는 연산 플랫폼 및 운영체제는 정의된 소프트웨어 모듈 경계 외부에 있다.
- 펌웨어 모듈은 제한되거나 변경이 불가능한 운영환경에서 실행하는 펌웨어 구성 요소들이며, 암호 경계는 펌웨어 경계를 이용하여 구분될 수 있도록 명세화된 모듈이다. 펌웨어 구성 요소가 실행되는 연산 플랫폼이나 운영체제는 정의된 펌웨어 모듈 경계의 외부에 있지만 펌웨어 모듈과 항상 결합된 형태이어야 한다.
- 하이브리드 소프트웨어 모듈은 소프트웨어 구성 요소 및 하드웨어 구성 요소를 조합한 유형이며, 소프트웨어 구성 요소는 하드웨어 모듈 경계와 분리되어야 한다. 소프트웨어 구성 요소가 실행되는 연산 플랫폼 및 운영체제는 정의된 하이브리드 소프트웨어 모듈 경계의 외부에 있다(예: 소프트웨어 모듈과 하드웨어 모듈의 조합은 하이브리드 하드웨어 모듈로 분류된다).
- 하이브리드 펌웨어 모듈은 펌웨어 구성 요소 및 하드웨어 구성 요소를 조합한 유형이며, 펌웨어 구성 요소는 하드웨어 모듈 경계와 분리되어야 한다. 펌웨어 구성 요소가 실행되는 연산 플랫폼 또는 운영체제는 정의된 하이브리드 펌웨어 모듈 경계의 외부에 있지만 항상 하이브리드 펌웨어 모듈과 결합된 형태이어야 한다(예: 펌웨어 모듈과 하드웨어 모듈의 조합은 하이브리드 펌웨어 모듈로 분류된다).

[벤더 요구사항]

VE02.03.01
벤더는 암호모듈 유형을 기술한 개발 문서를 제출해야 한다. 여기에 모듈 유형 선택의 근거를 명세한다.

VE02.03.02
벤더는 암호모듈의 모든 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소를 식별하는 개발 문서를 제출해야 한다.

[시험 절차]

TE02.03.01
시험자는 벤더가 제출한 개발 문서를 통해 **AS02.03**에 나열된 모듈 유형 중 하나와 동일한지 확인해야 한다.

TE02.03.02
시험자는 벤더가 제출한 개발 문서를 통해 암호모듈이 모든 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소들(**AS02.15**~**AS02.18**)의 암호모듈 유형과 일치하는지 확인해야 한다.

AS02.04: (명세 – 보안수준 1, 2, 3, 4)

하드웨어 모듈과 펌웨어 모듈은 해당되는 {KS X ISO/IEC 19790} **7.7** 및 **7.8**의 모든 물리적 보안 요구사항과 비침투 보안 요구사항을 충족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS02.05: (명세 – 보안수준 1, 2, 3, 4)

하이브리드 모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소는 해당되는 {KS X ISO/IEC 19790} **7.5**와 **7.6**의 모든 보안 요구사항을 충족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS02.06: (명세 – 보안수준 1, 2, 3, 4)

{하이브리드 모듈의} 하드웨어 구성 요소는 해당되는 {KS X ISO/IEC 19790} **7.7**, **7.8**의 모든 보안 요구사항을 충족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

6.2.3 암호 경계

6.2.3.1 암호 경계에 대한 일반 요구사항

AS02.07: (명세 – 보안수준 1, 2, 3, 4)

암호 경계는 암호모듈의 모든 구성 요소의 경계에 의해서 설정되는 통합 경계(즉, 하드웨어 구성 요소, 소프트웨어 구성 요소 및 펌웨어 구성 요소의 집합)이어야 한다.

[벤더 요구사항]

VE02.07.01
벤더는 암호 경계 안에 있는 모든 구성 요소들을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.07.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 **AS02.15**~**AS02.18**에 기술된 모든 구성 요소가 암호 경계 안에 있는지 확인해야 한다.

TE02.07.02
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 **AS02.15**~**AS02.18**에 명세되지 않은 구성 요소가 암호 경계 안에 없다는 것을 확인해야 한다.

AS02.08: (명세 – 보안수준: 1, 2, 3, 4)

해당 표준의 요구사항들은 암호모듈의 암호 경계 내 모든 알고리즘, 프로세스 및 구성 요소에 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS02.09: (명세 – 보안수준 1, 2, 3, 4)

암호 경계는 암호모듈(즉, 이 표준의 범위 내에 있는 보안에 관련된)의 모든 알고리즘, 모든 프로세서

및 모든 구성 요소를 반드시 포함해야 한다.

[벤더 요구사항]

VE02.09.01
벤더는 암호 경계 안에 있는 모든 보안에 관련된 알고리즘, 프로세스, 그리고 구성 요소의 목록을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.09.01
시험자는 벤더가 제출한 개발 문서에 암호 경계 안에 있는 모든 보안에 관련된 알고리즘, 프로세스, 그리고 구성 요소가 정의되어 있고 목록화되어 있는지 확인해야 한다.

AS02.10: (명세 – 보안수준 1, 2, 3, 4)

검증대상 동작모드에 사용되는 비보안 알고리즘, 비보안 프로세서 또는 비보안 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상시키지 않는 방법으로 구현되어야 한다.

[벤더 요구사항]

VE02.10.01
벤더는 검증대상 동작모드에 사용된 비보안 함수들의 목록을 작성하고, 모듈의 검증대상 동작모드에 방해가 되지 않는다는 것을 증명한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.10.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 비보안 함수들이 모듈의 검증대상 동작모드를 방해하거나 손상시키지 않는다는 것을 확인해야 한다.

TE02.10.02
시험자는 벤더가 제출한 개발 문서를 통하여 비보안 함수들이 모듈의 검증대상 동작모드를 방해하지 않고 손상시키지 않는다는 근거를 확인해야 한다. 벤더는 이를 증명해야 한다. 만일 부정확하고 모호한 부분이 존재한다면 시험자는 필요 시 벤더에게 추가 정보를 요청해야 한다.

AS02.11: (명세 – 보안수준 1, 2, 3, 4)

암호모듈의 명칭은 암호 경계 내에 있는 구성 요소만의 조합을 의미하도록 정해져야 하며, 암호 경계 내에 있는 구성 요소의 조합보다 더 큰 범위의 제품이나 구성 요소의 조합을 의미하는 명칭이 되지 않아야 한다.

[벤더 요구사항]

VE02.11.01
벤더는 암호모듈의 명칭을 제공해야 한다.

[시험 절차]

TE02.11.01
시험자는 암호 경계 안에 있는 구성 요소의 결합이 의미하는 것과 벤더가 제공한 모듈 명칭이 일치하는지 확인해야 한다.

TE02.11.02
시험자는 모듈 명칭이 암호 경계 안에 있는 구성 요소의 결합과 일치하지 않는 구성 요소 또는 기능을 의미하지 않음을 확인해야 한다.

AS02.12: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소 각각에 대하여 최소한 특정 버전 정보를 가져야 한다.

[벤더 요구사항]

VE02.12.01
벤더는 모듈에 포함된 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소 각각에 대하여 버전 정보를 제공해야 한다.

[시험 절차]

TE02.12.01
시험자는 버전 정보가 모듈에 포함된 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소 각각을 나타내는지 확인해야 한다.

AS02.13: (명세 – 보안수준 1, 2, 3, 4)

암호 경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 암호모듈의 검증대상 동작을 방해하거나 손상을 초래하지 않도록 구현되어야 한다.

※ 암호 경계 외부에 있는 하드웨어 구성 요소, 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 해당 표준의 보안 요구사항을 적용받지 않는다.

[벤더 요구사항]

VE02.13.01
벤더는 암호 경계 외부에 있는 모듈의 구성 요소를 명세하고, 이 구성 요소들이 모듈의 검증대상 동작모드를 방해하지 않는다는 것을 증명한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.13.01
시험자는 개발 문서를 통해 암호 경계 외부에 있는 구성 요소들이 모듈의 검증대상 동작모드를 방해하지 않는다는 것을 확인해야 한다.

AS02.14: (명세 – 보안수준 1, 2, 3, 4)

보안 요구사항에 해당하지 않는 하드웨어, 소프트웨어 또는 펌웨어는 {KS X ISO/IEC 19790} **부속서** A의 요구사항을 충족하도록 명세되어야 한다.

[벤더 요구사항]

VE02.14.01
벤더는 보안 요구사항을 적용받지 않는 모든 구성 요소들을 서술한 개발 문서를 제출해야 한다.

VE02.14.02
벤더는 VE02.13.01의 결과로 작성된 구성 요소 각각에 대해 {KS X ISO/IEC 19790}의 보안 요구사항에 적용받지 않는다는 근거를 명시한 개발 문서를 제출해야 한다. 벤더는 개발 문서에서 암호 경계의 외부에 있는 각 구성 요소가 오작동하거나 오용 시에도 암호모듈의 검증대상 동작모드를 손상시키지 않는 것을 보여야 한다.

[시험 절차]

TE02.14.01
시험자는 개발 문서를 통하여 KS X ISO/IEC 19790의 보안 요구사항에 해당하지 않는 모듈의 구성 요소가 존재하는지를 확인해야 한다.

TE02.14.02
KS X ISO/IEC 19790의 보안 요구사항을 적용받지 않는 모듈의 구성 요소가 존재한다면, 시험자는 개발 문서를 통해 구성 요소가 보안 요구사항에 적용받지 않는 근거를 확인해야 한다. 그 구성 요소가 오동작 시에도 오용하면 손상을 일으키는 평문 데이터 또는 기타 정보가 노출되지 않는다는 근거를 제시해야 한다. 개발 문서에 다음과 같은 내용을 포함시키면 그 근거는 충분하다.

a) 보안 요구사항을 적용받지 않는 외부 구성 요소는 오용 시 검증대상 동작모드에 손상을 초래할 수 있는 SSP, 평문 데이터 또는 기타 정보를 처리하지 않는다.
b) 보안 요구사항을 적용받지 않는 외부 구성 요소는 보안 관련 구성 요소와 오용 시 검증대상 동작모드에 손상을 초래할 수 있는 SSP, 평문 데이터 또는 기타 정보를 부적절하게 전송하는 연결을 가질 수 없다.
c) 구성 요소가 처리할 모든 정보는 모듈의 내부에서만 사용되어야 하고, 모듈이 연결된 장비에 영향을 주는 어떠한 방법도 없다.

TE02.14.03
시험자는 암호 경계 외부에 있고 보안 요구사항에 해당되지 않는 구성 요소에 대한 근거가 정확한지 확인해야 한다. 벤더는 해당 근거에 대한 증명을 제시해야 한다. 만일 그 근거가 부정확하거나 모호한 부분이 있다면 시험자는 벤더에게 추가 정보를 요구해야 한다.

6.2.3.2 암호 경계의 정의

AS02.15: (명세 – 보안수준 1, 2, 3, 4)

하드웨어 암호모듈의 암호 경계는 다음과 같이 범위를 명확히 정해야 한다.

- 하드웨어 구성 요소의 집합은 다음을 포함할 수 있다.
  - ① 회로 보드, ② 회로기판 또는 ③ 구성 요소 간을 배선으로 연결하는 기타 표면실장 부품 등을 포함하는 물리적 구조
  - 준주문형 IC(semi-integrated circuit), 주문형(custom) IC, 일반 상용(common) IC, 프로세서, 메모리, 전원 공급기, 변환기 등과 같은 능동 전기 소자
  - 봉함, 매몰재 혹은 캡슐화 물질, 커넥터 및 인터페이스 등과 같은 물리적 구조
  - 운영체제를 포함할 수 있는 펌웨어

◦ 상기에 기재되지 않은 기타 구성 요소들

[벤더 요구사항]

VE02.15.01
벤더는 암호모듈의 모든 하드웨어 구성 요소를 서술한 개발 문서를 제출해야 한다. 개발 문서에 서술된 구성 요소는 다음을 모두 포함해야 한다.

a) ① 회로 보드, ② 회로 기판 또는 ③ 구성 요소 간을 배선으로 연결하는 기타 표면실장 부품 등을 포함하는 물리적 구조
   1) 회로 보드, 회로 기판, 표면실장 부품

b) 준주문형 IC, 주문형 IC, 일반 상용 IC, 프로세서, 메모리, 전원 공급기, 변환기 등과 같은 능동 전기 소자
   1) 마이크로 프로세서, DSP, 주문형 프로세서, 마이크로 컨트롤러 또는 (제조사와 유형을 식별하는) 기타 프로세서 등을 포함하는 프로세스
   2) 실행 코드 및 데이터를 프로그래밍하는 ROM IC(예: 마스크 프로그램을 할 수 있는 PROM, 자외선으로 지울 수 있는 EPROM, 전기적으로 지울 수 있는 EEPROM 또는 플래시 메모리)
   3) RAM이나 임시 데이터 저장용 기타 IC
   4) 준주문형 IC 또는 ASIC(Application-specific Integrated Circuits)[예: GA(Gate Array) 소자, PLA (Programmable Logic Arrays) 소자, FPGA(Field Programmable Gate Array) 또는 기타 PLA 장치]
   5) 주문형 암호 IC를 포함한 완전 주문형 IC나 또는 ASIC
   6) 전압 변환기(예: AC－DC 변환 모듈 또는 DC－DC 변환 모듈, 변압기), 입력 전원 커넥터, 출력 전원 커넥터 등을 포함하는 전원 공급 구성 요소
   7) 기타 능동 전자 소자(풀업/풀다운 저항, 우회 커패시터와 같은 수동 회로 소자는 암호모듈의 부분으로 보안 관련 기능을 제공하지 않는 경우 암호 경계에 포함될 필요가 없음).

c) 물리적 구조(예: 봉함, 매몰재, 캡슐화 물질, 커넥터, 인터페이스)
   1) 제거 가능한 접근 개구부나 덮개를 포함한 물리적 구조와 봉함
   2) 매몰재 또는 캡슐화 물질
   3) 암호 경계상의 커넥터
   4) 모듈 안에 있는 독립된 주요 서브 조립품 사이의 커넥터

d) 운영체제를 포함할 수 있는 펌웨어
   1) 실행 가능한 코드
      i) 변경 불가능
      ii) 변경 가능

e) 상기에 기재되지 않은 기타 구성 요소 유형들
   1) 냉각기 또는 온열 장치(예: 전도판 또는 공기 냉각, 열교환기, 냉각핀, 팬, 히터, 기타 열을 추가하거나 제거하는 장치)

VE02.15.02
벤더는 축약 설계도를 포함한 모듈의 조립 방법(예: 고정 또는 부착)과 내부 레이아웃 설계를 명세한 개발 문서를 제출해야 한다.

VE02.15.03
벤더는 봉함, 연결 지점, 회로 기판, 전원 공급 위치, 내부 연결 배선, 냉각 장치, 그리고 기타 중요 파라미터를 포함한 모듈의 물리적 주요 파라미터가 명세한 개발 문서를 제출해야 한다.

VE02.15.04
벤더는 모듈의 암호 경계와 하드웨어 구성 요소들의 관계를 표현하는 블록도를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.15.01
시험자는 암호모듈의 모든 하드웨어 구성 요소들을 확인해야 한다. 구성 요소는 다음 모든 것을 포함해야 한다.

a) 회로 보드나 회로 기판, 구성 요소 간을 배선으로 연결하는 기타 표면실장 부품 등을 포함하는 물리적 구조
   1) 회로 보드, 회로 기판, 표면실장 부품

b) 준주문형 IC, 주문형 IC, 일반 상용 IC, 프로세서, 메모리, 전원 공급기, 변환기 등과 같은 능동 전기 소자
   1) 마이크로 프로세서, DSP, 주문형 프로세서, 마이크로 컨트롤러 또는 (제조사와 유형을 식별하는) 기타 프로세서 등을 포함하는 프로세스
   2) 실행 코드 및 데이터를 프로그램하는 ROM IC(예: 마스크 프로그램할 수 있는 PROM, 자외선으로 지울 수 있는 EPROM, 전기적으로 지울 수 있는 EEPROM 또는 플래시 메모리)
   3) RAM이나 임시 데이터 저장용 기타 IC
   4) 준주문형 IC 또는 ASIC(Application-specific Integrated Circuits)[예: GA(Gate Array) 소자, PLA (Programmable Logic Arrays) 소자, FPGA(Field Programmable Gate Array) 또는 기타 PLA 장치]
   5) 주문형 암호 IC를 포함한 완전 주문형 IC 결합 회로나 또는 ASIC 응용에 특화된 IC
   6) 전압 변환기(예: AC－DC 변환 모듈 또는 DC－DC 변환 모듈, 변압기), 입력 전원 커넥터, 출력 전원 커넥터 등을 포함하는 전원 공급 구성 요소
   7) 기타 능동 전자 소자(풀업/풀다운 저항, 우회 커패시터와 같은 수동 회로 소자는 암호모듈의 부분으로서 보안 관련 기능을 제공하지 않는 경우 암호 경계에 포함될 필요가 없음).

c) 물리적 구조(예: 봉함, 매몰재, 캡슐화 물질, 커넥터, 인터페이스)
   1) 제거 가능한 접근 개구부나 덮개를 포함한 물리적 구조와 봉함
   2) 매몰재 또는 캡슐화 물질
   3) 암호 경계상의 커넥터
   4) 모듈 안에 있는 독립된 주요 서브 조립품 사이의 커넥터

d) 운영체제를 포함할 수 있는 펌웨어
   1) 실행 가능한 코드
      i) 변경 불가능
      ii) 변경 가능

e) 상기에 기재되지 않은 기타 구성 요소들
   1) 전도판 또는 공기 냉각, 열교환기, 냉각핀, 팬, 히터, 기타 열을 제거하거나 추가할 수 있는 냉각 또는 히터 장치

TE02.15.02
시험자는 벤더의 구성 요소 목록이 아래에 정의된 이 절의 기타 시험 항목에 대해 제출된 정보와 일치하는지 확인해야 한다.

a) **AS02.07**의 암호 경계의 명세: 암호 경계 내부에 있는 모든 구성 요소들이 구성 요소 목록에 포함

되어 있고, 반대로 구성 요소 목록에 모든 구성 요소가 암호 경계 내부에 있는지 확인한다. 또한 암호 경계 외부에 있는 구성 요소들이 암호모듈 구성 요소 목록에 포함되지 않았음을 확인한다.

b) **ASA.01**의 블록도의 명세: 블록도에 정의된 각각의 구성 요소(예: 프로세서, 응용에 특화된 ASIC)도 구성 요소 목록에 제시되었는지 확인한다.
c) **AS02.13**과 **AS02.14**의 KS X ISO/IEC 19790의 요구사항에 해당되지 않는 외부 구성 요소: 외부 구성 요소가 구성 요소 목록에서 제외되어 있는지 확인한다.

TE02.15.03
시험자는 암호모듈에 통제 불가능한 입력, 출력 또는 기타 접근이 가능한 틈새가 없는지 암호 경계의 물리적 연속 접점을 확인해야 한다. (물리적 보호와 변조 보호는 KS X ISO/IEC 19790의 **7.7**의 요구사항에 의해 별도로 적용된다.) 모듈 설계는 오용 시 손상을 초래할 수 있는 SSP, 평문 데이터 또는 기타 정보를 내부 또는 외부로 통과시키는 암호모듈의 통제 불가능한 인터페이스가 존재하지 않는다는 것도 보장해야 한다.

TE02.15.04
시험자는 암호 경계가 오용 시 손상을 초래할 수 있는 SSP, 평문 데이터 또는 기타 정보를 입력하거나 출력하거나 처리하는 것과 같은 모든 구성 요소, 즉 **ASA.01**에 해당되는 블록도에서 식별되는 모든 구성 요소를 포함한다는 것을 확인해야 한다.

TE02.15.05
상기 요구사항의 일부 예외 사항으로 벤더는 해당 절의 **AS02.13**과 **AS02.14**의 요구사항은 만족하지만 KS X ISO/IEC 19790의 보안 요구사항에서 제외된 일부 구성 요소를 둘 수 있다. 이 경우, 시험자는 다음의 제외된 구성 요소와 모듈의 나머지 구성 요소 간의 인터페이스나 물리적 연결을 확인해야 한다.

a) 오용 시 손상을 초래할 수 있는 CSP, 평문 데이터 또는 기타 정보를 통제하지 않는 한 노출
b) 손상을 초래할 수 있는 SSP나 기타 정보의 통제하지 않는 수정

TE02.15.06
시험자는 벤더의 개발 문서가 모듈의 주요 식별이 가능한 구성 요소의 배치와 대략적인 치수를 포함한 모듈의 내부 레이아웃을 나타내고 있는지 확인해야 한다. 개발 문서는 대략적인 크기를 나타내는 그림을 포함해야 한다.

TE02.15.07
시험자는 벤더의 개발 문서가 모듈의 주요 물리적 조립 부품을 표기하고, 조립 방법 또는 삽입 방법을 명세하였는지 확인해야 한다.

TE02.15.08
시험자는 벤더의 개발 문서가 모듈의 중요한 물리적 파라미터를 명세하였는지 확인해야 한다. 이 명세는 최소한 다음과 같은 내용을 포함해야 한다.

a) 접근 도어나 커버를 포함한 봉함 모양과 대략적인 치수
b) 회로 보드의 대략적인 치수와 레이아웃, 내부 연결
c) 전원 공급의 위치, 전원 변환기, 전원 입출력
d) 내부 연결 배선: 라우팅과 터미널
e) 전도판이나 공기 냉각, 열교환기, 냉각핀, 팬, 히터 또는 모듈의 열을 제거/주입할 수 있는 기타 냉각 및 가열 장치
f) 상기에 기재되지 않은 기타 구성 요소들

TE02.15.09
시험자는 벤더가 제출한 개발 문서의 블록도가 모듈의 경계와 하드웨어 구성 요소들의 관계를 나타냈는지 확인해야 한다.

AS02.16: (명세 – 보안수준 1, 2, 3, 4)

소프트웨어 암호모듈의 다음 사항에 대한 암호 경계의 범위가 명확히 정해져야 한다.

- 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
- 메모리에 저장되어 있으며 한 개 또는 그 이상의 처리기에 의해 실행되는 암호모듈의 인스턴스 생성

[벤더 요구사항]

VE02.16.01
벤더는 암호모듈의 모든 소프트웨어 구성 요소를 명세한 개발 문서를 제출해야 한다. 명세된 구성 요소는 다음 내용을 모두 포함해야 한다.

a) 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
b) 상기에 언급되지 않은 보안에 관련된 구성 요소 유형

VE02.16.02
벤더는 소프트웨어 구성 요소가 상호 작동하는 방법을 포함한 내부 소프트웨어 구조를 명세한 개발 문서를 제출해야 한다.

VE02.16.03
벤더는 모듈이 실행되는 소프트웨어 환경(예: 운영체제, 실행 시간 라이브러리)을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.16.01
시험자는 개발 문서에 암호모듈의 모든 소프트웨어 구성 요소를 포함한 구성 요소 목록이 포함되었음을 확인해야 한다.

TE02.16.02
시험자는 모듈 내부에서 사용되지 않은 구성 요소 유형만 제외하고 다음 유형의 구성 요소가 구성 요소 목록에 포함되었음을 확인해야 한다.

a) 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
b) 상기에서 나열되지 않은 기타 구성 요소 유형들

TE02.16.03
시험자는 아래에서 정의된 것과 같은 해당 절의 다른 시험 항목에 필요한 정보와 구성 요소 목록이 일치하는지 확인해야 한다.

a) 시험 항목 **AS02.07**에 해당되는 암호 경계의 명세. 암호 경계의 내부에 있는 모든 구성 요소들이 구성 요소 목록에 포함되어 있는지 확인하고 또한 암호 경계 외부의 구성 요소가 암호모듈의 구성 요소에 포함되지 않았음을 확인한다.
b) 시험 항목 **ASA.01**에 해당되는 소프트웨어 명세. 소프트웨어 구성 요소 목록이 시험 항목 **AS02.07**에 해당되는 명세와 동일한지 확인한다.

c) 시험 항목 **ASA.01**에 해당하는 블록도 명세. 블록도에서 식별되는 각 구성 요소들이 구성 요소 목록에도 나열되어 있음을 확인한다.
d) 시험 항목 **AS02.13**과 **AS02.14** 규정에 해당하지만 KS X ISO/IEC 19790의 요구사항에서 제외된 구성 요소들. 여기에서 제외된 구성 요소들이 구성 요소 목록에도 제외되었는지 확인한다.

TE02.16.04
상기 요구사항에 대한 일부 예외 사항으로 벤더는 해당 장의 시험 항목 **AS02.13**과 **AS02.14**의 요구사항을 만족하지만 KS X ISO/IEC 19790의 요구사항에서 제외된 일부 구성 요소를 둘 수 있다. 이때 벤더는 제외된 구성 요소를 모듈의 암호 경계 외부로 다룰 수 있다. 이 경우, 시험자는 다음의 제외된 구성 요소와 모듈의 나머지 구성 요소 간의 인터페이스나 물리적 연결을 확인해야 한다.

a) 오용 시 손상을 초래할 수 있는 CSP, 평문 데이터 또는 기타 정보를 통제하지 않는 한 노출
b) 손상을 초래할 수 있는 SSP나 기타 정보의 통제하지 않는 수정

TE02.16.05
시험자는 벤더의 개발 문서가 모듈의 주요 소프트웨어 구성 요소들을 제시하고, 모듈을 형성하기 위한 그 구성 요소들의 링크 방법을 제시했음을 확인해야 한다.

AS02.17: (명세 – 보안수준 1, 2, 3, 4)

펌웨어 암호모듈의 다음 사항에 대한 암호 경계의 범위가 명확히 정해져야 한다.

- 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
- 메모리에 저장되어 있으며 한 개 또는 그 이상의 처리기에 의해 실행되는 암호모듈의 인스턴스 생성

[벤더 요구사항]

VE02.17.01
벤더는 암호모듈의 모든 펌웨어 구성 요소를 명세한 개발 문서를 제출해야 한다. 제시된 구성 요소들은 다음 내용을 모두 포함해야 한다.

a) 실행 가능한 파일이나 암호모듈의 구성 파일의 집합
b) 상기에 언급되지 않은 보안에 관련된 기타 구성 요소 유형

VE02.17.02
벤더는 펌웨어 구성 요소들이 상호 동작하는 방법을 포함한 내부 펌웨어 구조를 명세한 개발 문서를 제출해야 한다.

VE02.17.03
벤더는 모듈이 수행하는 펌웨어 환경(예: 운영체제, 실시간 실행 라이브러리 등)을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.17.01
시험자는 개발 문서에 암호모듈의 모든 펌웨어 구성 요소들을 포함한 구성 요소 목록이 포함되었음을 확인해야 한다.

TE02.17.02
시험자는 구성 요소 목록에 모듈 안에서 사용되지 않은 구성 요소 유형만 제외하고, 다음의 모든 구

성 요소 유형들이 포함되었음을 확인해야 한다.

a) 펌웨어 구성 요소들
b) 상기에서 나열되지 않은 기타 구성 요소 유형들

TE02.17.03
시험자는 아래에서 정의된 것처럼 제출된 구성 요소 목록이 이 절의 기타 시험 항목을 위해 제출한 정보와 동일한지 확인해야 한다.

a) 시험 항목 **AS02.07**에 해당되는 암호 경계 명세. 암호 경계의 내부에 있는 모든 구성 요소들이 구성 요소 목록에 포함되어 있는지 확인하고 또한 암호 경계 외부의 구성 요소가 암호모듈의 구성 요소에 포함되지 않았음을 확인한다.
b) 시험 항목 **ASA.01**에 해당되는 펌웨어 명세. 펌웨어 구성 요소 목록이 시험 항목 **AS02.07**에 해당되는 명세와 동일한지 확인한다.
c) 시험 항목 **ASA.01**에 해당하는 블록도 명세. 블록도에 제시된 각 구성 요소들이 구성 요소 목록에도 나열되어 있음을 확인한다.
d) 시험 항목 **AS02.13**, **AS02.14** 규정에 해당하지만 KS X ISO/IEC 19790의 요구사항에서 제외된 구성 요소들. 여기에서 제외될 구성 요소들이 구성 요소 목록에도 나열되었는지 확인한다.

TE02.17.04
상기 요구사항에 대한 일부 예외 사항으로 벤더는 해당 절의 시험 항목 **AS02.13**과 **AS02.14**의 요구사항을 만족하지만 KS X ISO/IEC 19790의 요구사항에서 제외된 일부 구성 요소를 둘 수 있다. 그러면 벤더는 제외된 구성 요소를 모듈의 암호 경계 외부로 다룰 수 있다. 이 경우, 시험자는 제외된 구성 요소와 모듈의 나머지 구성 요소 사이의 인터페이스나 물리적 연결이 오용 시 손상을 초래할 수 있는 CSP, 평문 데이터 또는 기타 정보를 통제하지 않는 한 노출할 수 없음을 확인해야 한다.

TE02.17.05
시험자는 벤더의 개발 문서가 모듈의 주요 펌웨어 구성 요소들을 제시하고, 모듈을 형성하기 위한 그 구성 요소들의 링크 방법을 제시했음을 확인해야 한다.

AS02.18: (명세 – 보안수준 1, 2, 3, 4)

하이브리드 암호모듈의 암호 경계는 다음과 같아야 한다.

- 모듈의 하드웨어 구성 요소 경계와 이 구성 요소와 별도로 분리되어 있는 소프트웨어 구성 요소 경계와의 조합
- 또는 모듈의 하드웨어 구성 요소 경계와 이 구성 요소와 별도로 분리되어 있는 펌웨어 구성 요소 경계와의 조합
- 각 구성 요소의 모든 포트와 인터페이스의 집합을 포함해야 한다.

비고 소프트웨어 구성 요소 또는 펌웨어 구성 요소와 조합하는 하드웨어 구성 요소는 소프트웨어 또는 펌웨어를 내장할 수 있다. 여기서 소프트웨어 구성 요소 또는 펌웨어 구성 요소는 하드웨어 구성 요소와 별도로 분리되어 있다.

[벤더 요구사항]

VE02.18.01
벤더는 암호모듈이 하이브리드 소프트웨어 모듈인지 하이브리드 펌웨어 모듈인지 명확하게 식별할 수 있도록 명세된 개발 문서를 제출해야 한다.

a) 하이브리드 소프트웨어 구성 요소들을 위해서 벤더 제출물은 VE02.15.01～VE02.15.04, 그리고 VE02.16.01～VE02.16.03에 요구하는 정보를 제공해야 한다.
b) 하이브리드 펌웨어 구성 요소들을 위해서 벤더 제출물은 VE02.15.01～VE02.15.04, 그리고 VE02.17.01～VE02.17.03에 요구하는 정보를 제공해야 한다.

[시험 절차]

TE02.18.01
시험자는 개발 문서가 모듈이 하이브리드 소프트웨어 모듈인지 하이브리드 펌웨어 모듈인지를 식별하는지 확인해야 한다.

a) 하이브리드 소프트웨어 구성 요소들을 위해서 벤더 제출물은 VE02.15.01～VE02.15.04, 그리고 VE02.16.01～VE02.16.03에 요구하는 정보를 제공해야 한다.
b) 하이브리드 펌웨어 구성 요소들을 위해서 벤더 제출물은 VE02.15.01～VE02.15.04, 그리고 VE02.17.01～ VE02.17.03에 요구하는 정보를 제공해야 한다.

6.2.4 동작모드

6.2.4.1 동작모드의 일반 요구사항

AS02.19: (명세 – 보안수준 1, 2, 3, 4)

운영자는 검증대상 동작모드에서 암호모듈을 작동할 수 있어야 한다.

[벤더 요구사항]

VE02.19.01
벤더는 검증대상 동작모드를 서술한 보안정책서를 포함하는 개발 문서를 제출해야 한다.

VE02.19.02
벤더는 검증대상 동작모드를 실행시키기 위한 명령을 서술한 보안정책서를 포함하는 개발 문서를 제출해야 한다.

[시험 절차]

TE02.19.01
시험자는 개발 문서를 검토하여 보안정책서가 검증대상 동작모드에 대한 명세를 포함하는지 확인해야 한다.

TE02.19.02
시험자는 개발 문서의 보안정책서에서 서술된 명령들을 이용하여 검증대상 동작모드를 실행해야 한다. 시험자는 개발 문서를 검토하고 암호모듈을 검사하여 개발 문서에 서술된 명령을 실행하면 암호모듈이 검증대상 동작모드에서 작동하는 것을 확인해야 한다.

AS02.20: (명세 – 보안수준 1, 2, 3, 4)

검증대상 동작모드는 검증대상 암호알고리즘이나 프로세스를 이용한 한 개 이상의 서비스를 포함한 서비스 집합으로 정의된다. 여기서 이들 서비스와 프로세스는 {KS X ISO/IEC 19790} **7.4.3**에 명세되어 있다.

[벤더 요구사항]

VE02.20.01
벤더는 사전 검토 단계에서 구현 적합성 검증을 수행할 검증대상 암호알고리즘의 목록을 포함하는 개발 문서를 제출해야 한다.

VE02.20.02
벤더는 모든 비검증대상 암호알고리즘의 목록을 제출해야 한다.

[시험 절차]

TE02.20.01
시험자는 사전 검토 단계에서 수행한 검증대상 암호알고리즘에 대한 구현 적합성 검증이 성공했는지 확인해야 한다.

TE02.20.02
시험자는 벤더가 비검증대상 암호알고리즘들의 목록을 제출했다는 것을 확인해야 한다.

AS02.21: (명세 – 보안수준 1, 2, 3, 4)

비검증대상 암호알고리즘이나 프로세스뿐만 아니라 {KS X ISO/IEC 19790} **7.4.3**에 명세되지 않은 기타 서비스도 검증대상 동작모드에서 운영자가 사용할 수 없어야 한다. 단, 비검증대상 암호알고리즘이 검증대상 프로세스의 일부분이면서, 검증대상 프로세스의 비보안 관련 동작일 경우는 비검증대상 암호알고리즘이 사용될 수 있다(예: 검증대상 동작모드에서 수행되는 비검증대상 알고리즘 또는 비검증대상 키 생성 알고리즘으로 생성된 키는 데이터나 CSP를 알기 어렵게 하기 위해 사용될 수 있지만, 그 결과는 검증대상 암호알고리즘으로 보호되기 전까지는 보호되지 않은 평문으로 취급되고, 비보안 관련 기능을 제공하는 것으로 간주된다).

[벤더 요구사항]

VE02.21.01
벤더는 각 검증대상 동작모드에서 지원되는 각 서비스에 사용된 모든 비검증대상 암호알고리즘이나 프로세스를 명세한 개발 문서를 제출해야 한다.

VE02.21.02
벤더는 비검증대상 암호알고리즘이나 프로세스가 검증대상 프로세스 동작과 보안 관련성이 없다는 근거를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.21.01
시험자는 암호모듈을 검사하여 개발 문서가 각 검증대상 동작모드에서 지원하는 각 서비스에 사용된 모든 비검증대상 암호알고리즘이나 프로세스를 서술하고 있는지 확인해야 한다.

TE02.21.02
시험자는 벤더가 제공한 근거의 정확성을 확인한다. 벤더는 해당 근거에 대한 증명을 제시해야 한다. 만일 그 근거가 부정확하거나 모호한 부분이 있다면 시험자는 벤더에게 추가 정보를 요구해야 한다.

6.2.4.2 정상 동작

AS02.22: (명세 – 보안수준 1, 2, 3, 4)

CSP는 검증대상 서비스 및 동작모드와 비검증대상 서비스 및 동작모드에서 독립적으로 분리되어야 한다(예: 상호 공유되거나 접근할 수 없어야 한다).

[벤더 요구사항]

VE02.22.01
벤더는 모듈에 포함되는 모든 CSP 목록을 명세하고, 이들 CSP가 검증대상 서비스 및 동작모드와 비검증대상 서비스 및 동작모드에서 사용되는 내역을 명세한 개발 문서를 제출해야 한다.

VE02.22.02
벤더는 각 CSP가 검증대상 서비스 및 동작모드와 비검증대상 서비스 및 동작모드에서 분리 사용되는 방법을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.22.01
시험자는 개발 문서에 검증대상 동작모드 또는 비검증대상 동작모드에서 사용되는 각 CSP에 대해 설명되었는지 확인해야 한다.

TE02.22.02
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 CSP가 검증대상 동작모드와 비검증대상 동작모드 사이에서 분리 사용되는지 확인해야 한다.

AS02.23: (명세 – 보안수준 1, 2, 3, 4)

모듈의 보안정책은 검증대상 동작모드와 비검증대상 동작모드에서 제공하는 모든 서비스의 집합을 정의해야 한다.

비고 해당 시험 항목은 **ASB.01**에 따라 시험된다.

AS02.24: (명세 – 보안수준 1, 2, 3, 4)

모든 서비스는 검증대상 동작모드에서 검증대상 암호알고리즘이나 프로세스를 사용할 때 각 서비스에 대한 표시기를 제공해야 한다. 여기서 이들 서비스와 프로세스는 {KS X ISO/IEC 19790} **7.4.3**에 명세되어 있다.

[벤더 요구사항]

VE02.24.01
벤더는 각 서비스에 대한 표시기를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE02.24.01
시험자는 서비스가 검증대상 동작모드에서 검증대상 암호알고리즘이나 프로세스를 사용할 때의 표시기를 개발 문서에 명세하고 있는지 확인해야 한다.

TE02.24.02

시험자는 모든 서비스를 실행해 보고, 각 서비스가 검증대상 동작모드에서 검증대상 암호알고리즘이나 프로세스를 사용하는지 아닌지에 따라 표시기가 정확하게 동작하는지 확인해야 한다.

6.2.4.3 기능 제한 동작

AS02.25: (명세 – 보안수준 1, 2, 3, 4)

기능 제한 동작에서 운영되는 암호모듈은 {KS X ISO/IEC 19790, **AS02.26**～**AS02.30**}에 해당된다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS02.26: (명세 – 보안수준 1, 2, 3, 4)

오류 상태를 벗어난 후에만 기능 제한 동작으로 전환되어야 한다.

[벤더 요구사항]

VE02.26.01
벤더는 암호모듈이 기능 제한 동작을 포함한다면 각 오류 상태를 벗어난 후의 모든 기능 제한 동작을 명세한 개발 문서를 제출해야 한다.

VE02.26.02
벤더는 다음과 같은 내용을 포함한 기능 제한 동작을 명세한 개발 문서를 제출해야 한다.

a) 기능 제한 동작으로의 전환 또는 기능 제한 동작으로부터의 종료에 대한 조건들
b) 작동 가능한 알고리즘, 서비스 또는 프로세스들
c) 비동작 알고리즘, 서비스 또는 프로세스들
d) 기능 제한 동작에서 분리하여 독립적으로 수행되는 메커니즘, 함수 또는 구성 요소들
e) 메커니즘, 함수 또는 구성 요소들을 분리하여 독립적으로 수행시키는 기술
f) 기능 제한 동작에서 제공되는 상태 정보
g) 기능 제한 동작이 비동작 알고리즘이나 프로세스를 사용하고자 하는 시도가 있을 때 이를 나타내는 상태 표시기

[시험 절차]

TE02.26.01
시험자는 개발 문서가 기능 제한 동작과 기능 제한 동작의 진입과 기능 제한 동작의 종료를 명세하고 있는지 확인해야 한다.

TE02.26.02
시험자는 오류 상태를 종료한 이후에만 기능 제한 동작에 접근할 수 있다는 것을 개발 문서를 통해 확인해야 한다. 시험자는 오류 상태 표시기(**AS03.11** 참조)가 정확하게 기재되었는지 확인해야 한다.

TE02.26.03
시험자는 암호모듈이 각 기능 제한 동작을 실행하는지 확인해야 한다. 시험자는 각 기능 제한 동작에 대해 어떠한 서비스가 수행될 때, 처음으로 암호알고리즘이 동작되기 전에 모든 조건부 알고리즘 자가시험이 수행되는지 확인해야 한다.

TE02.26.04
시험자는 암호모듈이 각 기능 제한 동작에서 작동하도록 먼저 실행한다. 그 다음 시험자는 동작 전

자가시험과 조건부 자가시험을 수행해서 암호모듈이 모든 동작 전 자가시험과 조건부 자가시험을 성공적으로 통과할 때까지 기능 제한 동작 상태로 남아 있는지 확인해야 한다.

TE02.26.05
시험자는 먼저 암호모듈이 각 기능 제한 동작에서 작동하도록 실행한다. 그 다음 시험자는 오류를 발생시키도록 동작 전 자가시험을 수행한다. 시험자는 암호모듈이 기능 제한 동작 상태에 있지 않고 오류 상태로 진입하는 것을 확인해야 한다.

AS02.27: (명세 – 보안수준 1, 2, 3, 4)

모듈이 재구성되고 기능 제한 동작 상태로 진입했을 때 상태 정보를 제공해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS02.26**의 일부분으로 시험된다.

AS02.28: (명세 – 보안수준 1, 2, 3, 4)

오동작을 일으킨 메커니즘이나 기능은 분리되어야 한다.

[벤더 요구사항]

VE02.28.01
개발 문서 요구사항은 VE02.26.02에 명세되어 있다. 개발 문서는 결함을 갖는 메커니즘, 함수 및 구성 요소에서 발생한 결함이 암호모듈의 검증대상 동작을 방해하거나 손상시킬 수 없다는 것을 보장해야 한다.

[시험 절차]

TE02.28.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 결함을 갖는 메커니즘, 함수 및 구성 요소의 작동은 기능 제한 동작 상태에 진입하기 전에 암호모듈의 검증대상 동작과 분리됨을 확인해야 한다.

TE02.28.02
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 결함을 갖는 메커니즘, 함수 및 구성 요소가 암호모듈의 검증대상 동작을 방해하거나 손상시킬 수 없다는 것을 확인해야 한다.

AS02.29: (명세 – 보안수준 1, 2, 3, 4)

기능 제한 동작 진입 후 모든 조건부 알고리즘 자가시험은 암호알고리즘이 처음 동작하기 전에 수행되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS02.26**의 일부분으로 시험된다.

AS02.30: (명세 – 보안수준 1, 2, 3, 4)

비동작 알고리즘이나 프로세스를 사용하려는 경우 서비스는 표시기를 제공해야 한다.

[벤더 요구사항]

VE02.30.01
개발 문서 요구사항은 VE02.26.02에 명세되어 있다. 개발 문서는 비동작 알고리즘이나 프로세스를

사용하려는 경우 서비스 출력이 해당 시도에 대한 표시기를 포함하고 있음을 보장해야 한다.

[시험 절차]

TE02.30.01
시험자는 개발 문서를 통해 비동작 알고리즘이나 프로세스를 사용하려는 시도에 대해 서비스가 표시기를 제공한다는 것을 확인해야 한다.

TE02.30.02
시험자는 비동작 알고리즘이나 프로세스를 사용하려는 시도에 대해 암호모듈을 실행하여 개발 문서에 명세된 표시기와 일치된 표시기를 제공하는지 확인해야 한다.

AS02.31: (명세 – 보안수준 1, 2, 3, 4)

암호모듈은 모든 동작 전 자가시험과 조건부 자가시험을 성공적으로 통과할 때까지 기능 제한 동작 상태로 남아 있어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS02.26**의 일부분으로 시험된다.

AS02.32: (명세 – 보안수준 1, 2, 3, 4)

암호모듈이 동작 전 자가시험을 실패한다면 모듈은 기능 제한 동작에 진입할 수 없다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS02.26**의 일부분으로 시험된다.

6.3 암호모듈 인터페이스

6.3.1 암호모듈 인터페이스에 대한 일반 요구사항

AS03.01: (모듈 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈은 모든 논리적 정보 흐름이 암호 경계의 입출구로 식별되는 물리적 접근 지점과 논리적 인터페이스에 제한되도록 해야 한다.

[벤더 요구사항]

VE03.01.01
개발 문서는 암호모듈의 다음 사항에 대한 각 물리적 포트와 논리적 인터페이스를 명세해야 한다.

a) 물리적 포트와 핀 할당
b) 물리적 덮개, 개구부 또는 통로
c) 논리적 인터페이스(예: API와 기타의 모든 데이터/제어/상태 신호)와 신호 명칭 및 기능들
d) 적용 가능한 물리적 제어 입력을 위한 수동 제어 장치(예: 버튼이나 스위치)
e) 적용 가능한 물리적 상태 출력을 위한 물리적 상태 표시기(예: 라이트나 디스플레이)
f) 암호모듈의 물리적 포트, 수동 제어 장치, 물리적 상태 표시기로의 논리적 인터페이스의 연관관계
g) 상기 포트와 인터페이스에서 존재할 수 있는 물리적, 논리적, 전기적 특성

VE03.01.02
벤더는 블록도, 설계 명세, 소스 코드, 그리고 이 표준의 **6.2**와 **6.11**에 명세된 스킴을 강조하거나 주석화를 통해 암호모듈의 정보 흐름과 물리적 접근 지점을 명세한 개발 문서를 제출해야 한다. 또한

벤더는 물리적 포트와 논리적 인터페이스에 대한 정보 흐름과 물리적 접근 지점들의 관계를 명세하기 위해 필요 시 별도의 문서를 제출해야 한다. 개발 문서에서의 입출력 포트에 대한 구성 요소들과 물리적 계층의 명세가 **AS02.07**과 **AS02.15**～**AS02.18**에 제공된 정보와 일치해야 한다.

VE03.01.03
암호모듈에 입력되는 각 물리적 또는 논리적 입력이나 암호모듈에서 출력되는 각 물리적 그리고 논리적 출력에 대해, 벤더는 물리적 입력·출력 포트 및 물리적 입력 또는 출력에 해당하는 논리적 인터페이스를 명세한 개발 문서를 제출해야 한다. 제출한 개발 문서는 이 표준의 **6.2**와 **6.11**에 명세된 암호모듈 구성 요소의 명세와 이 절의 **AS03.04**～**AS03.11**에 명세된 논리적 인터페이스의 명세와 일치해야 한다.

[시험 절차]

TE03.01.01
시험자는 개발 문서가 암호모듈의 물리적 포트들과 논리적 인터페이스를 각각 명세했는지 확인해야 한다. 개발 문서는 다음 내용을 포함해야 한다.

a) 포트의 핀 할당, 암호모듈 내부의 물리적 포트 배치도, 각 포트를 통과하는 논리적인 신호들의 명세를 포함하고 두 개 이상의 신호가 동일한 물리적인 핀을 공유하는 경우의 신호 흐름의 시간 순차도를 포함한 모든 물리적 입력 포트와 출력 포트에 대한 명세
b) 암호모듈 내부에 있는 물리적 배치도를 포함하고 각 덮개, 개구부 또는 통로를 통해 접근되거나 변경될 수 있는 구성 요소와 기능을 포함한 모든 물리적 덮개, 개구부, 통로에 대한 명세
c) 암호모듈의 모든 논리적인 데이터 입력과 제어 입력 및 데이터 출력과 상태 출력에 대한 목록화되고 주석화된 블록도를 포함하고 신호 명칭과 기능들의 목록과 명세를 포함한 모든 논리적 입출력 인터페이스(예: API와 모든 기타 데이터/제어/상태 신호들)에 대한 명세
d) 암호모듈 내부 물리적 배치도를 포함하고 수동적으로 입력될 수 있는 제어 신호의 목록과 명세를 포함한 스위치와 버튼 같은 제어 신호를 물리적으로 입력하는 데 사용될 모든 수동 제어 소자들에 대한 명세
e) 암호모듈 내부의 물리적 표시기 배치도를 포함하고 물리적으로 출력되는 상태 표시 신호의 목록과 명세를 포함한 모든 물리적 상태 표시기에 대한 명세
f) 암호모듈의 물리적 입출력 포트, 수동 제어 소자 그리고 물리적인 상태 표시기와 논리적 입출력 인터페이스 사이의 매핑 관계에 대한 명세
g) 위에서 언급한 물리적 포트와 인터페이스에 해당된다면, 포트 핀 할당에 대한 명세, 각 포트를 통해 전달되는 논리적 신호, 전압 레벨 및 전압 레벨의 논리적 의미(예: 저전압 또는 고전압을 논리적 의미로 “0”, “1” 또는 다른 표현으로 나타내는 것), 그리고 신호의 타이밍도를 포함한 물리적, 논리적 그리고 전기적 특성에 대한 명세

TE03.01.02
시험자는 해당 표준의 **6.2**와 **6.11**에 규정된 블록도, 설계 명세 또는 소스 코드 및 회로도 그리고 벤더가 제공한 다른 문서를 조사하여 개발 문서가 암호모듈의 모든 정보 흐름과 물리적 접근 지점을 명세하는지 확인해야 한다. 개발 문서는 암호모듈의 물리적 포트 및 논리적 인터페이스와 정보 흐름 및 물리적 접근 지점과의 관계를 명세해야 한다. 시험자는 **AS02.07**과 **AS02.15**～**AS02.18**에서 제공된 정보와 상기의 정보를 비교하고, 입출력 포트에 대한 구성 요소 및 물리적 레이아웃의 명세가 일치하는지 확인해야 한다.

TE03.01.03
시험자는 개발 문서를 통해 암호모듈에 입력되는 각 물리적 입력 또는 논리적 입력이나 암호모듈에서 출력되는 물리적 출력 및 논리적 출력에 대해 물리적 입력 또는 출력에 해당하는 논리적 인터페

이스와 물리적 입력 포트 또는 출력 포트를 명시하는지 확인해야 한다. 개발 문서는 이 표준의 **6.2**와 **6.11**에 명시된 암호모듈 구성 요소의 명세와 이 절의 **AS03.04**～**AS03.11**에 명세된 논리적 인터페이스의 명세와 일치해야 한다.

TE03.01.04
시험자는 암호모듈을 검사하여 개발 문서가 기술하는 상기의 모든 명세와 실제로 설계된 암호모듈이 일치하는지 확인해야 한다.

AS03.02: (암호모듈 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈 논리적 인터페이스들은 한 개의 물리적 포트를 공유하더라도 서로 구별되어야 하며(예: 입력 데이터와 출력 데이터가 동일한 포트를 통해 입출력될 수 있다), 하나 이상의 물리적 포트(예: 입력 데이터가 직렬 및 병렬 포트 모두를 통해 들어올 수 있다.)로 분산하여 사용될 수 있다.

비고 암호모듈의 소프트웨어 구성 요소의 API는 하나 이상의 논리적 인터페이스로 정의될 수 있다.

[벤더 요구사항]

VE03.02.01
벤더는 **AS03.04**에 서술된 항목들을 사용하고 또한 해당되는 경우 **AS03.12**와 **AS03.13**에서 서술된 항목들을 사용하여 암호모듈 인터페이스들을 논리적으로 구분되고 분리된 항목으로 분류한 개발 문서를 제출해야 한다. 이 정보는 해당 절의 **AS03.01**에서 제공된 논리적 인터페이스와 물리적 포트에 대한 명세와 일치되어야 한다.

VE03.02.02
벤더는 암호모듈의 물리적 포트와 논리적 인터페이스의 각 항목과의 연관관계를 명세한 개발 문서를 제출해야 한다. 논리적 인터페이스는 한 개 이상의 물리적 포트를 거쳐 물리적으로 분산될 수 있으며 또는 두 개 이상의 논리적 인터페이스는 정보의 흐름이 논리적으로 분리된다면 한 개의 물리적 포트를 공유할 수 있다. 두 개 이상의 논리적 인터페이스가 동일한 물리적 포트를 공유한다면 개발 문서는 다른 인터페이스 항목을 통한 정보가 논리적으로 분리되는 방법을 명세해야 한다.

[시험 절차]

TE03.02.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈 인터페이스가 **AS03.04**에 명세된 그리고 해당되는 경우 해당 절의 **AS03.12**와 **AS03.13**에 명세된 인터페이스 항목에 따라 논리적으로 구분되고 분리되는지 확인해야 한다. 이러한 정보는 해당 절의 **AS03.01**에서 명시한 논리적 인터페이스와 물리적 포트의 설계와 명세가 일치되어야 한다.

TE03.02.02
시험자는 개발 문서가 암호모듈의 논리적 인터페이스 각 항목이 어떤 물리적 포트와의 매핑 관계에 있는지를 명세하는지 확인해야 한다. 한 개의 논리적 인터페이스는 한 개 이상의 물리적 포트를 거쳐 물리적으로 분산될 수 있으며, 두 개 이상의 논리적 인터페이스는 정보의 흐름이 논리적으로 분리되기만 하면 한 개의 물리적 포트를 공유하여 사용할 수 있다. 만일 두 개 이상의 논리적 인터페이스가 동일한 물리적 포트를 공유한다면 시험자는 개발 문서가 입력 인터페이스, 출력 인터페이스, 제어 인터페이스 및 상태 인터페이스를 사용하는 정보 흐름이 논리적으로 분리되는 방법을 명세하고 있는지 확인해야 한다.

AS03.03: (암호모듈 인터페이스 – 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790 **부속서**} **A.2.3** 요구사항을 충족하는 개발 문서를 제출해야 한다.

[벤더 요구사항]

VE03.03.01
벤더는 KS X ISO/IEC 19790의 **A.2.3**에 명세된 개발 문서를 제출해야 한다.

[시험 절차]

TE03.03.01
시험자는 KS X ISO/IEC 19790의 **A.2.3**에서 명세된 개발 문서의 완성도를 확인해야 한다.

6.3.2 인터페이스 유형

- **하드웨어 모듈 인터페이스(HMI)**: 요청된 서비스의 일부처럼 모듈의 암호 경계에 들어가거나 나가는 매개변수를 포함한 하드웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합
- **소프트웨어 또는 펌웨어 모듈 인터페이스(SFMI)**: 요청된 서비스의 일부처럼 모듈의 암호 경계에 들어가거나 나가는 매개변수를 포함한 소프트웨어 또는 펌웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합
- **하이브리드 소프트웨어 또는 하이브리드 펌웨어 모듈 인터페이스(HSMI 또는 HFMI)**: 요청된 서비스의 일부로 모듈의 암호 경계에 들어가거나 나가는 매개변수를 포함한 하이브리드 소프트웨어 또는 하이브리드 펌웨어 모듈의 서비스를 요청하기 위해 사용하는 인터페이스 전체 집합

6.3.3 인터페이스 정의

AS03.04: (암호모듈 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈은 다음과 같은 5개의 인터페이스를 갖는다('입력'과 '출력'은 암호모듈의 관점에서 표시된다).

- 데이터 입력 인터페이스
- 데이터 출력 인터페이스
- 제어 입력 인터페이스
- 제어 출력 인터페이스
- 상태 출력 인터페이스

[벤더 요구사항]

VE03.04.01
벤더는 다음과 같은 암호모듈 내부의 5개로 분류된 논리적인 인터페이스에 따라 암호모듈의 인터페이스를 논리적으로 구분하고 분리된 항목으로 분류하여 명세한 개발 문서를 제출해야 한다.

a) 데이터 입력 인터페이스(**AS03.05**에 명세된 데이터 입력용)
b) 데이터 출력 인터페이스(**AS03.06**, **AS03.07**에 명세된 데이터 출력용)
c) 제어 입력 인터페이스(**AS03.08**에 명세된 명령어 입력용)
d) 제어 출력 인터페이스(**AS03.09**, **AS03.10**에 명세된 명령어 출력용)
e) 상태 출력 인터페이스(**AS03.11**에 명세된 상태 정보 출력용)

[시험 절차]

TE03.04.01
시험자는 개발 문서가 VE03.04.01에 명세된 5개의 논리적 인터페이스가 암호모듈 내부에 설계되었음을 서술하는지 확인해야 한다. 만일 확인된다면, 제시된 암호모듈 기능 내부의 논리적인 인터페이스를 해당 절에 있는 **AS03.05**～**AS03.11**에 따라 검증해야 한다.

데이터 입력 인터페이스

AS03.05: (데이터 입력 인터페이스－보안수준 1, 2, 3, 4)

암호모듈에 입력되고 모듈에 의해 처리되는(평문 데이터, 암호문 데이터, SSP, 다른 모듈로부터의 상태 정보를 포함한) 모든 데이터(제어 입력 인터페이스를 통해 들어오는 제어 데이터는 제외)는 데이터 입력 인터페이스를 통해 입력되어야 한다.

[벤더 요구사항]

VE03.05.01
암호모듈은 데이터 입력 인터페이스를 가져야 한다. 암호모듈에 입력되고 처리되는 다음을 포함한 모든 데이터(제어 입력 인터페이스를 통해 들어오는 제어 데이터는 제외)는 데이터 입력 인터페이스를 통해 입력되어야 한다.

a) 평문 데이터
b) 암호문 또는 서명 데이터
c) 암호키 및 기타 키 관리 데이터(평문 또는 암호문)
d) 인증 데이터(평문 또는 암호문)
e) 외부 소스로부터의 상태 정보
f) 기타 모든 입력 데이터

VE03.05.02
해당되는 경우, 벤더는 스마트카드, 토큰, 키패드, 키로더 또는 생체 장치와 같은, 데이터 입력 인터페이스로 데이터를 입력하기 위해 암호모듈과 사용하는 모든 외부 장치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.05.01
시험자는 암호모듈을 검사하여 암호모듈이 데이터 입력 인터페이스를 포함하고 있는지 확인하고, 또한 데이터 입력 인터페이스가 개발 문서에 명세된 것처럼 작동하는지 확인해야 한다. 시험자는 (제어 입력 인터페이스를 통해 들어오는 제어 데이터는 제외) 암호모듈로 입력되고 처리되는 다음을 포함한 모든 데이터가 데이터 입력 인터페이스를 통해 입력되는지 확인해야 한다.

a) 암호모듈에 의해 암호화되거나 서명되는 평문 데이터
b) 암호모듈에 의해 복호화되거나 검증되는 암호문이나 서명된 데이터
c) 초기 데이터, 초기 벡터, 분산 키 정보 또는 키 계정 정보를 포함한 암호모듈에 입력되고 처리되는 평문 또는 암호화된 암호키, 그리고 그 밖의 키 관리 데이터(기타 키 관리 정보 요구사항은 KS X ISO/IEC19790의 **7.9**에서 명세됨.)
d) 패스워드, 핀 또는 생체 정보 등 암호모듈에 입력되는 평문 또는 암호화된 인증 데이터
e) 외부 소스(예: 다른 암호모듈 또는 장치)로부터의 상태 정보

f) **AS03.08**에 별도로 명세된 제어 정보를 제외한, 처리 및 저장을 위해 암호모듈에 입력되는 기타 모든 정보

TE03.05.02
시험자는 스마트카드, 토큰, 키패드, 키로더 또는 생체 장치와 같은 데이터 입력 인터페이스로 데이터를 입력하기 위해 암호모듈과 함께 사용되는 모든 외부 입력 장치가 개발 문서에 명세되어 있는지 확인해야 한다. 시험자는 식별된 외부 입력 장치를 이용하여 데이터 입력 인터페이스로 데이터를 입력하고, 외부 입력 장치를 사용한 데이터 입력이 개발 문서에 명세된 대로 작동하는지 확인해야 한다.

데이터 출력 인터페이스

AS03.06: (데이터 출력 인터페이스 – 보안수준 1, 2, 3, 4)

(평문 데이터, 암호문 데이터, SSP를 포함한) 암호모듈에서 출력되는 모든 데이터(상태 출력 인터페이스를 통해 출력되는 상태 데이터와 제어 출력 인터페이스를 통해 출력되는 제어 데이터 제외)는 데이터 출력 인터페이스를 통해 출력되어야 한다.

[벤더 요구사항]

VE03.06.01
암호모듈은 데이터 출력 인터페이스를 가져야 한다. 암호모듈에서 처리되고 출력되는 다음을 포함한 모든 데이터(상태 출력 인터페이스를 통해 출력되는 상태 데이터와 제어 출력 인터페이스를 통해 출력되는 제어 데이터는 제외됨.)는 데이터 출력 인터페이스를 통해 출력되어야 한다.

a) 평문 데이터
b) 암호문 데이터와 전자서명
c) 암호키와 기타 키 관리 데이터(평문 또는 암호문)
d) **AS03.11**에서 별도로 명세된 상태 정보와 **AS03.09**, **AS03.10**에서 명세된 제어 정보를 제외한 암호모듈에서 처리 또는 저장된 후에 출력되는 모든 기타 정보

VE03.06.02
해당되는 경우, 벤더는 스마트카드, 토큰, 키패드, 키로더 또는 생체 장치와 같은, 데이터 출력 인터페이스로 데이터를 출력하기 위해 암호모듈과 함께 사용하는 모든 외부 장치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.06.01
시험자는 암호모듈을 검사하여, 암호모듈이 데이터 출력 인터페이스를 포함하는지, 그리고 데이터 출력 인터페이스의 기능이 서술된 것과 일치하는지 확인한다. 시험자는 다음을 포함하여, (상태 출력 인터페이스를 통과하여 출력되는 상태 데이터와 제어 출력 인터페이스를 통과하여 출력되는 제어 데이터를 제외한) 암호모듈에 의해 처리되고 출력되는 모든 데이터가 데이터 출력 인터페이스를 통과하여 출력되는지 확인해야 한다.

a) 암호모듈에 의해 복호화된 평문 데이터
b) 암호모듈에 의해 암호화된 암호문과 암호모듈에 의해 생성된 전자서명
c) 평문 또는 암호화된 암호키, 초기 데이터, 초기 벡터, 분리된 키 정보, 그리고/또는 키 계정 정보를 포함한 암호모듈에서 내부적으로 생성되고 외부로 출력되는 그 밖의 키 관리 데이터(다른 키 관리 요구사항은 KS X ISO/IEC 19790의 **7.9**에서 다뤄진다.)

d) **AS03.11**에서 별도로 명세된 상태 정보와 **AS03.09**, **AS03.10**에서 명세된 제어 정보를 제외한 암호 모듈에서 처리 또는 저장된 후에 출력되는 모든 기타 정보

TE03.06.02
시험자는 개발 문서가 스마트카드, 토큰, 디스플레이 또는 다른 저장 장치 등 암호모듈이 데이터 출력을 위해 데이터 출력 인터페이스로 사용하는 모든 외부 출력 장치를 기술하는지 확인해야 한다. 시험자는 식별된 외부 출력 장치를 이용하여 데이터 출력 인터페이스로 데이터를 출력하고, 외부 출력 장치의 데이터 출력이 서술된 것과 같이 출력되는지 확인해야 한다.

AS03.07: (데이터 출력 인터페이스 – 보안수준 1, 2, 3, 4)

수동 SSP를 주입하는 상태, 동작 전 자가시험 상태, 소프트웨어/펌웨어를 로드하는 상태 및 제로화하는 상태 또는 암호모듈이 오류 상태에 있을 때는 '데이터 출력' 인터페이스를 통과하는 모든 데이터 출력이 금지되어야 한다.

[벤더 요구사항]

VE03.07.01
벤더는 수동 SSP 주입 상태, 동작 전 자가시험 상태, 소프트웨어/펌웨어 로딩 상태와 제로화 상태 또는 암호모듈이 오류 상태에 있을 때, 암호모듈이 데이터 출력을 금지하는 방법을 명세한 개발 문서를 제출해야 한다.

VE03.07.02
암호모듈의 설계가 수동 SSP 주입 상태, 동작 전 자가시험 상태, 소프트웨어/펌웨어 로딩 상태와 제로화 상태 또는 암호모듈이 오류 상태에 있을 때, 데이터 출력 인터페이스에서 모든 데이터 출력의 금지를 보장하는 방법을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.07.01
시험자는 개발 문서가 데이터 출력 인터페이스를 통한 모든 데이터 출력을 금지하는 방법을 명세하는지 확인해야 한다.

a) 암호모듈이 다음을 수행할 때
   1) 수동 SSP 주입
   2) 동작 전 자가시험
   3) 소프트웨어/펌웨어 로딩 상태
   4) 제로화 상태
b) 암호모듈이 오류 상태에 있을 때

시험 절차는 다음과 같은 방법으로 확인할 수 있다.

a) 시험자는 개발 문서에 의해 다음 서비스 각각의 시작부터 성공적으로 끝날 때까지 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지됨을 확인한다.
   1) 수동 SSP 주입
   2) 동작 전 자가시험
   3) 소프트웨어/펌웨어 로딩 상태
   4) 제로화 상태
b) 시험자는 개발 문서에 의해 오류 상태의 검출과 오류 상태 진입 및 이러한 오류로부터 복구될 때

까지 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인해야 한다.

TE03.07.02
시험자는 암호모듈을 다음의 상태로 진입할 수 있다.

a) 수동 SSP 주입을 수행하는 상태
b) 동작 전 자가시험을 수행하는 자가시험 상태
c) 소프트웨어/펌웨어 로딩을 수행하는 상태
d) 제로화를 수행하는 상태
e) 오류 상태

시험자는 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인해야 한다.

만약 시험자가 오류를 유도하는 것이 불가능하다면, 벤더는 시험자에게 이 시험이 왜 수행될 수 없는지에 대한 근거를 제출해야 한다. 이 경우에 시험자는 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인을 위한 검증기관에서 허용한 다른 방법을 수행해야 한다(예: 적용 가능한 소스 코드 시험).

TE03.07.03
시험자는 개발 문서가 암호모듈이 자가시험 상황에 있을 때 데이터 출력 인터페이스를 통한 모든 데이터 출력을 금지하는 것을 명세했는지 확인해야 한다. 시험자는 개발 문서를 통해, 일단 자가시험이 수행되면 시험이 완료될 때까지 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지를 확인해야 한다. CSP, 평문 데이터 또는 기타 정보가 오용되어도 손상을 초래할 수 없다는 것을 시험자가 확인할 수 있다면, 자가시험의 결과를 표시하기 위한 상태 정보는 상태 출력 인터페이스에서 출력될 수 있다. 시험자는 해당 시험 항목에 따라 명세된 자가시험 조건이 **AS10.14**에 명세된 자가시험과 동일한지 확인해야 한다.

TE03.07.04
시험자는 모듈이 자가시험을 수행하게 하고, 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인해야 한다. 자가시험 결과를 표시하기 위한 상태 출력 인터페이스를 통한 상태 정보가 출력되면, 시험자는 CSP, 평문 데이터 또는 기타 정보 등이 오용되어도 손상을 초래할 수 없는지 확인해야 한다. 만약 시험자가 특정 자가시험 상태에서 데이터 출력을 시도할 수 없다면 벤더는 시험자에게 이 시험이 왜 수행될 수 없는지에 대한 근거를 제출해야 한다. 이 경우에 시험자는 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인을 위한 검증기관에서 허용한 다른 방법을 수행해야 한다(예: 적용 가능한 소스 코드 시험, 시뮬레이터 사용, 디버거 사용).

TE03.07.05
시험자는 개발 문서에서 암호모듈이 오류 상태나 자가시험 조건에 있는 동안 데이터 출력 인터페이스를 통한 모든 데이터 출력을 금지하는 방법을 명세하고 있는지 확인한다. 시험자는 또한 암호모듈의 설계를 검사하여 실제로 데이터 출력 인터페이스가 이들 조건하에서 논리적으로 또는 물리적으로 금지되는지 확인해야 한다.

제어 입력 인터페이스

AS03.08: (제어 입력 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈의 동작을 제어하는 데 사용되는 모든 입력 명령, 신호(예: 클럭 입력) 및 제어 데이터(함수 호출과 스위치, 버튼 및 키보드 같은 수동 제어 장치를 포함)는 '제어 입력' 인터페이스를 통해 입력되어야 한다.

[벤더 요구사항]

VE03.08.01
벤더는 암호모듈이 가지는 제어 입력 인터페이스를 명세한 개발 문서를 제출해야 한다. 암호모듈의 동작을 제어하는 데 사용되는 모든 명령, 신호, 다음의 제어 데이터(데이터 입력 인터페이스를 통해 입력되는 데이터를 제외한)는 제어 입력 인터페이스를 통해 입력되어야 한다.

a) API를 통한 논리적 입력 명령(예: 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소에 대한)
b) 한 개 이상의 물리적 포트를 통한 논리적이거나 물리적인 입력 신호(예: 암호모듈의 하드웨어 구성 요소에 대한)
c) 수동 제어 입력(예: 스위치, 버튼, 키보드를 이용하는)
d) 기타 입력 제어 데이터

VE03.08.02
해당되는 경우, 벤더는 제어 입력 인터페이스를 통한 명령, 신호 및 제어 데이터의 입력을 위해 암호모듈과 함께 사용되는 스마트카드, 토큰, 키패드 같은 모든 외부 입력 장치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.08.01
시험자는 암호모듈을 검사하여 암호모듈에 포함된 제어 입력 인터페이스와 개발 문서에 명세된 제어 입력 인터페이스가 일치하는지 확인한다. 시험자는 암호모듈의 동작을 제어하는 데 사용되는 모든 명령, 신호, (데이터 입력 인터페이스를 통해 입력되는 데이터를 제외한) 제어 데이터가 다음을 포함하여 제어 입력 인터페이스를 통해 입력되는지 확인한다.

a) 소프트웨어 라이브러리나 스마트카드로의 함수 호출 같은, API를 통해 논리적으로 입력되는 명령
b) 직렬 포트나 PC 카드를 통해 전송된 명령과 신호 같은, 한 개 이상의 물리적 포트를 통한 논리적이거나 물리적인 입력 신호
c) 수동 제어 입력(예: 스위치, 버튼 또는 키보드의 이용 같은)
d) 기타 입력 제어 데이터

TE03.08.02
시험자는 개발 문서가 제어 입력 인터페이스에 명령과 신호, 제어 데이터를 입력하기 위해 암호모듈과 함께 사용되는 스마트카드, 토큰, 키패드 같은 모든 외부 입력 장치를 명세했는지 확인해야 한다. 시험자는 식별된 외부 입력 장치를 이용한 제어 입력 인터페이스에 명령을 입력해 보고, 외부 입력 장치에 명령을 입력하는 것과 명세된 것이 동일하게 동작하는지 확인해야 한다.

제어 출력 인터페이스

AS03.09: (제어 출력 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈의 동작 상태를 제어하거나 표시하는 모든 출력 명령, 신호 및 제어 데이터(예: 다른 모듈에 입력시키는 제어 명령)는 '제어 출력' 인터페이스를 통해 출력되어야 한다.

[벤더 요구사항]

VE03.09.01
벤더는 암호모듈의 동작 상태를 제어하거나 표시하기 위해 사용되는 모든 출력 명령, 신호, 제어 데

이터(예: 다른 모듈에 대한 제어 명령)가 제어 출력 인터페이스를 통해 출력되는 것을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.09.01
시험자는 개발 문서가 제어 출력 인터페이스를 통해 출력되는 암호모듈의 동작 상태를 제어하거나 명령하기 위해 사용되는(예: 다른 모듈에 대한 제어 명령 같은) 모든 출력 명령과 신호, 제어 데이터를 명세했는지 확인한다.

TE03.09.02
만약 제어 출력 인터페이스가 명세되었다면, 시험자는 암호모듈을 검사하여 제어 출력 인터페이스가 명세된 내용에 맞게 작동하는지 확인해야 한다.

AS03.10: (제어 출력 인터페이스 – 보안수준 1, 2, 3, 4)

개발 문서의 보안정책에 서술된 예외 사항 이외의 오류 상태에 있을 때, 제어 출력 인터페이스를 통한 암호모듈의 제어 출력은 모두 금지되어야 한다.

[벤더 요구사항]

VE03.10.01
벤더는 암호모듈이 오류 상태에 있을 때마다, 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는 방법을 명세한 개발 문서를 제출해야 한다(오류 상태는 KS X ISO/IEC 19790의 **7.11**에 서술되어 있다). CSP, 평문 데이터 또는 기타 정보가 오용되어도 손상되지 않는다면 상태 정보는 오류 유형을 나타내기 위해 상태 출력 인터페이스를 통해 출력될 수 있다.

VE03.10.02
벤더는 암호모듈의 설계가 모듈이 자가시험 상태에 있을 때, 제어 출력 인터페이스를 통한 모든 제어 출력이 금지됨을 보장하는 방법을 명세한 개발 문서를 제출해야 한다(자가시험은 KS X ISO/IEC 19790의 **7.10**에 서술되어 있다). 자가시험 결과를 표시하기 위한 상태 정보는 CSP, 평문 데이터 또는 기타 정보가 오용되어도 손상되지 않는 한 상태 출력 인터페이스를 통해 출력될 수 있다.

[시험 절차]

TE03.10.01
시험자는 개발 문서가 암호모듈이 오류 상태에 있을 때, 제어 출력 인터페이스를 통과하는 모든 제어 출력이 금지한다는 것을 명세했는지 확인해야 한다. 시험자는 오류 조건이 탐지되고 오류 상태에 들어갔을 때, 오류에서 복구되기 전까지 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는지 개발 문서를 통해 확인해야 한다. 시험자가 CSP, 평문 데이터 또는 기타 정보가 오용되어도 손상되지 않는 것을 확인한다면, 오류 유형을 나타내기 위한 상태 정보는 상태 출력 인터페이스를 통해 출력될 수 있다. 시험자는 해당 시험 항목에 따라 명세된 오류 상태가 **AS11.08**에 명세된 오류 상태와 동일한지 확인해야 한다.

TE03.10.02
시험자는 암호모듈을 각 특정 오류 상태에 진입시키고 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는지 확인한다. 상태 정보가 오류의 유형을 나타내기 위해 상태 출력 인터페이스를 통해 출력되면, 시험자는 출력된 정보가 중요하지 않음을 확인해야 한다. 다음 조치는 암호모듈이 오류 상태로 진입하게 된다[변조 탐지 덮개 혹은 개구부의 개방, 잘못된 형식의 명령, 키 또는 파라미터의

입력, 입력 전압의 저하 또는 그 밖의 오류 유발 조치].

만약 시험자가 오류 상태를 유도할 수 없다면, 벤더는 해당 시험이 수행되지 못하는 근거를 제시해야 한다.

TE03.10.03
시험자는 개발 문서가 암호모듈의 자가시험 상태에서 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는지 확인해야 한다. 시험자는 개발 문서를 통해 자가시험이 수행되면 시험이 종료될 때까지 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는지 확인해야 한다. 시험자가 CPS, 평문 데이터 또는 기타 정보가 오용이 되어도 손상되지 않음을 확인하는 한, 자가시험의 결과를 나타내는 상태 정보는 상태 출력 인터페이스를 통해 출력될 수 있다. 시험자는 해당 시험 항목에 따라 명세된 자가시험이 **AS10.07**에 명세된 자가시험과 동일한지 확인해야 한다.

TE03.10.04
시험자는 암호모듈이 자가시험을 수행하도록 하고, 제어 출력 인터페이스를 통한 모든 제어 출력이 금지되는지 확인한다. 만약 자가시험 결과를 나타내는 상태 정보가 상태 출력 인터페이스를 통해 출력될 수 있다면 시험자는 CSP, 평문 데이터, 기타 정보가 오용되어도 손상되지 않음을 확인해야 한다. 만약 시험자가 오류를 유도할 수 없다면 벤더는 시험자에게 이 시험이 수행될 수 없는 근거를 제공해야 한다.

TE03.10.05
시험자는 개발 문서가 암호모듈이 오류 상태나 자가시험 상태에서 제어 출력 인터페이스를 통해 모든 제어 출력을 금지하는 방법을 명세했는지 확인해야 한다. 시험자는 암호모듈의 구현을 검사하여 제어 출력 인터페이스가 논리적, 물리적으로 금지되었는지 확인해야 한다.

상태 출력 인터페이스

AS03.11: (상태 출력 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈의 상태를 표시하기 위해 사용되는 모든 출력 신호, 표시기(예: 오류 표시기) 및 상태 데이터 [응답 코드 및 (디스플레이, 표시기 램프 같은) 시각 신호, (버저, 톤, 벨소리 같은) 소리, (진동 같은) 기계적 신호와 같은 물리적 표시기]는 “상태 출력” 인터페이스를 통해서 출력되어야 한다.

비고 상태 출력은 암시적이거나 명시적일 수 있다.

[벤더 요구사항]

VE03.11.01
암호모듈은 상태 출력 인터페이스를 가져야 한다. 모듈의 상태를 알리거나 표시하는 데 사용되는 모든 상태 정보, 신호, 논리적 표시기, 물리적 표시기는 다음을 포함한 상태 출력 인터페이스를 통해 출력되어야 한다.

a) API를 통한 논리적인 상태 정보 출력
b) 한 개 이상의 물리적 포트를 통한 논리적 또는 물리적 신호 출력
c) 수동 상태 출력(예: 디스플레이, 표시기, 램프, 버저, 톤, 벨소리 같은)
d) 기타 출력 상태 정보

VE03.11.02
해당되는 경우, 벤더는 상태 출력 인터페이스를 통한 상태 정보, 신호, 논리적 표시기 그리고 물리적

표시기를 출력하는, 암호모듈과 함께 사용되는 스마트카드, 토큰, 디스플레이 또는 저장 장치 같은 모든 외부 출력 장치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.11.01
시험자는 암호모듈을 검사하여 암호모듈이 상태 출력 인터페이스를 포함하는지 확인하고, 상태 출력 인터페이스가 명세된 것처럼 동작하는지 확인해야 한다. 시험자는 모듈의 상태를 알리거나 표시하기 위해 사용되는 모든 상태 정보, 신호, 논리적 표시기, 물리적 표시기가 다음을 포함하여, 상태 출력 인터페이스를 통해 출력되는지 확인해야 한다.

a) 소프트웨어 라이브러리나 스마트카드로부터의 반환 코드 같은, API를 통한 논리적인 상태 정보 출력
b) 직렬 포트나 PC 카드 접속기를 통해 전송되는 상태 정보 같은 한 개 이상의 물리적 포트를 통한 논리적 또는 물리적 신호 출력
c) 수동 상태 출력(예: LED, 버저, 디스플레이의 사용)
d) 기타 출력 상태 정보

TE03.11.02
시험자는 해당되는 경우, 개발 문서가 상태 출력 인터페이스를 통해 상태 정보, 신호, 논리적 표시기, 물리적 표시기를 출력하기 위해 암호모듈과 함께 사용되는 모든 외부 출력 장치를 명세하는지 확인해야 한다.

AS03.12: (모듈 인터페이스 – 보안수준 1, 2, 3, 4)

소프트웨어 암호모듈을 제외한 모든 모듈은 다음과 같은 인터페이스를 가져야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS03.13: (모듈 인터페이스 – 보안수준 1, 2, 3, 4)

전원 인터페이스: 암호모듈에 공급되는 모든 외부 전력은 전원 인터페이스를 통과하여 공급되어야 한다.

비고 모든 전원이 모듈 내부에서 공급되거나 유지되고 또한 물리적 정비 활동에 의해 내장 배터리 교체 작업이 수행되고, KS X ISO/IEC 19790의 **7.7**에 명세된 요구사항을 만족한다면 전원 인터페이스는 필요하지 않다.

[벤더 요구사항]

VE03.13.01
만약 암호모듈이 암호 경계 외부에 있는(예: 전원 공급기나 외부 배터리) 다른 장치로 전원을 공급하거나 다른 장치로부터 전원을 받는다면, 벤더는 전원 인터페이스 및 이에 대응되는 물리적 포트를 명세한 개발 문서를 제출해야 한다.

VE03.13.02
암호모듈에서 암호 경계의 외부 장치로부터 입력되거나 외부 장치로 출력되는 모든 전원은 명세된 전원 인터페이스를 통과해야 한다.

[시험 절차]

TE03.13.01
시험자는 개발 문서가 암호모듈이 암호 경계 외부에 있는 장치(예: 전원 공급기나 전력선, 전원 입구/출력, 외부 배터리)로 전원을 공급하거나, 외부 장치로부터 전원을 받는다는 것을 명세하는지 확인해야 한다. 시험자는 또한 개발 문서가 전원 인터페이스와 이에 대응되는 물리적 포트를 명세하는지 확인한다.

TE03.13.02
시험자는 암호모듈을 검사하여 암호 경계의 외부에 있는 장치로부터 입력되거나 외부 장치로 출력되는 모든 전원이 명세된 전원 인터페이스를 통과하는지 확인해야 한다.

AS03.14: (모듈 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈은 입력에 사용되는 데이터, 제어 정보 및 전원과 출력에 사용되는 데이터, 제어 및 상태 정보를 구별해야 한다.

[벤더 요구사항]

VE03.14.01
벤더는 암호모듈이 입력에 사용되는 데이터 및 제어와 출력에 사용되는 데이터, 제어 및 상태를 구별하는 방법을 명세하고 또한 입력 인터페이스를 통해 암호모듈에 입력되는 데이터와 제어 정보에 사용된 물리적·논리적인 경로와 출력 인터페이스를 통해 암호모듈에서 출력되는 데이터, 제어 정보 및 상태 정보에 사용된 물리적·논리적 경로가 물리적으로 또는 논리적으로 단절되는 방법을 명세한 개발 문서를 제출해야 한다.

VE03.14.02
개발 문서는 입력 데이터와 입력 제어 정보에 사용되는 물리적·논리적인 경로가 출력 데이터, 출력 제어, 출력 상태 정보에 사용되는 물리적·논리적 경로와 물리적으로 또는 논리적으로 단절되는 방법을 명세해야 한다. 만약 입력 데이터 및 입력 제어 정보와 출력 데이터, 출력 제어 및 출력 상태 정보에 사용되는 물리적·논리적 경로가 물리적으로 공유된다면, 개발 문서는 암호모듈이 논리적으로 이들 경로가 분리하는 방법을 명세해야 한다.

VE03.14.03
개발 문서는 암호모듈이 입력 데이터 및 입력 제어와 출력 데이터, 출력 제어 및 출력 상태를 구분하는 것을 입증해야 하고, 입력 인터페이스를 통해 암호모듈에 입력되는 데이터와 제어 정보에 사용되는 물리적·논리적인 경로는 출력 인터페이스를 통해 암호모듈에서 출력되는 데이터, 제어 및 상태 정보에 사용되는 물리적·논리적 경로와 물리적으로 또는 논리적으로 단절되는지 입증해야 하고 또한 이러한 명세는 암호모듈과의 일관성을 보여야 한다.

[시험 절차]

TE03.14.01
시험자는 개발 문서가 암호모듈이 입력에 사용되는 데이터 및 제어와 출력에 사용되는 데이터, 제어 및 상태를 구분하는 방법을 명세하는지 확인해야 한다. 데이터 입력 인터페이스를 통해 입력된 데이터와 제어 입력 인터페이스를 통해 입력된 제어 정보는 출력 데이터 인터페이스에서 출력된 데이터와 출력 제어 인터페이스에서 출력된 제어와 상태 출력 인터페이스에서 출력된 상태 정보와 논리적·물리적으로 구분되어야 한다.

TE03.14.02
시험자는 개발 문서가 입력 데이터 및 입력 제어 정보에 사용되는 물리적·논리적 경로와 출력 데이

터, 출력 제어 및 출력 상태 정보에 사용되는 물리적·논리적인 경로를 단절하는 방법을 명세하는지 확인해야 한다. 만약 입력 데이터 및 입력 제어 정보와 출력 데이터, 출력 제어, 출력 상태 정보에 사용되는 물리적·논리적 경로가 물리적으로 공유된다면, 시험자는 개발 문서에서 암호모듈이 이들 경로를 분리하는 방법을 명세하는지 확인해야 한다.

TE03.14.03
시험자는 암호모듈을 검사하여 개발 문서의 일관성을 확인하고, 암호모듈이 입력에 사용되는 데이터 및 제어와 출력에 사용되는 데이터, 제어 또는 상태를 구분하는지 확인하고 또한 입력 인터페이스를 통해 암호모듈에 입력되는 데이터와 제어 정보에 사용되는 물리적·논리적인 경로와 출력 인터페이스를 통해 암호모듈에서 출력되는 데이터, 제어 및 상태 정보에 사용되는 물리적·논리적 경로가 물리적으로 또는 논리적으로 단절되는지 확인해야 한다.

AS03.15: (모듈 인터페이스 – 보안수준 1, 2, 3, 4)

암호모듈 명세는 모든 입력의 가변 길이를 제한하는 것과 같이 입력 데이터와 제어 정보의 형식을 명확하게 명세해야 한다.

[벤더 요구사항]

VE03.15.01
벤더는 데이터 입력 인터페이스와 물리적 포트를 통해 암호모듈에 입력되는 데이터에 사용된 물리적·논리적 경로를 명세한 개발 문서를 제출해야 한다. 개발 문서는 해당 경로를 (회로도를 강조하거나 주석 처리한 복사본, 블록도 또는 **AS02.07**과 **AS02.15**～**AS02.18**에서 제공된 기타 정보에 의해) 명세해야 한다. 데이터 입력 인터페이스를 통해 암호모듈에 입력되는 모든 데이터는 암호모듈의 물리적 또는 논리적 부분에서 처리되거나 저장되는 동안에 특정 경로만 사용해야 한다.

비고 입력되는 데이터는 **AS03.05**의 데이터 입력과 **AS03.08**의 상태 입력이 될 수 있다.

VE03.15.02
개발 문서는 데이터 입력 인터페이스와 물리적 포트를 통해 암호모듈에 입력되는 모든 데이터가 특정 경로만을 사용하는 것을 명세해야 한다. 개발 문서는 입력 데이터가 사용하는 모든 논리적·물리적인 정보 흐름이 암호모듈의 설계 및 작동과 일치하는 것을 보여야 한다. 개발 문서는 CSP, 평문 데이터 또는 암호모듈의 기타 정보의 손상을 초래할 수 있는 경로들 사이의 충돌이 없음을 명세해야 한다.

VE03.15.03
개발 문서는 모든 가변 길이 입력을 위해 길이 제한을 포함한 입력 데이터와 제어 정보를 명확하게 명세해야 한다.

VE03.15.04
개발 문서는 암호모듈 경계 내부의 구성 요소가 검증된 형식인지 식별해야 한다.

[시험 절차]

TE03.15.01
시험자는 개발 문서가 데이터 입력 인터페이스를 통해 암호모듈에 입력되는 데이터에 사용되는 물리적·논리적인 경로를 명세하는지 확인해야 한다. 시험자는 (회로도를 강조하거나 주석 처리한 복사본, 블록도 또는 **AS02.07**과 **AS02.15**～**AS02.18**에서 제공된 기타 정보에 의해) 개발 문서가 그 경로들을 명세하는지 확인해야 한다. 입력 데이터 경로는 각 물리적 포트를 통과하는 데이터 유형을 시험자가

확인할 수 있도록 자세하게 명세되어야 한다.

TE03.15.02
시험자는 개발 문서를 검토하고 암호모듈을 검사하여 데이터 입력 인터페이스와 물리적 포트를 통해 암호모듈에 입력되는 모든 데이터가 특정 경로만을 사용하는지 확인해야 한다. 시험자는 입력 데이터가 사용하는 모든 논리적·물리적인 정보 흐름이 암호모듈의 설계와 운영과 일치하는지 시험해야 한다. 시험자는 CSP, 평문 데이터 또는 기타 정보의 손상을 초래할 수 있는 경로들 사이에서 충돌이 없음을 확인해야 한다.

TE03.15.03
시험자는 개발 문서 검토와 암호모듈을 검사하여 모든 가변 길이 입력을 위한 길이 제한을 포함한 입력 및 제어 정보 대한 포맷이 명확한지 확인해야 한다.

TE03.15.04
시험자는 암호모듈 내 식별된 구성 요소가 VE03.15.02에서 명시한 특정 경로에 위치하는지 확인해야 한다.

TE03.15.05
시험자는 식별된 구성 요소가 실제 문서화된 포맷과 확인하기 위해서 적용 가능한 소스 코드를 검사한다.

TE03.15.06
시험자는 포맷을 준수하지 않은 데이터나 제어 정보를 입력하여 시도하고, 암호모듈이 그런 서비스 입력에 대해 거절함을 확인해야 한다.

비고 시험 플랫폼이나 설정에서 포맷/제한 부분으로 부여할 수 있다.

보기 1 암호모듈을 사용하기 위한 디바이스 드라이브가 포맷 부분을 규정한다.
보기 2 프로토콜 스택 내의 레이어는 단지 고정된 길이 패킷만을 지원한다.

만약 시험자가 특정 자가시험 상태에서 데이터 출력을 시도할 수 없다면, 벤더는 시험자에게 이 시험이 왜 수행될 수 없는지에 대한 근거를 제출해야 한다. 이 경우에 시험자는 데이터 출력 인터페이스를 통한 모든 데이터 출력이 금지되는지 확인을 위한 검증기관에서 허용한 다른 방법을 수행해야 한다.

6.3.4 신뢰 채널

AS03.16: (신뢰 채널 – 보안수준 3, 4)

암호모듈과 송신자(또는 수신자) 종단 간의 보호되지 않은 평문 CSP, 키 구성 요소, 인증 데이터의 전송을 위하여 암호모듈은 신뢰 채널을 구현해야 한다.

[벤더 요구사항]

VE03.16.01
벤더는 보호되지 않은 CSP의 전송 방법과 이들 CSP가 신뢰 채널을 통해 보호되는 방법을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.16.01
시험자는 암호모듈 경계와 송신자(또는 수신자) 종단 사이의 신뢰 채널이 보호되지 않은 CSP를 보호할 수 있는지 확인해야 한다.

AS03.17: (신뢰 채널 – 보안수준 3, 4)

신뢰 채널은 통신 링크에서 인가되지 않은 변경, 교체, 노출을 방지해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS03.18**이나 **AS03.19**의 일부분으로 시험된다.

AS03.18: (신뢰 채널 – 보안수준 3, 4)

신뢰 채널에 사용되는 물리적 포트는 다른 모든 포트들과 물리적으로 분리되어야 한다(또는 **AS03.19**를 충족해야 한다).

[벤더 요구사항]

VE03.18.01
해당된다면 벤더는 암호모듈이 평문 CSP를 입출력하는 개발 문서를 제출해야 한다. 평문 CSP의 입출력에 사용되는 물리적 포트는 암호모듈의 다른 모든 물리적 포트와 분리되어야 한다.

VE03.18.02
만일 암호모듈이 평문 CSP를 입출력한다면, 암호모듈이 해당 물리적 포트를 통해 평문 CSP만 입출력하고 다른 데이터, 즉 평문 또는 암호문은 그 물리적 포트를 사용하지 않는다는 것을 보장해야 한다.

[시험 절차]

TE03.18.01
시험자는 개발 문서가 암호모듈이 평문 CSP를 입출력한다고 명세하는지 확인해야 한다. 시험자는 개발 문서를 검사하고 암호모듈의 물리적 포트를 검사하여, 평문 CSP의 입출력에 사용되는 해당 물리적 포트가 암호모듈의 다른 모든 물리적 포트와 분리되는지 확인해야 한다.

TE03.18.02
만약 암호모듈이 평문 CSP를 입출력한다면, 시험자는 암호모듈이 해당 물리적 포트를 통해 평문 CSP만 입출력하고 다른 데이터, 즉 평문 또는 암호문은 그 물리적 포트를 사용하지 않는다는 것을 확인해야 한다.

AS03.19: (신뢰 채널 – 보안수준 3, 4)

신뢰 채널에 사용된 논리적 인터페이스는 다른 모든 인터페이스와 논리적으로 분리되어야 한다. {또는 **AS03.18**을 충족해야 한다.}

[벤더 요구사항]

VE03.19.01
벤더는 암호모듈이 평문 CSP를 입출력하는 것을 명세하는 개발 문서를 제출해야 한다. 평문 CSP의 입출력에 사용되고 신뢰 채널을 사용하는 논리적 인터페이스는 다른 모든 인터페이스들과 논리적으로 분리되어야 한다.
VE03.19.02
만약 암호모듈이 평문 CSP를 입출력한다면, 신뢰 채널을 이용하는 해당 논리적 포트를 통해 평문

CSP만 입출력되고 다른 데이터, 즉 평문 또는 암호문은 신뢰 채널을 이용하는 해당 논리적 포트를 통해 입출력되지 않는다는 것을 보장해야 한다.

VE03.19.03
벤더는 신뢰 채널이 통신 링크에서 비인가된 변경, 대체 또는 노출을 방지하는 방법에 대한 근거를 서술한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.19.01
해당된다면 시험자는 개발 문서가 암호모듈이 평문 CSP를 입출력하는 것을 명세하는지 확인한다. 시험자는 개발 문서를 검토하고 암호모듈을 검사하여 평문 CSP의 입출력에 사용되고 신뢰 채널을 이용하는 해당 논리적 인터페이스가 다른 모든 논리적 인터페이스와 논리적으로 분리되는지 확인한다.

TE03.19.02
암호모듈이 평문 CSP를 입출력한다면, 시험자는 신뢰 채널을 이용하는 해당 논리적 인터페이스를 통해 평문 CSP만 입출력되고 다른 데이터, 즉 평문 또는 암호문은 신뢰 채널을 이용하는 해당 논리적 인터페이스를 통해 입출력되지 않는다는 것을 확인해야 한다.

TE03.19.03
시험자는 벤더가 제공한 근거의 정확성을 확인해야 한다. 벤더는 해당 근거에 대한 증명을 제시해야 한다. 만약 그 근거가 부정확하거나 모호한 부분이 있다면 시험자는 벤더에게 추가 정보를 요구해야 한다.

TE03.19.04
시험자는 통신 링크에 접근을 시도해 신뢰 채널이 통신 링크상에서 비인가된 변경, 대체 및 노출을 방지하는지 확인해야 한다.

AS03.20: (신뢰 채널 – 보안수준 3, 4)

신원 기반 인증은 신뢰 채널을 이용하는 모든 서비스에 적용되어야 한다.

[벤더 요구사항]

VE03.20.01
벤더는 신뢰 채널에 사용되는 인증 메커니즘를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.20.01
시험자는 신뢰 채널을 이용하는 모든 서비스에 대해 신원 기반 인증 메커니즘이 적용되었는지 확인해야 한다. 시험자는 운영자 인증을 성공적으로 통과하지 않는 한 신뢰 채널을 이용하는 서비스가 제공되지 않음을 확인해야 한다.

AS03.21: (신뢰 채널 – 보안수준 3, 4)

신뢰 채널이 사용될 때는 상태 표시기가 제공되어야 한다.

[벤더 요구사항]

VE03.21.01
벤더는 신뢰 채널이 사용될 때 제공되는 표시기에 대해 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.21.01
시험자는 암호모듈을 실행하여 신뢰 채널이 사용될 때 상태 표시기가 제공되는지 확인해야 한다.

AS03.22: (신뢰 채널 – 보안수준 4)

보안수준 4는 보안수준 3의 보안 요구사항에 추가하여 신뢰 채널을 이용하는 모든 서비스에 다중체계 신원 기반 인증이 적용되어야 한다.

[벤더 요구사항]

VE03.22.01
벤더는 신뢰 채널에 사용되는 다중체계 신원 기반 인증 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE03.22.01
시험자는 다중체계 신원 기반 인증 메커니즘이 신뢰 채널을 이용하는 모든 서비스에 제공되는지 확인해야 한다. 시험자는 운영자 인증을 통과하지 않는 한 신뢰 채널을 이용하는 서비스가 제공되지 않음을 확인해야 한다.

6.4 역할, 서비스 및 인증

6.4.1 역할, 서비스 및 인증 일반 요구사항

AS04.01: (역할, 서비스 및 인증 – 보안수준 1, 2, 3, 4)

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

비고 해당 시험 항목은 **AS04.11**에서 시험된다.

AS04.02: (역할, 서비스 및 인증 – 보안수준 1, 2, 3, 4)

암호모듈이 복수 운영자가 모듈을 동시에 이용하는 것을 지원하는 경우, 암호모듈은 내부적으로 각 운영자의 역할과 이에 상응하는 서비스를 분리하여 유지할 수 있어야 한다.

[벤더 요구사항]

VE04.02.01
벤더는 복수 운영자가 동시에 암호모듈을 이용하도록 허용할지 여부를 개발 문서에 명세해야 한다. 개발 문서는 각 운영자별로 할당되어 있는 인가된 역할 및 서비스를 분리하는 방법을 서술해야 하고, 동시에 이용하는 복수 운영자에 대한 모든 제한 사항을 서술해야 한다.

보기 1 유지 관리 역할을 맡는 운영자와 사용자 역할을 맡은 운영자는 동시에 허가되지 않는다.
보기 2 하나의 사용자 역할로 16명의 복수 운영자가 지원하나, 암호모듈에서 한 번에 오직 하나의 RSA 키 생성이 동작될 수 있다.

보기 3 암호 관리자 역할에서 복수 운영자가 로그인 할 경우, 각 암호 관리자는 다른 운영자의 인증 데이터를 변경할 수 있다.

[시험 절차]

TE04.02.01
시험자는 개발 문서를 검토하여 암호모듈이 복수의 운영자에 의해 실행되는 역할과 서비스를 분리하는 방법이 서술되어 있는지 확인해야 한다.

TE04.02.02
시험자는 두 명의 독립적인 운영자(운영자 1과 운영자 2)의 상이한 역할을 설정해야 한다. 시험자는 각 역할에 할당된 서비스만이 그 역할에서 실행될 수 있는지 확인해야 한다. 또한 동시에 복수 운영자가 암호모듈을 사용할 수 있는 경우, 운영자별 역할과 서비스가 분리되는지 검증하기 위해서 한 운영자가 다른 운영자가 맡고 있는 역할에 상응하는 서비스를 이용할 수 있는지 시험해야 한다.

TE04.02.03
개발 문서에서 암호모듈을 동시에 사용하는 복수 운영자에 대한 제한을 명세하고 있을 경우, 시험자는 암호모듈의 복수 운영자들의 역할을 담당하여 해당 운영자 역할을 위반하는 사항을 시험해야 하고, 이를 방지하는 제한 조치를 암호모듈이 수행하고 있는지 확인해야 한다.

AS04.03: (역할 – 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790 **부속서**} **A.2.4**를 충족하는 개발 문서가 제출되어야 한다.

[벤더 요구사항]

VE04.03.01
벤더는 {KS X ISO/IEC 19790 **부속서**} **A.2.4**가 충족되는 개발 문서를 제출해야 한다.

[시험 절차]

TE04.03.01
시험자는 개발 문서에서 {KS X ISO/IEC 19790 **부속서**} **A.2.4**에 위반되는 것이 있는지 확인해야 한다.

6.4.2 역할

AS04.04: (역할 – 보안수준 1, 2, 3, 4)

암호모듈은 적어도 하나의 암호 관리자 역할을 지원해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.05**의 일부분으로 시험된다.

AS04.05: (역할 – 보안수준 1, 2, 3, 4)

암호 관리자 역할은 암호 초기화나 관리 기능 및 일반 보안 서비스를 수행하는 역할이어야 한다(예: 암호모듈의 초기화, PSP와 CSP의 관리, 감사 기능).

[벤더 요구사항]

VE04.05.01: 개발 문서에서는 최소 한 명의 암호 관리자 역할을 포함해야 한다. 역할의 명칭과 이에

따른 서비스가 명세되어야 한다.

[시험 절차]

TE04.05.01
시험자는 개발 문서를 검토하고, 적어도 하나의 암호 관리자 역할이 정의되어 있는지 확인해야 한다. 시험자는 역할의 명칭과 **AS04.05**에 따르는 서비스가 개발 문서에 명세되어 있는지 확인해야 한다.

AS04.06: (역할 – 보안수준 1, 2, 3, 4)

암호모듈이 사용자 역할을 지원하면, 사용자 역할은 암호 기능과 검증대상 암호알고리즘을 포함한 일반 보안 서비스를 수행하는 것이다.

[벤더 요구사항]

VE04.06.01
암호모듈이 사용자 역할을 지원하면, 개발 문서는 ① 사용자 역할이 제공되는지 명확히 명시하고, ② 역할의 명칭과 그 명칭에 따른 서비스를 명세해야 한다.

[시험 절차]

TE04.06.01
시험자는 개발 문서를 검토하여 사용자 역할이 제공되는지 확인해야 한다. 만약 사용자 역할을 제공한다면 이 역할의 명칭과 허용된 서비스가 명세되어 있는지 확인해야 한다.

AS04.07: (역할 – 보안수준 1, 2, 3, 4)
모든 보호되지 않은 SSP는 암호모듈이 유지보수 역할로 들어가거나 혹은 벗어날 때 제로화되어야 한다.

[벤더 요구사항]

VE04.07.01
만약 암호모듈이 유지보수 인터페이스를 가진다면, 개발 문서는 ① 유지보수 역할이 제공되는지를 명확히 명시하고, ② 역할의 이름, 목적 및 상응되는 서비스를 전부 명시해야 하고, ③ VE07.11.01에 따라 유지보수 인터페이스를 명세해야 한다.

VE04.07.02
개발 문서에 KS X ISO/IEC 19790의 **AS04.07**에 정의된 바와 같이 SSP들이 유지보수 역할로 들어가거나 빠져나올 때 어떠한 방식으로 제로화되는지 서술해야 한다.

[시험 절차]

TE04.07.01
시험자는 모듈 인터페이스의 명세를 확인하여 유지보수 인터페이스가 명세되어 있는지 확인해야 한다(**AS07.11** 참조). 그러한 경우 개발 문서를 검토하여 인가된 역할을 확인하고 유지보수 역할의 명칭, 목적, 허용된 서비스가 명세되어 있는지 확인한다.

TE04.07.02
시험자는 모듈 인터페이스의 명세에서 유지보수 인터페이스가 정의되어 있는지 확인하고 개발 문서에 서술된 대로 암호모듈의 보호되지 않은 SSP가 제로화되는지 확인해야 한다.

TE04.07.03
유지보수 역할 중일 때 시험자는 보호되지 않은 SSP값에 대해서 제로화를 검증하는 데 효율적인 것으로 알려진 값을 입력하고, 유지보수 역할을 빠져나올 때 제로화되는지 확인해야 한다.

6.4.3 서비스

6.4.3.1 서비스 일반 요구사항

AS04.08: (서비스 – 보안수준 1, 2, 3, 4)

서비스는 모듈에서 수행되는 모든 동작, 서비스, 기능으로 정의된다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.09: (서비스 – 보안수준 1, 2, 3, 4)

서비스 입력은 특정 서비스, 동작 또는 기능을 시작하거나 동작하기 위해 암호모듈로 입력되는 데이터 입력과 제어 입력으로 구성된다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.10: (서비스 – 보안수준 1, 2, 3, 4)

서비스 출력은 서비스 입력에 의해 시작되거나 수행되는 서비스, 동작 및 기능으로부터 얻어지는 데이터 출력과 상태 출력으로 구성된다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.11: (서비스 – 보안수준 1, 2, 3, 4)

각 서비스 입력의 결과로 서비스 출력이 생성된다.

[시험 절차]

TE04.11.01
시험자는 개발 문서에 각 서비스의 목적과 기능이 서술되어 있는지 확인해야 한다. 시험자는 개발 문서를 검토하여 서비스 입력, 이에 대응하는 서비스 출력, 인가된 역할과 그 서비스를 실행할 수 있는 역할이 각 서비스에 규정되어 있는지 확인해야 한다.

TE04.11.02
시험자는 각 서비스(보안 및 비보안 서비스, 검증 및 비검증 서비스)에 대하여 다음 항목을 수행해야 한다.

- 각 서비스 입력을 수행하고, 서비스 출력을 확인한다.
- 어떤 역할이 필요한 서비스에 대해서는, 그 역할을 맡아서 명세된 대로 서비스 입력을 수행하고 명세된 서비스 출력이 되는지 확인한다.
- 어떤 역할이 필요한 서비스에 대해서, 그 서비스에 대응되지 않은 역할을 맡아서 명세된 서비스 입력을 수행하고 서비스가 제공되지 않는 것을 확인한다.
- 어떤 인증된 역할을 필요로 하는 서비스에 대해서, 그 역할을 맡아서 암호모듈로부터 인증받고 명

세된 대로 서비스 입력을 수행하고 명세된 서비스 출력이 되는지 확인한다.
- 어떤 인증된 역할을 필요로 하는 서비스에 대해서, 그 역할을 맡아서 암호모듈로부터의 인증에 실패하도록 인증 데이터를 변경하고 명세된 서비스 입력을 수행하고 서비스가 제공되지 않는 것을 확인한다.
- 데이터 출력 인터페이스를 통하여 데이터 출력을 하는 서비스에 대해서, 시험자는 출력된 결과가 예상한 출력과 같은지 확인해야 한다.

보기 어떤 서비스가 서비스 데이터 입력에 대한 함수를 수행한 결과로 데이터 출력을 제공한다면, 시험자는 제공된 입력에 대한 함수를 수행한 결과가 데이터 출력으로 나타나는지 확인해야 한다.

AS04.12: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 운영자에게 다음 서비스를 제공해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

모듈의 버전 정보 표시

AS04.13: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 검증 목록과 관련된 명칭 또는 모듈 식별자 그리고 버전 정보(예: 하드웨어, 소프트웨어 또는 펌웨어 버전 정보)를 출력해야 한다.

[벤더 요구사항]

VE04.13.01
개발 문서에는 암호모듈의 현재 명칭과 버전 정보가 기술되어야 한다.

VE04.13.02
개발 문서는 검증 목록을 제공할 암호모듈의 명칭과 버전 정보를 제공해야 한다.

VE04.13.03
개발 문서, 보안정책서, 안내서는 현재 암호모듈의 이름과 버전 정보가 검증 목록과 어떻게 연관되는지 명세해야 한다.

[시험 절차]

TE04.13.01
시험자는 서비스 출력(명칭, 모듈 식별자, 버전 정보)들이 **AS02.11**, **AS02.12**, **AS11.04**의 요구사항에 대한 명세와 일치함을 확인해야 한다.

TE04.13.02
시험자는 개발 문서(보안정책서, 안내서)가 모듈의 버전을 명확하게 식별하는 충분한 정보를 제공하는지 확인해야 한다.

TE04.13.03
시험자는 보안정책서나 안내서를 검토하고 암호모듈의 명칭 또는 식별자, 버전 정보의 출력을 통하여 운영자가 암호모듈과 검증 목록을 충분히 연관시킬 수 있는지 확인해야 한다.

상태 표시

AS04.14: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 현재 상태 정보를 출력해야 한다.

[벤더 요구사항]

VE04.14.01
개발 문서에 암호모듈의 현재 상태의 출력에 대한 내용을 명세해야 한다.

[시험 절차]

TE04.14.01
시험자는 개발 문서를 통해 상태 표시 서비스가 적어도 하나 이상의 인가된 역할에 할당되어 있는 것을 확인해야 한다. 시험자는 이러한 서비스가 **AS04.14** 항목을 준수하는지 확인해야 한다.

TE04.14.02
시험자는 '상태 표시'와 개발 문서가 일치하는지 확인해야 한다.

자가시험 수행

AS04.15: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 {KS X ISO/IEC 19790} **7.10.2**에 명세된 대로 동작 전 자가시험을 수행해야 한다.

[벤더 요구사항]

VE04.15.01
개발 문서에 사용자가 호출할 수 있는 자가시험의 초기화 및 실행에 대해 명세해야 한다.

[시험 절차]

TE04.15.01
시험자는 모듈이 {KS X ISO/IEC 19790} **7.10**에 명세된 대로 동작 전 자가시험의 초기화 및 실행을 제공하는지 확인해야 한다. 이는 TEA.01.01의 문서를 기반으로 수행된다.

검증대상 암호알고리즘 수행

AS04.16: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 {KS X ISO/IEC 19790} **7.2.4**에 명시된 대로 검증대상 동작모드에서 사용되는 검증대상 암호알고리즘을 적어도 한 개 이상 수행해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

제로화 수행

AS04.17: (서비스 – 보안수준 1, 2, 3, 4)

암호모듈은 {KS X ISO/IEC 19790} **7.9.7**에 명시된 대로 파라미터의 제로화를 수행해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

6.4.3.2 우회 기능

AS04.18: (우회 기능 – 보안수준 1, 2, 3, 4)

암호모듈이 특정 데이터나 상태값을 암호로 보호된 형태(예: 암호문)로 출력할 수 있고, 또한 이들을 (모듈의 설정이나 운영자 개입의 결과로) 보호되지 않은 형태(예: 평문)로도 출력할 수 있다면 우회 기능이 정의되어 있어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.19: (우회 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 우회 기능이 구현된 경우, 인가된 역할의 사용자만이 우회 기능을 설정할 수 있다.

[벤더 요구사항]

VE04.19.01
암호모듈에 우회 기능이 구현되어 있는 경우, 개발 문서에는 **AS04.19**에 규정되어 있는 우회 서비스를 명세해야 한다.

VE04.19.02
유한 상태 모델 및 개발 문서에는 배타적 우회 상태나 선택적 우회 상태에 대하여, 각 우회 상태 사이에 전환하는 데 필요한 두 개의 독립된 내부 조치를 명세해야 한다.

[시험 절차]

TE04.19.01
시험자는 우회 기능이 모듈에 구현되어 있는지 확인해야 한다. 시험자는 개발 문서를 검토하여 우회 기능이 적어도 하나의 인가된 역할에 할당되는지 확인해야 한다.

TE04.19.02
시험자는 유한 상태 모델 및 개발 문서를 통하여 어떤 우회 상태로의 전환은 배타적 우회 상태 혹은 선택적 우회 상태로 전환시키는 데 필요한 두 개의 독립된 내부 조치가 암호모듈에서 모두 동작하는지 확인해야 한다.

TE04.19.03
시험자는 각 우회 상태에서 각각 다른 우회 상태로의 전환을 시도하고 그 전환이 두 개의 내부 조치를 거쳐 일어나는지 확인해야 한다.

AS04.20: (우회 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 우회 기능이 구현된 경우, 단순한 오류로 인한 평문 데이터의 의도하지 않은 유출을 방지하기 위해 우회 기능을 활성화하는 두 개의 독립된 내부 조치가 요구되어야 한다.

[벤더 요구사항]

VE04.20.01
암호모듈이 우회 기능이 구현되어 있을 경우, 개발 문서에 **AS04.20**에 규정된 우회 서비스를 명세해야 한다.

VE04.20.02
유한 상태 모델 및 개발 문서에 배타적 또는 선택적 우회 상태에 대하여 각 우회 상태로 전환하는데 필요한 두 개의 독립 내부 조치를 명세해야 한다.

[시험 절차]

TE04.20.01
시험자는 우회 기능이 모듈에 의해서 구현되었는지 여부를 확인해야 한다. 시험자는 우회 기능이 적어도 하나의 인가된 역할에 할당되었는지 개발 문서를 확인해야 한다.

TE04.20.02
암호모듈이 배타적 우회 상태 혹은 선택적 우회 상태로 전환될 때 두 개의 독립적인 내부 조치가 작동하는 것을 유한 상태 모델 및 개발 문서를 통하여 확인해야 한다.

TE04.20.03
시험자는 각 우회 상태에서 각각 다른 우회 상태로의 전환을 시도하여 전환이 일어나는지 확인해야 하고, 그 전환이 두 개의 내부 작동을 거쳐 일어나는지 확인해야 한다.

AS04.21: (우회 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 우회 기능이 구현된 경우, 두 개의 독립된 내부 조치가 우회 기능만을 수행하는 전용 소프트웨어 혹은 하드웨어를 작동할 수 있어야 한다.

[벤더 요구사항]

VE04.21.01
암호모듈에 우회 기능이 구현된 경우, 개발 문서에 두 개의 독립된 내부 조치가 우회 기능만을 수행하는 전용 소프트웨어 또는 하드웨어를 작동시키는 방법을 명세해야 한다.

VE04.21.02
개발 문서에 두 개의 독립된 내부 조치가 단순한 오류로 인한 의도하지 않은 평문 데이터의 출력을 방지하는 방법을 명세해야 한다.

[시험 절차]

TE04.21.01
시험자는 개발 문서를 검토하여 두 개의 독립된 내부 조치가 단순 오류로 인한 우회로 출력되는 평문 데이터를 방지하는 방법을 확인해야 한다.

TE04.21.02
시험자는 각 상태에서 각 우회 상태로의 전환을 시도하고 검사하여 두 개의 독립된 내부 조치가 우회 기능만 수행하는 전용 소프트웨어 혹은 하드웨어를 작동시키는지 확인해야 한다.

AS04.22: (우회 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 우회 기능이 구현된 경우 그 모듈은 다음과 같이 우회 기능의 상태를 표시해야 한다:

a) 우회 기능이 비활성화 상태이고 모듈은 암호 처리만을 제공한다(예: 평문의 암호화).
b) 우회 기능이 활성화 상태이고 모듈은 암호 처리를 제외한 서비스만 제공한다(평문을 암호화하지 않음).
c) 우회 기능이 선택적으로 활성화, 비활성화되며, 일부 서비스는 암호 처리와 함께, 일부 서비스는 암호 처리 없이 제공한다(예: 복수 통신 채널을 가진 모듈의 경우 평문 데이터는 각 채널 설정에 따라 암호화되거나 또는 암호화되지 않는다).

[벤더 요구사항]

VE04.22.01
개발 문서에 상태 표시 서비스가 우회 상태를 표시하는지 나타내야 한다.

[시험 절차]

TE04.22.01
시험자는 상태 표시 서비스를 명세한 개발 문서를 검토하여 우회 상태 표시를 확인해야 한다.

TE04.22.02
시험자는 각 우회 상태로 전환하고 상태 표시기가 해당되는 우회 상태를 표시하는지 확인해야 한다.

6.4.3.3 자가 초기화된 암호 출력 기능

AS04.23: (자가 초기화된 암호 출력 기능 – 보안수준 1, 2, 3, 4)

자가 초기화된 암호 출력 기능은 암호 관리자에 의해 설정되고, 이러한 설정은 모듈의 리셋, 재부팅 또는 전원 재인가 시 보존되어야 한다.

[벤더 요구사항]

VE04.23.01
벤더는 자가 초기화된 암호 출력 기능을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE04.23.01
시험자는 자가 초기 암호 출력 기능이 암호 관리자에 의해서만 설정될 수 있는지 확인해야 한다.

AS04.24: (자가 초기 암호 출력 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 자가 초기 암호 출력 기능이 구현된 경우, 단순 오류로 인한 의도하지 않은 출력을 방지하기 위해 두 개의 독립된 내부 조치가 필요하다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.25**의 일부분으로 시험된다.

AS04.25: (자가 초기 암호 출력 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 자가 초기화된 암호 출력 기능이 구현된 경우, 두 개의 독립된 내부 조치를 통해서만 암호 출력 기능을 조정하는 전용 소프트웨어 혹은 하드웨어를 동작시킬 수 있어야 한다(예: 두 개의 서로 다른 소프트웨어 또는 하드웨어 플래그를 설정하고 그중 하나는 사용자가 시작시키도록 한다).

[벤더 요구사항]

VE04.25.01
벤더는 자가 초기화된 암호 출력 기능을 활성화하기 위해 독립적으로 수행되는 두 개의 내부 조치를 정의해야 한다.

VE04.25.02
벤더는 두 개의 독립된 내부 조치가 자가 초기화된 암호 출력 기능만을 조정하는 전용 소프트웨어 혹은 하드웨어를 동작시키는 방법을 명세한 개발 문서를 제출해야 한다.

VE04.25.03
벤더는 두 개의 독립된 내부 조치에 의해 단순한 오류로 인한 의도하지 않은 출력을 방지하는 방법을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE04.25.01
시험자는 암호모듈에 자가 초기화된 암호 출력 기능이 구현되었는지 확인해야 한다. 시험자는 개발 문서를 검토하여 자가 초기화된 암호 출력 기능이 활성화되기 전에 암호모듈에 의해 수행되는 두 개의 독립된 내부 조치를 확인해야 한다. 시험자는 개발 문서를 통하여 두 개의 독립된 내부 조치에 의해 단순한 오류로 인한 의도하지 않은 출력을 방지하는 방법을 확인해야 한다.

TE04.25.02
시험자는 자가 초기화된 암호 출력 기능을 활성화시켜 두 개의 독립된 내부 조치가 명시된 대로 작동하는지 확인해야 한다. 이때 프로세스가 활성화될 때 어떤 소프트웨어 구성 요소나 펌웨어 구성 요소가 실행된다면, 시험자는 소프트웨어 구성 요소 또는 펌웨어 구성 요소가 두 개의 독립적인 내부 조치에 대한 요구사항을 지원하는지 확인하기 위해 자가 초기화된 암호 출력 기능이 동작하기 전에 그에 해당되는 소스 코드를 검사해야 한다.

TE04.25.03
시험자는 자가 초기화된 암호 출력 기능이 활성화됨을 표시하는 상태 표시기가 제공되는지 확인해야 한다.

AS04.26: (자가 초기화된 암호 출력 기능 – 보안수준 1, 2, 3, 4)

암호모듈에 자가 초기화된 암호 출력 기능이 구현된 경우, 모듈은 그 기능이 활성화되었는지 상태를 표시해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.25**의 일부분으로 시험된다.

6.4.3.4 소프트웨어/펌웨어 로드

AS04.27: (소프트웨어/펌웨어 로드 – 보안수준 1, 2, 3, 4)

암호모듈이 소프트웨어나 펌웨어를 외부로부터 로드하는 기능을 가지고 있으면 다음과 같은 요구사항을 만족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.28**의 일부분으로 시험된다.

AS04.28: (소프트웨어/펌웨어 로드－보안수준 1, 2, 3, 4)

로드되는 소프트웨어나 펌웨어의 검증을 유지하기 위해서 로드되어 암호모듈에 사용되기 전에 소프트웨어 또는 펌웨어는 검증기관(validation authority)에 의해 검증받아야 한다.

[벤더 요구사항]

VE04.28.01
벤더는 로드 대상 소프트웨어 또는 펌웨어가 검증받았다는 사실을 제공해야 한다. 검증대상 암호모듈의 암호 정책 문서는 암호모듈에 로드되는 소프트웨어 또는 펌웨어를 명확하게 식별할 수 있어야 한다.

[시험 절차]

TE04.28.01
시험자는 암호모듈에 로드되는 소프트웨어 또는 펌웨어 버전이 검증대상 암호모듈의 암호 정책을 명세한 개발 문서를 준수하는지 확인한다. 이러한 식별은 KS X ISO/IEC 19790의 **7.2.3.1**에서 확인한 사항과 일치해야 한다.

AS04.29: (소프트웨어/펌웨어 로드－보안수준 1, 2, 3, 4)

데이터 출력 인터페이스를 통한 데이터 출력은 소프트웨어 또는 하드웨어에 대한 로드와 로드 시험이 성공된 후 실행되어야 한다.

[벤더 요구사항]

VE04.29.01
벤더는 소프트웨어 또는 하드웨어를 로드하는 과정에서와 로드 시험을 하는 중에 데이터 출력을 방지하는 프로세스를 개발 문서에 명세해야 한다.

[시험 절차]

TE04.29.01
시험자는 소프트웨어 또는 하드웨어가 로드되는 과정에서와 로드 시험이 되는 중에 데이터가 출력되지 않음을 확인해야 한다.

AS04.30: (소프트웨어/펌웨어 로드－보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790} **7.10.3.4**에 명시된 소프트웨어·펌웨어 로드 시험은 로드된 코드가 실행되기 전에 수행되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS10.37**～**AS10.41**의 일부분으로 시험된다.

AS04.31: (소프트웨어/펌웨어 로드－보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790} **7.10.2**에 명시된 사전 동작 시험이 성공적으로 완료되기 전까지 모든 로드 또는 변경된 검증대상 암호알고리즘의 실행을 보류해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS10.37**～**AS10.41**의 일부분으로 시험된다.

AS04.32: (소프트웨어/펌웨어 로드 – 보안수준 1, 2, 3, 4)

모듈의 버전 정보는 새로 로드된 소프트웨어 또는 펌웨어의 추가 및 업데이트를 반영하여 변경되어야 한다({KS X ISO/IEC 19790} **7.4.3**).

[벤더 요구사항]

VE04.32.01
벤더는 새로 로드된 소프트웨어 또는 펌웨어의 버전을 읽을 수 있는 방법을 제공해야 한다.

[시험 절차]

TE04.32.01
시험자는 소프트웨어/펌웨어 로드 시험을 시작해야 한다. 소프트웨어/펌웨어 로드 시험 후에 전원인가 시험이 성공적으로 완료된 후, 시험자는 새로 로드된 소프트웨어 또는 펌웨어의 추가 또는 업데이트를 반영하여 버전 정보가 변경되었는지 확인해야 한다.

AS04.33: (소프트웨어/펌웨어 로드 – 보안수준 1, 2, 3, 4)

새로운 소프트웨어 또는 펌웨어 로드로 전체 이미지가 대체되면, 이 전체 이미지는 검증을 유지하기 위해 검증기관의 신규 검증이 필요한 완전히 새로운 모듈로 간주된다.

[벤더 요구사항]

VE04.33.01
벤더는 모듈이 소프트웨어/펌웨어 로드 시험의 결과로 전체 이미지 변경이 일어나는지를 명세한 개발 문서를 제출해야 한다.

VE04.33.02
벤더는 로드된 소프트웨어/펌웨어에 의해 전체 이미지가 변경되었다면, 검증기관으로부터 변경된 전체 이미지에 대하여 검증받은 사실을 제공해야 한다.

검증대상 암호모듈의 보안정책을 서술한 개발 문서는 암호모듈에 로드된 소프트웨어 또는 하드웨어를 명확하게 식별해야 한다.

[시험 절차]

TE04.33.01
시험자는 **AS04.13**에 표시된 대로 이름과 버전을 검사해 새로 일어난 전체 이미지 대체물이 검증기관에 의해 검증받았는지 확인해야 한다.

AS04.34: (소프트웨어/펌웨어 로드 – 보안수준 1, 2, 3, 4)

새로운 소프트웨어 또는 펌웨어 이미지는 전원 인가 리셋을 통해 모듈 전환이 완료된 후 실행되어야 한다.

[벤더 요구사항]

VE04.34.01
암호모듈의 전체 이미지 대체가 지원되면, 벤더는 개발 문서에 전원 인가 리셋을 통해 모듈이 전환

된 후에 새로운 이미지가 실행되는 방법을 명세해야 한다.

[시험 절차]

TE04.34.01
시험자는 소프트웨어/펌웨어 로드 시험을 시작한다. 로드 시험이 통과된 후 시험자는 전원 인가 리셋 수행을 통해 동작 전 자가시험이 성공적으로 통과되기 전까지 로드된 소프트웨어 또는 하드웨어가 사용될 수 없음을 확인해야 한다.

AS04.35: (소프트웨어/펌웨어 로드 – 보안수준 1, 2, 3, 4)

새로운 이미지가 실행되기 전에 모든 SSP는 제로화되어야 한다.

[벤더 요구사항]

VE04.35.01
이미지 전체 교체가 지원되면 벤더는 개발 문서에 SSP의 제로화가 새로운 이미지의 실행 이전에 이루어짐을 명세해야 한다.

VE04.35.02
이미지 전체 교체물이 지원되면 벤더는 개발 문서에 SSP 제로화에 대한 다음과 같은 정보를 명세해야 한다.

a) 제로화 방법
b) 제로화 방법이 SSP가 손상되지 않을 시간 내에 수행된다는 근거

[시험 절차]

TE04.35.01
시험자는 개발 문서를 검토하여 VE04.35.01에 명세된 정보가 있는지 확인해야 한다. 시험자는 벤더에 의해 제시된 근거의 정확성을 판단해야 한다. 이를 증명할 의무는 벤더에게 있다. 만약 개발 문서에 명세된 내용이 명확하지 않는 경우, 시험자는 필요에 따라 벤더에게 추가 정보의 작성을 요구해야 한다.

TE04.35.02
시험자는 모듈 내에 어떤 키가 존재하는지 확인하고 소프트웨어/펌웨어 로드 시험 후에 전원 인가 리셋을 수행한다. 동작 전 자가시험이 완료되면, 시험자는 모듈에 저장되어 있었던 각각의 SSP를 이용한 암호 연산을 시도하여 각각의 SSP에 대해 접근할 수 없음을 확인해야 한다.

6.4.4 인증

역할 기반 인증

AS04.36: (역할 기반 인증 – 보안수준 2, 3, 4)

암호모듈이 역할 기반 인증 메커니즘을 지원하면, 운영자는 암시적 또는 명시적으로 하나 이상의 역할을 선택해야 하고 {선택된 역할(또는 역할들의 집합)이 잘 부여되었는지 확인해야 한다}.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.37**의 일환으로 시험된다.

AS04.37: (역할 기반 인증 – 보안수준 2, 3, 4)

{암호모듈이 역할 기반 인증 메커니즘을 지원하면, 운영자는 암시적 또는 명시적으로 하나 이상의 역할을 선택해야 하고} 선택된 역할(또는 역할들의 집합)이 잘 부여되었는지 확인해야 한다.

[벤더 요구사항]

VE04.37.01
벤더는 암호모듈이 수행하는 인증의 종류를 명세한 개발 문서를 제출해야 한다. 벤더는 개발 문서에 역할 또는 역할들의 집합을 암시적, 명시적으로 선택하는 메커니즘과 역할을 맡은 운영자를 인증하는 방법을 명세해야 한다.

[시험 절차]

TE04.37.01
시험자는 개발 문서에 하나 또는 그 이상의 역할을 선택하는 메커니즘과 이를 맡는 운영자를 인증하는 방법이 명시되어 있는지 확인해야 한다.

TE04.37.02
시험자는 각 역할을 부여하고 그 역할을 맡은 상태에서, 인증 수행 도중에 오류를 발생시켜 암호모듈이 각 역할에 대한 접근을 거부하는지 확인해야 한다.

AS04.38: (역할 기반 인증 – 보안수준 2, 3, 4)

암호모듈이 운영자의 역할 변경을 허용하는 경우, 암호모듈은 그 운영자가 이전에 인증받지 않은 역할을 인증해야 한다.

[벤더 요구사항]

VE04.38.01
개발 문서에 운영자가 역할을 변경하기 위해 필요한 조건을 서술해야 하고, 새로운 역할에 대한 운영자 인증이 필요하다는 것을 명시해야 한다.

[시험 절차]

TE04.38.01
시험자는 개발 문서를 검토하여 운영자가 역할을 변경할 수 있는 방법과 새로운 역할에 대한 운영자 인증이 포함되어 있는지 확인해야 한다.

TE04.38.02: 시험자는 다음 시험을 수행해야 한다.

a) 운영자는 하나의 역할을 맡고 나서 맡은 역할을 인가된 다른 역할로 변경해 본 후, 암호모듈이 운영자에게 새로운 역할에 할당된 서비스를 허용하는지 확인한다.
b) 운영자는 하나의 역할을 맡고 나서 맡은 역할을 인가되지 않은 다른 역할로 변경해 본 후, 암호모듈이 운영자에게 새로운 역할에만 할당된 서비스를 허용하지 않는지 확인한다.

신원 기반 인증

AS04.39: (신원 기반 인증 – 보안수준 3, 4)

암호모듈이 신원 기반 인증 메커니즘을 지원하면, 암호모듈은 운영자가 개별적이고 유일하게 식별될 것을 요구해야 한다. {운영자에 의해 선택된 하나 이상의 암시적 또는 명시적 역할을 요구해야 한다. 또한 운영자가 선택된 역할을 맡을 권한이 있는지 여부와 함께 운영자의 신원을 인증해야 한다.}

[벤더 요구사항]

VE04.39.01
벤더는 암호모듈에 구현된 인증의 종류를 명세한 개발 문서를 제출해야 한다. 벤더는 운영자를 식별하고, 운영자의 신원을 인증하고, 운영자의 역할 또는 역할들의 집합을 암시적이거나 명시적으로 선택하고, 역할을 맡은 운영자 인증 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE04.39.01
시험자는 개발 문서를 검토하여 운영자를 유일하게 식별하는 방법, 신원을 인증하는 방법, 운영자가 역할을 선택하는 방법, 그리고 신원 기반 인증에 의한 운영자 권한 부여 방법을 확인해야 한다.

TE04.39.02
시험자는 인증 수행 중 오류를 발생시켜 암호모듈의 인증 과정이 더 이상 진행되지 않는지 여부를 확인해야 한다.

TE04.39.03
시험자는 암호모듈에 대해 자신의 신원 인증을 성공적으로 수행해야 한다. 하나 또는 그 이상의 역할 선택이 요구될 때, 인증된 신원에 적합하지 않은 역할을 선택하고 권한이 부여되지 않는지 확인해야 한다.

AS04.40: (신원 기반 인증 – 보안수준 3, 4)

{암호모듈이 신원 기반 인증 메커니즘을 지원한다면 암호모듈은 운영자가 개별적이고 유일하게 식별되어야 하며} 운영자가 하나 이상의 역할을 암시적이거나 명시적으로 선택하도록 요구해야 한다. {또한 운영자가 선택된 역할을 맡을 권한을 가지고 있는지 여부와 운영자의 신원을 인증해야 한다.}

[벤더 요구사항]

VE04.40.01
개발 문서에 운영자의 역할 변경에 필요한 조건이 기술되어야 하며, 새로운 역할에 대한 운영자 인증이 필요하다는 것을 명세해야 한다.

[시험 절차]

TE04.40.01
운영자 신원의 재인증 없이(이전에 인증되지 않은 역할에 대한 권한을 검증하는 것을 포함) 운영자가 역할을 변경할 수 있는 방법에 대해서 시험자는 개발 문서를 통해 확인해야 한다.

TE04.40.02
시험자는 다음 시험을 수행해야 한다.

a) 하나의 역할을 맡은 시험자가 인가된 다른 역할로의 변경을 시도하여, 시험자의 신원을 재인증하지 않는지 검증하고, 시험자가 새로운 역할에 할당된 서비스에 접근할 수 있는지 확인해야 한다. 또한 시험자가 변경된 다른 역할을 맡고 있는지 검증하기 위해서 새로운 역할의 서비스를 수행해

야 한다. 이때 암호모듈이 재인증을 요구하지 않으면 해당 시험 절차는 실패한 것으로 판정된다.
b) 하나의 역할을 맡은 시험자가 인가되지 않은 역할로의 변경을 시도해 보고 암호모듈이 접근을 거부하는지 확인해야 한다.

AS04.41: (신원 기반 인증 – 보안수준 3, 4)

{암호모듈이 신원 기반 인증 메커니즘을 제공한다면, 암호모듈은 개별적이고 유일하게 운영자를 식별해야 하고, 운영자에 의해 암시적 혹은 명시적으로 선택된 1개 이상의 역할을 요구해야 한다.} 또한 운영자가 선택한 역할 또는 역할의 집합을 맡을 권한이 있는지 여부와 함께 운영자의 신원을 인증해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.42: (신원 기반 인증 – 보안수준 3, 4)

암호모듈이 운영자의 역할 변경을 허용하는 경우, 이전에 인증받지 않았던 역할을 수행하는 식별된 운영자를 인증해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS04.43: (운영자 인증 – 보안수준 1, 2, 3, 4)

암호모듈의 리셋, 재부팅, 전원 재인가 후에 모듈은 운영자를 인증해야 한다.

[벤더 요구사항]

VE04.43.01
암호모듈의 전원이 꺼졌을 때 이전 인증이 소멸되도록 하는 방법을 개발 문서에 명시해야 한다.

[시험 절차]

TE04.43.01
시험자는 개발 문서를 검토하여 암호모듈의 전원을 껐을 때 이전의 인증 효력이 소멸되도록 설계되었는지 확인해야 한다.

TE04.43.02: 시험자는 암호모듈로부터 인증받은 후 암호모듈의 전원을 껐다 다시 켠 다음 이전의 역할에 할당된 서비스를 요청한다. 해당 시험 항목을 충족하기 위해서 암호모듈은 해당 서비스에 대한 수행을 거부하고 재인증을 요구해야 한다.

AS04.44: (운영자 인증 – 보안수준 1, 2, 3, 4)

암호모듈 내의 인증 데이터는 인가되지 않은 사용, 노출, 변경 및 대체로부터 보호되어야 한다.

비고 검증대상 암호알고리즘은 인증 메커니즘의 일부분으로 사용될 수 있다.

[벤더 요구사항]

VE04.44.01
개발 문서에 암호모듈 내의 모든 인증 데이터를 보호하는 방법을 서술해야 한다. 인가되지 않은 노출, 변경, 대체로부터 인증 데이터를 보호하는 메커니즘이 포함되어야 한다.

[시험 절차]

TE04.44.01
시험자는 인가되지 않은 노출, 변경, 대체에 대하여 인증 데이터를 보호하는 방법이 개발 문서에 서술되어 있는지 확인해야 한다.

TE04.44.02
시험자는 다음 시험을 수행해야 한다.

a) 시험자는 (문서화된 보호 메커니즘을 우회하여) 접근 권한이 없는 인증 데이터에 접근을 시도한다. 만약 암호모듈이 인증 데이터에 대한 접근을 거부하거나, 암호화되었거나 기타 방법으로 보호된 데이터에 대한 접근만을 허용한다면 요구사항을 충족하는 것이다.
b) 개발 문서에 명시되지 않은 방법을 사용하여 인증 데이터를 변경하고, 변경된 데이터의 입력을 시도한다. 암호모듈은 시험자가 변경된 데이터를 사용하여 인증받도록 허용해서는 안 된다.

AS04.45: (운영자 인증 – 보안수준 2, 3, 4)

운영자가 암호모듈에 접근하는 것이 처음이어서 암호모듈이 운영자를 인증하기 위한 데이터를 가지고 있지 않다면, 암호모듈에 대한 접근을 통제하고 인증 메커니즘을 초기화하기 위해 다른 인가된 방법(예: 통제 절차, 제품 출하 시 설정된 인증 데이터 또는 기본적으로 설정된 인증 데이터)이 사용되어야 한다.

[벤더 요구사항]

VE04.45.01
인증 메커니즘이 초기화되기 전 암호모듈에 접근하는 방법을 개발 문서에 명시해야 한다.

[시험 절차]

TE04.45.01
시험자는 운영자가 최초로 암호모듈에 접근할 때 운영자를 인증하는 절차가 개발 문서에 명시되어 있는지 확인해야 한다.

TE04.45.02
암호모듈이 초기화되기 전 모듈에 대한 접근 통제 기능이 작동하는 경우, 초기화되지 않은 암호모듈에 오류를 발생시켜 암호모듈이 접근을 거부하는지 확인해야 한다. 시험자는 인가된 역할을 맡아, 개발 문서에 명시된 인증 절차를 따라 인증이 이루어지는지 확인해야 한다. 또 시험자는 암호모듈이 초기화되기 전 인가받지 않은 역할을 맡으려는 시도를 하고, 암호모듈이 이를 거부하는지 확인해야 한다.

TE04.45.03
모듈 접근과 인증 메커니즘 초기화를 위해 기본 설정(default) 인증 데이터가 사용될 경우, 시험자는 최초 인증 후 기본 설정 인증 데이터가 교체되는지 확인해야 한다. 이를 위해 최초 인증 이후에 기본 설정 인증 데이터를 입력하고 암호모듈이 인증을 거부하는지 확인해야 한다.

AS04.46: (운영자 인증 – 보안수준 2, 3, 4)

모듈을 통제하는 데 기본 설정 인증 데이터가 사용될 경우, 최초 인증 후 기본 설정 인증 데이터는 교체되어야 한다({KS X ISO/IEC 19790} **7.9.7**).

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.45**의 일부분으로 시험된다.

AS04.47: (운영자 인증 – 보안수준 2, 3, 4)

암호모듈이 운영자를 인증하는 데 암호알고리즘을 사용할 경우 이들 암호알고리즘은 검증대상 암호알고리즘이어야 한다.

[벤더 요구사항]

VE04.47.01
벤더는 운영자를 인증하는 데 사용하는 암호알고리즘 목록을 명세한 개발 문서를 제출해야 한다.

VE04.47.02
벤더는 각각의 검증대상 암호알고리즘에 대한 수행을 확인할 수 있는 시험서를 제공해야 한다.

[시험 절차]

TE04.47.01
시험자는 운영자 인증에 필요한 암호알고리즘들이 검증대상 암호알고리즘인지 확인해야 한다.

AS04.48: (운영자 인증 – 보안수준 2, 3, 4)

모듈은 {KS X ISO/IEC 19790} **부속서** E에 명시된 대로 검증대상 인증 메커니즘을 구현해야 한다.

[벤더 요구사항]

VE04.48.01
운영자를 인증하는 방법에 사용된 검증대상 인증 메커니즘을 개발 문서에 서술해야 한다.

VE04.48.02
모듈에 검증대상 인증 메커니즘이 구현된 경우, 벤더는 VE02.20.01에 명시된 바와 같이 사전 검토 단계에서 구현 적합성 검증을 수행할 검증대상 암호알고리즘의 목록을 제출해야 한다.

[시험 절차]

TE04.48.01
시험자는 운영자 인증 메커니즘이 검증대상인지 확인해야 한다.

AS04.49: (운영자 인증 – 보안수준 2, 3, 4)

검증대상 인증 메커니즘의 보안 강도는 보안정책 문서에 명시되어야 한다({KS X ISO/IEC 19790} **부속서** B).

비고 해당 시험 항목은 별도로 시험되지 않는다. **ASB.01**의 일부분으로 시험된다.

AS04.50: (운영자 인증 – 보안수준 2, 3, 4)

검증대상 인증 메커니즘을 수행할 때마다 모듈은 인증 객체의 보안 강도를 충족시켜야 한다.

[벤더 요구사항]

VE04.50.01
개발 문서에는 각각의 인증 메커니즘과 허용되는 오류 확률 또는 랜덤 시도 성공 확률이 명시되어야 한다.

[시험 절차]

TE04.50.01
시험자는 개발 문서에 각각의 인증 메커니즘에 대하여 허용되는 오류 확률 또는 랜덤 시도 성공 확률이 명시되었는지 확인해야 한다.

TE04.50.02
시험자는 개발 문서를 통하여 각각의 인증 메커니즘이 목표치를 충족하는지 확인해야 한다.

AS04.51: (운영자 인증 – 보안수준 2, 3, 4)

1분 동안 검증대상 인증 메커니즘을 사용하기 위해 여러 번 시도를 할 경우 모듈은 인증 객체의 보안 강도를 충족해야 한다.

[벤더 요구사항]

VE04.51.01
개발 문서에는 각각의 인증 메커니즘과 그에 따른 1분 동안의 랜덤 시도 성공 확률이 서술되어야 한다.

[시험 절차]

TE04.51.01
시험자는 각각의 인증 메커니즘에 대한 랜덤 시도 성공 확률이 개발 문서에 명시되었는지 확인해야 한다.

TE04.51.02
시험자는 개발 문서를 통하여 랜덤 시도 성공 확률이 목표 사항을 충족할 수 있는지 확인해야 한다.

AS04.52: (운영자 인증 – 보안수준 2, 3, 4)

검증대상 인증 메커니즘은 요구사항에 적합하게 모듈에 구현되어야 하며, 문서로 규정한 통제 절차 또는 보안 규칙(예: 패스워드 크기 제한)에 의존하지 않아야 한다.

[벤더 요구사항]

VE04.52.01
벤더는 인증 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE04.52.01
시험자는 개발 문서를 검토하고 암호모듈을 검사하여 검증대상 인증 메커니즘이 요구사항에 적합하게 구현되었는지 확인해야 하고 문서로 규정한 통제 절차 또는 보안 규칙에 의존하지 않는지 확인해야 한다.

AS04.53: (운영자 인증 – 보안수준 2)

운영체제에 인증 기능이 구현되어 있을 때 인증 메커니즘은 이 조항의 요구사항을 충족해야 한다.

[벤더 요구사항]

VE04.53.01
벤더는 운영체제의 인증 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE04.53.01
시험자는 개발 문서를 검토하고 인증 메커니즘을 검사하여 운영체제에 구현된 검증대상 인증 메커니즘이 해당 요구사항을 충족하는지 확인해야 한다.

AS04.54: (운영자 인증 – 보안수준 2, 3, 4)

인증을 수행하는 동안에 운영자는 피드백되는 인증 데이터를 인식할 수 없어야 한다(예: 입력되고 있는 패스워드를 시각적으로 볼 수 없어야 한다).

[벤더 요구사항]

VE04.54.01
운영자가 인증 데이터를 입력하는 동안 피드백되는 인증 데이터를 인식하지 못하게 하는 방법이 개발 문서에 명세되어야 한다.

[시험 절차]

TE04.54.01
시험자는 개발 문서를 검토하여 데이터가 입력되는 동안 인증 데이터가 인식되지 않는지 확인한다.

TE04.54.02
시험자는 인증 데이터를 입력하여 입력 중에 인증 데이터가 시각적으로 표시되지 않는지 확인해야 한다.

AS04.55: (운영자 인증 – 보안수준 2, 3, 4)

인증을 수행하는 동안 운영자에게 피드백되는 정보로 인해 인증 메커니즘의 (마땅한, 적절한, 필수적인) 강도가 약화되어서는 안 된다.

[벤더 요구사항]

VE04.55.01
운영자가 인증 데이터를 입력할 때 받을 수 있는 피드백 메커니즘을 개발 문서에 명세해야 한다.

[시험 절차]

TE04.55.01
시험자는 개발 문서를 검토하여, 피드백 메커니즘이 인증 데이터를 추정하거나 결정할 수 있는 어떠한 정보도 제공하지 않음을 확인해야 한다.

TE04.55.02
시험자는 각 역할을 맡기 위한 인증 데이터를 입력하여 피드백 메커니즘을 통해 유용한 정보를 얻을 수 없음을 확인해야 한다.

AS04.56: (운영자 인증 – 보안수준 1)

암호모듈이 인증 메커니즘을 제공하지 않는 경우에도 운영자는 암호모듈에서 암시적 또는 명시적으로 하나 이상의 역할을 맡아야 한다.

[벤더 요구사항]

VE04.56.01
벤더는 개발 문서에 모듈에 대해 수행되는 인증 유형을 서술해야 한다. 벤더는 개발 문서에 하나의 역할(들)을 암시적 또는 명시적으로 선택하기 위해서 사용되는 메커니즘과 그 역할을 맡는 운영자의 인증을 서술해야 한다.

VE04.56.02
벤더는 운영자가 암시적 또는 명시적으로 맡을 수 있는 역할의 명세가 보안정책에 포함된 개발 문서를 제출해야 한다.

VE04.56.03
벤더는 운영자가 암시적 또는 명시적으로 역할을 맡게 하는 지침이 보안정책에 포함된 개발 문서를 제출해야 한다.

[시험 절차]

TE04.56.01: 시험자는 벤더가 제공한 개발 문서의 보안정책에 운영자가 맡을 수 있는 역할에 대한 설명과 각 역할을 부여받는 방법이 서술되어 있는지 확인해야 한다.

TE04.56.02: 시험자는 개발 문서의 보안정책에 서술된 방법을 통해 각각의 역할이 암호모듈에 명시적 또는 암시적으로 할당될 수 있는지 확인해야 한다.

AS04.57: (운영자 인증 – 보안수준 2)

암호모듈은 최소한 역할 기반 인증 메커니즘을 사용해 암호모듈에의 접근을 통제해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.13**의 일부분으로 시험된다.

AS04.58: (운영자 인증 – 보안수준 3, 4)

암호모듈은 암호모듈 접근 통제를 위해 신원 기반 인증 메커니즘을 사용해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS04.16**, **AS04.17**의 일부분으로 시험된다.

AS04.59: (운영자 인증 – 보안수준 4)

암호모듈은 암호모듈 접근 통제를 위해 다중체계 신원 기반 인증 메커니즘을 사용해야 한다.

[벤더 요구사항]

VE04.59.01
벤더는 다중체계 신원 기반 인증 메커니즘을 명세한 개발 문서를 제출하고 메커니즘 시험 기능을 제공해야 한다.

[시험 절차]

TE04.59.01
시험자는 개발 문서를 통해 다중체계 신원 기반 인증을 확인하고 암호모듈을 수행시켜 이를 평가해야 한다.

6.5 소프트웨어/펌웨어 보안

AS05.01: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

해당 절의 요구사항은 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소에 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.02**～**AS05.21**의 일부분으로 시험한다.

AS05.02: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790} **A.2.5**를 충족하는 개발 문서가 제출되어야 한다.

[벤더 요구사항]

VE05.02.01
벤더는 KS X ISO/IEC 19790의 **A.2.5**를 충족하는 개발 문서를 제출해야 한다.

[시험 절차]

TE05.02.01
시험자는 KS X ISO/IEC 19790의 **A.2.5**에 명시된 개발 문서를 확인해야 한다.

AS05.03: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

보안수준 1의 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소에는 다음과 같은 요구 사항이 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS05.04: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

모든 소프트웨어와 펌웨어는 {KS X ISO/IEC 19790} **7.11.7**의 요구사항을 충족해야 하며, 설치 전에 변경되어서는 안 된다.

[벤더 요구사항]

VE05.04.01
벤더는 소프트웨어와 펌웨어를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.04.01
시험자는 암호모듈을 검사하여 벤더가 제출한 개발 문서와 암호모듈의 실제 설계가 일치하는지 확인해야 한다.

AS05.05: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

검증대상 무결성 기법을 사용하는 암호 메커니즘은 모듈의 정의된 암호 경계 내에서 모든 소프트웨어 구성 요소와 펌웨어 구성 요소에 다음 중 한 가지 방법을 적용해야 한다.

- 암호모듈 자체로 무결성 검증
- 다른 검증대상 암호모듈의 검증대상 동작모드에서 무결성 검증

[벤더 요구사항]

VE05.05.01
벤더는 암호모듈의 모든 소프트웨어 구성 요소 및 펌웨어 구성 요소에 대하여 ① 암호모듈 자체적으로 무결성 검증을 수행하거나 ② 다른 검증대상 암호모듈의 검증대상 동작모드에서 무결성 검증을 수행하는 무결성 검증 기법을 명세한 개발 문서를 제출해야 한다.

VE05.05.02
벤더는 암호모듈의 모든 소프트웨어 구성 요소 및 펌웨어 구성 요소에 대하여 ① 단일 인증 코드나 서명 또는 ② 복수 인증 코드나 서명을 사용하여 무결성 검증을 수행하는 무결성 검증 기법을 명세하는 개발 문서를 제출해야 한다.

VE05.05.03
벤더는 무결성 검증에 사용된 암호키의 저장 위치를 명세한 개발 문서를 제공해야 한다. 검증대상 전자서명이 무결성 검증 기법에 사용되었다면 벤더는 참조 서명을 생성하는 데 사용된 개인키의 저장 위치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.05.01
시험자는 암호모듈을 검사하여 검증대상 무결성 기술이 모듈 내의 모든 소프트웨어 구성 요소와 펌웨어 구성 요소에 적용되었는지 검증해야 한다.

AS05.06: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

무결성 시험이 실패하면 모듈은 오류 상태로 전환되어야 한다.

[벤더 요구사항]

VE05.06.01
벤더는 소프트웨어/펌웨어의 무결성 시험을 명세한 개발 문서를 제출해야 한다. 해당 메커니즘은 검증대상 암호알고리즘이어야 한다.

[시험 절차]

TE05.06.01

시험자는 무결성 시험이 실패하면 모듈이 오류 상태로 전환됨을 검증해야 한다.

TE05.06.02
시험자는 무결성 시험이 완료된 후 무결성 시험 과정에서 생성되는 중간값들이 모두 제로화되었는지를 검증해야 한다.

AS05.07: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

검증대상 무결성 기술은 단일 인증 코드/서명 또는 복수 인증 코드/서명으로 구성되며, 복수 인증 코드/서명의 경우 하나라도 실패하면 모듈이 오류 상태로 전환되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.05**와 **AS05.06**의 일부분으로 시험된다.

AS05.08: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

소프트웨어 또는 펌웨어 무결성 시험 중 임시로 생성된 값은 무결성 시험이 완료되면 모듈에 의해 제로화되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.06**의 일부분으로 시험된다.

AS05.09: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

운영자는 {KS X ISO/IEC 19790} **7.3.2**에 명세한 HMI 또는 SFMI, HSMI, HFMI 서비스를 통해서 들어온 요청에 따라 검증대상 무결성 기술을 수행할 수 있어야 한다.

[벤더 요구사항]

VE05.09.01
벤더는 HMI 또는 SFMI, HSMI, HFMI 서비스를 통해 들어온 요청에 따라 검증대상 무결성 기술을 수행하는 방법을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.09.01
시험자는 HMI, SFMI, HSMI 또는 HFMI를 통하여 무결성 시험이 수행될 수 있는지 검증해야 한다.

TE05.09.02
시험자는 무결성 시험이 수행되는 동안 (**7.3.2**에 명세된) 모든 데이터 입력, 제어 입력, 데이터 출력 및 상태 출력이 (**7.4.3**에 명세된) HMI 또는 SFMI, HFMI, HSMI 서비스를 통해 전달되는지 검증해야 한다.

AS05.10: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

암호모듈과 ({KS X ISO/IEC 19790} **7.4.3**에 명세된) 서비스의 ({KS X ISO/IEC 19790} **7.3.3**에 명세된) 모든 데이터 입력, 제어 입력, 데이터 출력, 제어 출력 및 상태 출력은 정의된 HMI 또는 SFMI, HFMI, HSMI를 통해 이뤄져야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.09**의 일부분으로 시험된다.

AS05.11: (소프트웨어/펌웨어 보안수준 1, 2, 3, 4)

로드된 소프트웨어 또는 펌웨어가 ① 검증대상 암호모듈과 연계되거나 결합되는 경우 또는 ② 검증대상 암호모듈을 변경하는 경우 ③ 검증대상 암호모듈을 실행시키는 핵심 부분인 경우에 해당하지만 검증대상 모듈을 완전히 대체하거나 오버레이가 아닌 경우, 로드된 소프트웨어 또는 펌웨어는 소프트웨어/펌웨어 로드 시험이 적용되어야 하고 이 시험은 검증대상 모듈에 의해 수행되어야 한다.

[벤더 요구사항]

VE05.11.01
벤더는 검증대상 암호모듈에 의해 수행되는 소프트웨어/펌웨어 로드 시험을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.11.01
시험자는 개발 문서와 벤더 구현물을 검증해야 한다.

AS05.12: (소프트웨어/펌웨어 보안수준 2, 3, 4)

다음과 같은 요구사항이 보안수준 2에 대한 암호모듈의 소프트웨어와 펌웨어 구성 요소에 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.13**～**AS05.16**의 일부분으로 시험된다.

AS05.13: (소프트웨어/펌웨어 보안수준 2, 3, 4)

암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소는 실행 형태[예: 소스 형태가 아닌 코드, 오브젝트 코드 또는 적시(just-in-time) 컴파일 코드]의 코드만 포함해야 한다.

[벤더 요구사항]

VE05.13.01
벤더는 실행 형태의 소프트웨어 및 펌웨어가 명세된 개발 문서를 제출해야 한다.

[시험 절차]

TE05.13.01
시험자는 개발 문서를 통하여 동적으로 코드가 변경되지 않는 것을 확인하기 위해 소프트웨어 명세와 벤더 구현물을 검증해야 한다.

AS05.14: (소프트웨어/펌웨어 보안수준 2, 3, 4)

HMI, SFMI, HFMI 또는 HSMI 인터페이스를 통한 서비스 중에서 운영자가 실행 코드를 검사할 수 있어서는 안 된다.

[벤더 요구사항]

VE05.14.01
벤더는 HMI, SFMI, HFMI 또는 HSMI 서비스를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.14.01
시험자는 벤더가 기술한 서비스를 명세한 개발 문서를 검증해야 한다.

TE05.14.02
시험자는 운영자가 실행 코드를 조사하지 못하도록 하는 서비스에 대한 개발 문서를 검증해야 한다.

VE05.14.03
시험자는 운영자가 실행 코드를 조사하지 못하는지 검증하기 위하여 해당 서비스들을 시험해야 한다.

AS05.15: (소프트웨어/펌웨어 보안수준 2, 3, 4)

검증대상 전자서명 또는 키 메시지 인증 코드는 모듈의 정의된 암호 경계 내 모든 소프트웨어와 펌웨어에 적용할 수 있어야 한다.

[벤더 요구사항]

VE05.15.01
벤더는 암호 소프트웨어 구성 요소와 펌웨어 구성 요소의 무결성을 유지하는 데 사용되는 기술을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.15.01
시험자는 개발 문서에 VE05.15.01에 명세된 정보가 포함되어 있는지 검증해야 한다. 만약 정보가 포함되어 있지 않다면 해당 시험 항목은 실패한 것으로 판정된다.

TE05.15.02
시험자는 암호 소프트웨어 구성 요소와 펌웨어 구성 요소를 손상시켜 무결성이 유지되는지 확인한다. 무결성이 유지되면 해당 시험 항목은 실패한 것으로 판정된다.

AS05.16: (소프트웨어/펌웨어 보안수준 2, 3, 4)

계산된 결과와 성공적으로 검증되지 않는다면 무결성 시험은 실패이며 모듈은 오류 상태로 전환되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.15**의 일부분으로 시험된다.

AS05.17: (소프트웨어/펌웨어 보안수준 3, 4)

다음 요구요항은 보안수준 3과 4에 대한 암호모듈의 소프트웨어 구성 요소 및 펌웨어 구성 요소에 적용된다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS05.18: (소프트웨어/펌웨어 보안수준 3, 4)

검증대상 전자서명을 사용하는 암호 메커니즘은 암호모듈에 대하여 정의된 암호 경계 내의 모든 소프트웨어 구성 요소 및 펌웨어 구성 요소에 적용되어야 한다.

[벤더 요구사항]

VE05.18.01
벤더는 검증대상 전자서명 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE05.18.01
시험자는 암호모듈을 검사하여 검증대상 전자서명을 사용하는 암호메커니즘은 암호 경계 내의 모든 소프트웨어 구성 요소 및 펌웨어 구성 요소에 적용되는지 검증해야 한다.

AS05.19: (소프트웨어/펌웨어 보안수준 3, 4)

계산된 결과와 성공적으로 검증되지 않는다면 무결성 시험은 실패이며 모듈은 오류 상태로 전환되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.15**의 일부분으로 시험된다.

AS05.20: (소프트웨어/펌웨어 보안수준 3, 4)

전자서명 기술은 단일 서명 또는 복수 서명으로 구성되며, 복수 서명 중 어느 하나라도 실패할 경우 모듈이 오류 상태로 전환되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS05.15**의 일부분으로 시험된다.

AS05.21: (소프트웨어/펌웨어 보안수준 3, 4)

개인 서명키는 모듈의 외부에 존재해야 한다.

[벤더 요구사항]

VE05.21.01
벤더가 제출해야 할 개발 문서는 VE05.05.03에 명세되어 있다. 벤더는 서명을 생성하기 위한 개인 서명키가 암호모듈 경계 내에 존재하지 않음을 보장하는 개발 문서를 제출해야 한다.

[시험 절차]

TE05.21.01
시험자는 개발 문서를 검토하고 암호모듈을 검사하여 개인 서명키가 암호 경계 안에 존재하지 않음을 검증해야 한다.

6.6 운영환경

6.6.1 운영환경 일반 요구사항

AS06.01: (운영환경 – 보안수준 1, 2)

변경 불가능한 운영환경 또는 제한적인 운영환경인 경우, {KS X ISO/IEC 19790} **7.6.2**의 운영체제 요구사항을 적용해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.04**의 일부분으로 시험된다.

AS06.02: (운영환경 – 보안수준 1, 2)

변경 가능한 운영환경인 경우, {KS X ISO/IEC 19790} **7.6.3**의 운영체제 요구사항을 적용해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.05**～**AS06.29**의 일부분으로 적용 가능한 것이 시험된다.

AS06.03: (운영환경 – 보안수준 1, 2)

{KS X ISO/IEC 19790 **부속서**} **A.2.6**에 명시된 요구사항을 만족하는 개발 문서를 제공해야 한다.

[벤더 요구사항]

VE06.03.01
벤더는 KS X ISO/IEC 19790의 **A.2.6**에 명시된 문서 요구사항을 제공해야 한다.

[시험 절차]

TE06.03.01
시험자는 벤더가 KS X ISO/IEC 19790의 **A.2.6**에 명시된 문서 요구사항을 제공하는지 확인해야 한다.

6.6.2 제한적인 운영환경 또는 변경 불가능한 운영환경의 요구사항

AS06.04: (운영환경 – 보안수준 1)

암호모듈이 {KS X ISO/IEC 19790} **7.7**의 보안수준 1인 경우, {KS X ISO/IEC 19790} **7.6.3**의 보안수준 1 요구사항이 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.05**～**AS06.08**의 일부분으로 시험된다.

6.6.3 변경 가능한 운영환경의 요구사항

AS06.05: (운영환경 – 보안수준 1, 2)

암호모듈의 각 인스턴스는 암호모듈 스스로의 SSP를 제어해야 한다.

비고 1 암호모듈의 각 인스턴스는 스스로 SSP를 제어하고 외부 프로세스나 운영자에 의해 제어되지 않는다.
비고 2 이 요구사항은 관리자 설명서 및 절차에 의해 시행될 수 없으며 암호모듈 자체에 의해 수행되어야 한다.

[벤더 요구사항]

VE06.05.01
벤더는 암호 프로세스가 작동하는 동안 암호모듈의 각 인스턴스가 스스로의 SSP를 제어하는 데 사용되는 운영체제 메커니즘을 기술해야 한다.

[시험 절차]

TE06.05.01
시험자는 암호모듈이 사용되는 동안 암호모듈의 각 인스턴스가 스스로 SSP를 제어한다는 것을 개발 문서와 운영체제의 점검에 의해 확인해야 한다.

TE06.05.02
시험자는 요구사항이 암호모듈 스스로에 의해 수행되고 있다는 것을 개발 문서와 운영체제의 점검에 의해 확인해야 한다.

TE06.05.03
암호 관리자 및 사용자 설명서에 서술된 대로 시험자는 암호 함수를 수행해야 한다. 암호 함수가 실행되는 동안, 동일한 시험자 또는 다른 시험자가 비밀키와 개인키, 중간키 생성값 및 암호모듈이 제어하는 기타 SSP에 대하여 인가되지 않은 접근을 시도해야 한다.

AS06.06: (운영환경 – 보안수준 1, 2)

운영환경은 응용 프로그램의 데이터가 운영환경 내의 프로세스 메모리에 있든지 영구 저장소에 저장되든지 상관없이, 인가되지 않은 CSP에 대한 접근과 제어되지 않는 보안매개변수의 변경을 방지하여 각각의 응용 프로세스가 독립적으로 작동할 수 있도록 하는 기능을 제공해야 한다.

[벤더 요구사항]

VE06.06.01
벤더는 응용 프로그램의 데이터가 운영환경 내의 프로세스 메모리에 있든지 영구 저장소에 저장되든지 상관없이, 인가되지 않은 CSP에 대한 접근과 제어되지 않는 보안매개변수의 변경을 방지하여 각각의 응용 프로세스가 독립적으로 작동할 수 있도록 하는 기능을 제공하기 위해 사용되는 운영환경 메커니즘을 기술해야 한다.

[시험 절차]

TE06.06.01
시험자는 응용 프로그램의 데이터가 운영환경 내의 프로세스 메모리에 있든지 영구 저장소에 저장되든지 상관없이, 인가되지 않은 CSP에 대한 접근과 제어되지 않는 보안매개변수의 변경을 방지하여 각각의 응용 프로세스가 독립적으로 작동할 수 있도록 하는 기능을 제공하기 위해 개발 문서와 사용되는 운영환경 메커니즘 점검에 의해 확인해야 한다.

TE06.06.02
시험자는 암호 관리자나 사용자 안내 문서에 서술된 암호화 기능을 수행해야 한다. 암호화 기능이 수행되는 동안, 동일한 시험자 또는 다른 시험자가 운영환경 내의 프로세스 메모리에 있든지 영구 저장소에 저장되든지 상관없이, 인가되지 않은 CSP에 대한 접근과 제어되지 않는 보안매개변수의 변경을 시도해야 한다.

AS06.07: (운영환경 – 보안수준 1, 2)

운영환경 설정에 대한 제한 사항은 암호모듈의 보안정책 문서에 서술되어야 한다.

[벤더 요구사항]

VE06.07.01: 벤더는 운영환경에 대한 모든 규제를 서술해야 한다.

[시험 절차]

TE06.07.01
시험자는 개발 문서에서 운영환경에 대한 모든 규제를 확인해야 한다.

TE06.07.02
시험자는 운영환경에 대한 모든 규제가 보안정책에 문서화되어 있는지 확인해야 한다.

AS06.08: (운영환경 – 보안수준 1, 2)

암호모듈에 인해 생성된 프로세스는 해당 암호모듈에 의해서만 소유되어야 하며 외부 프로세스나 운영자에 의해 소유될 수 없다.

비고 이 요구사항은 관리자 설명서 및 절차에 의해 시행될 수 없으며, 암호모듈 자체에 의해 수행되어야 한다.

[벤더 요구사항]

VE06.08.01
벤더는 암호모듈에 의해 발생한 프로세스들이 모듈에 의해서만 사용되고 외부 프로세스나 운영자에 의해서는 사용되지 않는다는 점을 확인할 수 있는 운영체제 메커니즘에 대한 문서를 제공해야 한다.

[시험 절차]

TE06.08.01
시험자는 개발 문서와 운영체제 검사로부터 암호모듈에 의해 생성된 프로세스들이 암호모듈에 포함되고 외부 프로세스/운영자에 의해 소유되지 않음을 확인해야 한다.

TE06.08.02
시험자는 개발 문서와 운영체제를 검사하여 위 조건이 암호모듈 자체적으로 실행될 수 있음을 확인해야 한다.

TE06.08.03
시험자는 암호 책임자와 사용자 지침서에 기술된 대로 암호 기능을 실행해야 한다. 암호 기능이 실행되는 동안, 동일 시험자 또는 다른 시험자는 외부 프로세스나 운영자가 암호모듈에 의해 생성된 프로세스의 소유권 얻을 수 있는지 확인해야 한다.

AS06.09: (운영환경 – 보안수준 2)

보안수준 2에서 운영환경은 다음과 같은 요구사항이나 관련 검증기관이 인정하는 조건들을 충족해야 한다.

비고 1 운영환경 요구사항이 검증기관에 의해 명시되지 않을 경우 **AS06.10**～**AS06.29**와 같이 시험된다.
비고 2 운영환경 요구사항이 검증기관에 의해 명시될 경우 다음과 같이 시험된다.

[벤더 요구사항]

VE06.09.01
벤더는 운영환경에 대해 기술한 문서를 제공해야 한다.

VE06.09.02
벤더는 운영환경과 검증기관이 허용한 운영환경을 비교하는 문서를 제공해야 한다.

[시험 절차]

TE06.09.01
시험자는 개발 문서에 운영체제에 대한 기술이 있는지 확인해야 한다.

TE06.09.02
시험자는 운영체제가 벤더로부터 제공받은 설명서와 일치하는지 조사를 통해 확인해야 한다.

TE06.09.03
시험자는 운영체제와 벤더가 제공한 운영체제 설명서를 조사하여 운영체제가 검증기관의 허가를 받았는지 확인해야 한다.

AS06.10: (운영환경 – 보안수준 2)

모든 암호 소프트웨어, SSP, 제어 정보 및 상태 정보는 역할 기반 접근 통제나 최소한 임의 접근 제어(DAC)를 제공하는 운영체제의 통제를 따라야 한다. 여기서 임의적 접근 통제란, 예를 들면 새 그룹을 정의하고 대응되는 제한적 권한을 접근 통제 목록(ACL)을 통해 할당하는 메커니즘을 갖고, 각 사용자를 하나 이상의 그룹에 배정하는 것이다.

[벤더 요구사항]

VE06.10.01
벤더는 역할 기반 접근 제어 또는 새 그룹을 정의하고 접근 제어 리스트를 통해 제한적인 승인을 부여하고 각각의 사용자를 하나 이상의 그룹에 배정할 수 있는 임의 접근 제어를 구현한 운영체제 제어 메커니즘에 대해 설명하는 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.10.01
시험자는 벤더가 제공하는 문서를 확인하고 운영체제 제어 메커니즘 검사를 통해 이 운영체제가 역할 기반 접근 제어 또는 새 그룹을 정의하고 접근 제어 리스트를 통해 제한적인 승인을 부여하고 각각의 사용자를 하나 이상의 그룹에 배정하는 임의 접근 제어를 할 수 있음을 확인해야 한다.

TE06.10.02
시험자는 특정 사용자나 그룹에 허가를 주기 위해 운영체제의 역할 기반 접근 제어 또는 임의 접근 제어를 설정할 수 있다. 시험자는 허가된 사용자나 그룹의 역할을 맡아 SSP, 제어 또는 접근이 허용된 상태 데이터를 실행, 변경, 읽기 위해 시도해야 한다.

TE06.10.03
시험자는 특정 사용자나 그룹에 허가를 주기 위해 운영체제의 역할 기반 접근 제어나 임의 접근 제어를 설정할 수 있다. 시험자는 다른 사용자나 그룹의 역할을 맡아 SSP와 제어, 접근이 허용되지 않은 상태 데이터를 실행, 변경 또는 읽기 위해 시도해야 한다.

AS06.11: (운영환경 – 보안수준 2)

운영체제는 인가되지 않은 ① 실행, ② 변경, ③ SSP, 제어 정보 및 상태 정보의 읽기를 방지하도록 설정되어야 한다.

[벤더 요구사항]

VE06.11.01
벤더는 인가되지 않은 실행, 변경이나 인가되지 않는 SSP, 제어 정보 및 상태 정보 읽기를 방지하는 운영체제 제어 메커니즘에 대해 설명하는 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.11.01
시험자는 개발 문서를 확인하고 운영체제 제어 메커니즘 검사를 통해 운영체제가 인가되지 않는 실행, 변경이나 인가되지 않은 SSP, 제어 정보 및 상태 정보 읽기 등을 방지하도록 설정될 수 있는지 확인해야 한다.

TE06.11.02
시험자는 운영체제가 인가되지 않은 실행, 변경이나 SSP, 제어 정보 및 상태 정보 읽기를 방지할 수 있도록 설정해야 한다. 암호 프로세스 실행 중에 시험자는 허용된 SSP, 제어 또는 상태 정보의 실행, 변경, 읽기를 시도해야 한다.

TE06.11.03
시험자는 인가되지 않은 실행, 변경이나 SSP, 제어 정보 및 상태 정보의 읽기를 방지하기 위해 운영체제를 설정해야 한다. 암호 실행 과정에서 시험자는 허용되지 않은 SSP, 제어나 접근이 허용되지 않는 상태 데이터 읽기를 시도해야 한다.

AS06.12: (운영환경 – 보안수준 2)

{평문 데이터, 운영체제의 암호 소프트웨어, SSP, 인증 데이터를 보호하기 위한 접근 통제 메커니즘은} 역할을 정의하고, 저장된 암호화 소프트웨어에 대한 독점적 실행 권한을 제한적으로 허용하는 것이 어떻게 정의된 역할과 관계되는지 정의하고 적용하도록 설정되어야 한다.

[벤더 요구사항]

VE06.12.01
벤더는 운영 체제의 접근 통제 메커니즘을 적용하고 구성하는 방법에 대해 기술한 문서를 제공해야 한다. 해당 문서는 역할을 어떻게 정의하고 분류하는지, 저장된 암호화 소프트웨어를 실행할 수 있는 배타적 권리에 대한 제한적 허용을 역할에 따라 어떻게 부여하는지에 대한 내용을 포함해야 한다.

[시험 절차]

TE06.12.01
시험자는 개발 문서를 확인하고 운영체제 제어 메커니즘 검사를 통해 역할이 어떻게 정의되고 분류되는지, 저장된 암호화 소프트웨어에 대한 독점적 실행 권한에 대한 제한적 허용이 어떻게 정의되고 부여되는지 확인해야 한다.

TE06.12.02
시험자는 역할이 어떻게 정의되고 분류되는지, 저장된 암호화 소프트웨어에 대한 독점적 실행 권한

에 대한 제한적 허용이 어떻게 정의되고 부여되는지 운영체제 제어 메커니즘을 설정해야 한다. 시험자는 운영체제가 저장된 암호 소프트웨어를 실행하기 위한 접근 권한을 가지고 있는지 확인해야 한다.

TE06.12.03
시험자는 운영체제 제어 메커니즘을 통해 역할 또는 그룹이 저장된 암호 소프트웨어를 실행하기 위한 권한을 가지지 않도록 설정하고 역할이나 그룹이 암호 소프트웨어를 실행할 권한을 가지지 않는다는 점을 확인해야 한다.

AS06.13: (운영환경 – 보안수준 2)

{평문 데이터, 운영체제의 암호 소프트웨어, SSP, 인증 데이터를 보호하기 위한 접근 제어 메커니즘은} 일련의 역할이나 그룹이 암호 경계 내에 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터(예: 암호 감사 데이터), SSP, 평문 데이터]를 변경할 수 있는 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다.

[벤더 요구사항]

VE06.13.01
벤더는 운영체제 제어 메커니즘이 일련의 역할이나 그룹에 암호 경계 내에 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터, 감사 데이터, SSP, 평문데이터]를 제한적으로 변경할 수 있는 권한(쓰기, 대체, 삭제)을 부여하는지에 대해 기술된 문서를 제공해야 한다.

[시험 절차]

TE06.13.01
시험자는 운영체제 제어 메커니즘이 일련의 역할이나 그룹에 암호 경계 내에 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터, 감사 데이터, SSP, 평문 데이터]를 제한적으로 변경할 수 있는 권한(쓰기, 대체, 삭제)을 부여하는지 개발 문서에 기술되어 있는지 검증해야 한다.

TE06.13.02
시험자는 운영체제 제어 메커니즘이 암호 경계 내 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터, 감사 데이터, SSP, 평문 데이터]에 대해 일련의 역할이나 그룹이 가지고 있는 권한을 정의하고 역할이나 그룹이 실행할 수 있도록 설정한다. 그리고 시험자는 이 역할이나 그룹에 암호 경계 내에 저장된 다음의 암호모듈 소프트웨어를 변경할 수 있는 권한(쓰기, 대체, 삭제)이 있는지 확인해야 한다.

TE06.13.03
시험자는 운영체제 제어 메커니즘이 암호 경계 내 저장된 암호모듈 소프트웨어[암호 프로그램, 암호 데이터, 감사 데이터, SSP, 평문 데이터]에 대해 일련의 역할이나 그룹이 가지고 있는 권한을 정의하고 역할이나 그룹이 실행할 수 없도록 설정한다. 그리고 시험자는 이 역할이나 그룹이 암호 경계 내에 저장된 다음의 암호모듈 소프트웨어를 변경할 수 있는 권한(쓰기, 대체, 삭제)이 없는지 확인해야 한다.

AS06.14: (운영환경 – 보안수준 2)

{평문 데이터, 암호 소프트웨어, SSP, 인증 데이터를 보호하기 위한 운영체제의 접근 제어 메커니즘은} 일련의 역할이나 그룹이 암호 데이터(예: 암호 감사 데이터), CSP, 평문 데이터를 읽으려고 접근하는 것에 대해 제한적으로 정의하고, 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다.

[벤더 요구사항]

VE06.14.01
벤더는 운영체제 제어 메커니즘이 암호 데이터, CSP, 평문 데이터를 읽을 수 있게 역할이나 그룹에 부여한 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있음을 설명하는 문서를 제공해야 한다.

[시험 절차]

TE06.14.01
시험자는 운영체제 제어 메커니즘이 암호 데이터, CSP, 평문 데이터를 읽을 수 있게 역할이나 그룹에 부여한 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있는지 개발 문서를 확인해야 한다.

TE06.14.02
시험자는 운영체제 제어 메커니즘이 암호 데이터, CSP, 평문 데이터를 읽을 수 있게 역할이나 그룹에 부여한 제한적 접근을 정의하고 실행할 수 있도록 설정한다. 그리고 역할이나 그룹이 이를 실행할 수 있는지 확인해야 한다.

TE06.14.03
시험자는 운영체제 접근 제어 메커니즘이 역할이나 그룹에 암호 데이터, CSP, 평문 데이터를 읽을 수 있는 권한을 주지 않도록 설정한다. 그리고 이러한 권한을 부여하지 않으면 역할이나 그룹이 이 메커니즘을 통해 암호 데이터, CSP, 평문 데이터를 읽을 수 없음을 확인해야 한다.

AS06.15: (운영환경 – 보안수준 2)

{평문 데이터, 암호화 소프트웨어, SSP, 인증 데이터를 보호하기 위해서, 운영체제의 제어 메커니즘은} 일련의 역할이나 그룹이 SSP를 입력할 수 있도록 하는 제한적 권한을 정의하고 역할이나 그룹이 이를 실행할 수 있도록 설정해야 한다.

[벤더 요구사항]

VE06.15.01
벤더는 운영체제 제어 메커니즘이 역할이나 그룹이 SSP를 입력할 수 있도록 하는 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있음을 설명하는 문서를 제공해야 한다.

[시험 절차]

TE06.15.01
시험자는 운영체제 제어 메커니즘이 역할이나 그룹이 SSP를 입력할 수 있도록 하는 제한적 접근을 정의하고 역할이나 그룹이 이를 실행할 수 있음이 개발 문서에 설명되었는지 확인해야 한다.

TE06.15.02
시험자는 운영체제 제어 메커니즘이 역할이나 그룹이 SSP를 입력할 수 있도록 하는 제한적 접근을 정의하고 실행할 수 있도록 설정한다. 그리고 역할이나 그룹이 이를 실행할 수 있는지 확인해야 한다.

TE06.15.03
시험자는 운영체제 접근 제어 메커니즘이 역할이나 그룹이 SSP를 입력할 수 있는 권한을 가지지 않도록 설정하고, 역할이나 그룹이 SSP에 입력할 수 없음을 확인해야 한다.

AS06.16: (운영환경 – 보안수준 2)

다음의 명세는 역할이나 지정된 그룹의 권한 및 보안정책에서 정의하는 서비스와 일치해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.17**～**AS06.20**의 일부분으로 시험된다.

AS06.17: (운영환경 – 보안수준 2)

유지보수 역할을 지원하지 않을 때 운영체제는 모든 운영자와 실행 중인 다른 프로세스들이 암호 프로세스(예: 암호 프로그램 이미지의 로드 및 실행)를 변경하는 것을 방지해야 한다.

[벤더 요구사항]

VE06.17.01
벤더는 운영체제가 유지보수 상태가 아닐 때 모든 운영자와 실행 중인 프로세스들이 실행 중인 암호 프로세스(예: 암호 프로그램 이미지의 로드 및 실행)를 변경하는 것을 방지함을 문서로 제공해야 한다.

VE06.17.02
유지보수 상태가 아닐 때 운영체제가 운영자와 실행 중인 프로세스들이 실행 중인 암호 프로세스를 변경하는 것을 방지하는 방법은 지정된 그룹의 권한과 보안정책에 정의한 서비스와 일치해야 한다.

[시험 절차]

TE06.17.01
시험자는 유지보수 상태가 아닐 때 운영체제 제어 메커니즘 검사를 통해 운영체제가 어떠한 방법으로 모든 운영자와 실행 중인 프로세스들이 실행 중인 암호 프로세스의 변경을 방지하는지 개발 문서를 확인해야 한다.

TE06.17.02
시험자는 보안정책에 정의된 역할이나 지정된 그룹의 권한이 유지보수 상태가 아닐 때 모든 운영자와 실행 중인 프로세스들이 실행 중인 암호 프로세스를 변경하는 것을 방지하기 위한 운영체제 설정과 어떻게 일치하는지 확인해야 한다.

TE06.17.03
시험자는 유지보수 상태가 아닐 때 모든 운영자와 실행 중인 프로세스들이 실행 중인 암호 프로세스를 변경하지 못하도록 운영체제 제어 시스템을 설정한다. 시험자는 운영자 역할을 맡아 실행 중인 암호 프로세스들이 변경되지 않음을 확인해야 한다. 또한 실행 중인 프로세스들이 실행 중인 암호 프로세스를 변경하지 못함을 확인해야 한다.

AS06.18: (운영환경 – 보안수준 2)

운영체제는 사용자 역할 또는 사용자 그룹의 프로세스가 다른 프로세스가 소유한 SSP나 시스템 SSP에 대한 읽기 또는 쓰기 권한을 획득하는 것을 방지해야 한다.

[벤더 요구사항]

VE06.18.01
벤더는 사용자 역할의 프로세스가 다른 사용자 역할이나 그룹의 프로세스가 소유한 SSP를 얻고 쓰는 것을 운영체제가 어떻게 방지하는지 문서로 제공해야 한다.

VE06.18.02
운영체제가 다른 사용자 역할이나 그룹의 프로세스가 가지는 SSP를 얻고 쓰는 것을 어떻게 방지하는지에 대한 명세는 보안정책에 정의된 역할 또는 지정 그룹의 권한과 서비스와 일치해야 한다.

[시험 절차]

TE06.18.01
시험자는 제어 메커니즘 검사를 통해 사용자 역할이나 사용자 그룹의 프로세스가 다른 프로세스가 소유한 SSP와 시스템 보안매개변수에 대해 읽기/쓰기 권한을 가지는 것을 운영체제가 방지하도록 설정되는지 개발 문서를 확인해야 한다.

TE06.18.02
시험자는 다른 사용자 역할이나 그룹의 프로세스가 소유한 SSP를 얻고 쓰는 것을 어떻게 운영체제가 방지하는지에 대한 명세가 보안정책에 정의된 역할 또는 지정 그룹의 권한과 서비스와 일치하는지 확인해야 한다.

TE06.18.03
시험자는 사용자 역할이나 사용자 그룹이 다른 그룹이 소유한 SSP를 읽거나 쓰지 못하도록 운영체제를 설정하고, 사용자 역할이나 사용자 그룹이 다른 그룹이 소유한 SSP를 읽거나 쓰지 못함을 확인해야 한다.

AS06.19: (운영환경 – 보안수준 2)

위의 요구사항 {**AS06.16**～**AS06.18**}을 충족시키는 운영체제의 설정은 관리자 지침에 구체적으로 명세해야 한다.

[벤더 요구사항]

VE06.19.01
벤더는 운영체제가 **AS06.16**～**AS06.18**의 요구사항을 충족시키도록 설정된 방법을 기술한 관리자 지침을 제공해야 한다.

[시험 절차]

TE06.19.01
시험자는 운영체제가 **AS06.16**～**AS06.18**의 요구사항을 충족시키도록 설정된 방법을 벤더가 관리자 지침에서 제공함을 확인해야 한다.

AS06.20: (운영환경 – 보안수준 2)

관리자 지침은 콘텐츠를 보호하기 위하여 {**AS06.16**～**AS06.18**에} 명세된 것처럼 운영체제 구성에 대하여 기술해야 한다.

[벤더 요구사항]

VE06.20.01
벤더는 보호 대상이라 생각되는 암호 콘텐츠를 위해 **AS06.16**～**AS06.18**에 명세된 것처럼 운영체제가 구성됨을 알리는 관리자 안내 문서를 제공해야 한다.

[시험 절차]

TE06.20.01
시험자는 벤더가 보호 대상이라 생각되는 암호 콘텐츠를 위해 **AS06.16**～**AS06.18**에 명세된 것처럼 운영체제가 구성됨을 알리는 관리자 안내 문서를 제공함을 확인해야 한다.

AS06.21: (운영환경 – 보안수준 2)

운영체제를 위한 식별과 인증 메커니즘은 {KS X ISO/IEC 19790} **7.4.3**의 요구사항에 부합되고 모듈 보안정책에 명세되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.24**～**AS06.28**의 일부분으로 시험된다.

AS06.22: (운영환경 – 보안수준 2)

모든 암호 소프트웨어, SSP, 제어와 상태 정보는 {최소한 다음의 속성을 가지는 운영체제}의 제어를 받아야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.24**～**AS06.28**의 일부분으로 시험된다.

AS06.23: (운영환경 – 보안수준 2)

모든 암호 소프트웨어, SSP, 제어 및 상태 정보는 {최소한 다음의 속성을 가지는 운영체제}의 제어를 받아야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.24**～**AS06.28**의 일부분으로 시험된다.

AS06.24: (운영환경 – 보안수준 2)

운영체제는 각각의 감사 이벤트의 감사 메커니즘을 시간과 같이 제공해야 한다.

비고 이 항목에서는 암호모듈이 식별된 이벤트를 감사하기 위해 운영체제가 제공하는 감사 메커니즘을 사용한다는 것을 가정한다. 아무리 잘 보호되더라도 암호모듈 소프트웨어가 감사 로그로 운영체제가 제공하지 않은 다른 파일을 사용하는 것은 바람직하지 않다.

[벤더 요구사항]

VE06.24.01
벤더는 운영체제에 의해 제공되는 감사 메커니즘과 각 사건이 어떻게 시간을 기록하는지 기술한 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.24.01
시험자는 운영체제를 검사하여 감사 메커니즘이 제공되는지 각 사건에 시간이 표시되어 있는지 개발 문서를 통해 확인해야 한다.

AS06.25: (운영환경 – 보안수준 2)

암호모듈은 감사 기록의 일환으로 SSP를 포함하지 않아야 한다.

[벤더 요구사항]

VE06.25.01
벤더는 운영체제의 감사 메커니즘에 대한 기록을 제공하는 암호모듈 서비스에 대해 기술한 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.25.01
시험자는 운영체제의 감사 메커니즘에 의한 감사 기록을 제공하는 암호모듈 서비스를 검사하여 SSP가 감사 기록 내에 없는지 개발 문서를 확인해야 한다.

TE06.25.02
시험자는 감사 기록을 제공하고 SSP가 제공되지 않는다는 것을 확인하기 위해 운영체제 감사 로그를 시험하는 모듈 서비스를 실행해야 한다.

AS06.26: (운영환경 – 보안수준 2)

암호모듈은 다음의 이벤트들을 운영체제의 감사 메커니즘에 의해 기록해야 한다.

- 암호 데이터와 SSP의 변경, 접근, 삭제, 추가
- 암호 관리자 기능을 위해 유효하지 않은 입력을 제공하려는 시도
- 암호 관리자 역할에 의한 운영자의 추가 또는 삭제(이 역할이 암호모듈에 의해 관리된다면)
- 보안 관련 암호 관리자 기능의 사용
- 암호모듈과 관련된 인증 데이터에 접근하기 위한 요청
- 암호모듈과 관련된 인증 메커니즘(예: 로그인)의 사용
- 암호 관리자 권한에 대한 요청

[벤더 요구사항]

VE06.26.01
벤더는 운영체제의 감사 메커니즘에 의해 제공되고 기록되는 암호모듈 이벤트를 기술한 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.26.01
시험자는 운영체제의 감사 메커니즘에 감사 기록을 제공하는 암호모듈 서비스 조사를 통해 **AS06.26**에 명세된 대로 {암호 데이터와 SSP에 대한 변경·접근·삭제·추가, 암호 관리자 기능에 대한 유효하지 않은 입력의 시도, (역할들이 암호모듈에 의해 관리될 때) 암호 관리자 역할에서 임의의 사용자를 추가하거나 제거하는 행위, 보안과 관련된 암호 관리자 기능의 사용, 암호모듈과 관련된 사용자 인증 데이터에 접근하기 위한 요청 암호모듈과 관련된 사용자 인증 메커니즘(예: 로그인)의 사용, 암호 관리자 권한에 대한 요청}과 같은 이벤트의 목록이 이벤트 기록을 위해 암호모듈에서 제공되는지 개발 문서를 확인해야 한다.

TE06.26.02
시험자는 **AS06.26**에 명세된 {암호 데이터와 SSP에 대한 변경·접근·삭제·추가, 암호 관리자 기능에 대한 유효하지 않은 입력의 시도, (역할들이 암호모듈에 의해 관리될 때) 암호 관리자 역할에서 임의의 사용자를 추가하거나 제거하는 행위, 보안과 관련된 암호 관리자 기능의 사용, 암호모듈과 관련된

사용자 인증 데이터에 접근하기 위한 요청, 암호모듈과 관련된 사용자 인증 메커니즘(예: 로그인)의 사용, 암호 관리자 권한에 대한 요청}과 같은 사건들이 기록되는지 확인하기 위해 감사 사건 기록을 제공하는 암호모듈 서비스를 실행하고 운영체제 감사 로그를 확인해야 한다.

비고 운영체제에 의해 제공되고 벤더에 의해 식별되는 감사 메커니즘의 경우 시험자가시험할 필요는 없다.

AS06.27: (운영환경 – 보안수준 2)

운영체제의 감사 메커니즘은 다음의 운영체제 관련 이벤트를 감사할 수 있어야 한다.

- 감사 흔적을 저장하는 감사 데이터에 대한 모든 운영자 읽기 또는 쓰기 접근
- 암호 데이터 또는 SSP를 저장하기 위해 암호모듈을 사용하는 파일에 대한 접근
- 암호 관리자 역할에 의한 운영자의 추가 또는 삭제(이 역할이 운영환경에 의해 관리된다면)
- 인증 데이터 관리 메커니즘 사용을 위한 요청
- 현 보안수준에서 신뢰 채널이 제공될 때, 신뢰 채널 기능을 사용하기 위한 요청과 요청의 수락 여부
- 현 보안수준에서 신뢰 채널이 제공될 때, 개시자의 신원과 신뢰 채널의 대상

[벤더 요구사항]

VE06.27.01
벤더는 운영체제의 감사 메커니즘에 의해 제공되고 기록되는 운영체제 이벤트를 기술하는 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.27.01
시험자는 운영체제 문서를 검사하여, 운영체제가 운영체제의 감사 메커니즘을 위한 감사 사건 기록과 같이 **AS06.27**에 명세된 사건의 목록 {감사 흔적을 저장하는 감사 데이터에 대한 모든 운영자 읽기 또는 쓰기 접근, 암호 데이터 또는 SSP를 저장하기 위해 암호모듈을 사용하는 파일에 대한 접근, 암호 관리자 역할에 의한 운영자의 추가 또는 삭제(이 역할이 운영환경에 의해 관리된다면), 인증 데이터 관리 메커니즘 사용을 위한 요청, 현 보안수준에서 신뢰 채널이 제공될 때 신뢰 채널 기능을 사용하기 위한 요청과 요청의 보장 여부 그리고 현 보안수준에서 신뢰 채널이 제공될 때 신뢰된 채널을 수립하려는 측과 상대방 측의 신원}을 제공하는지 개발 문서를 확인해야 한다.

TE06.27.02
시험자는 개발 문서와 OS 문서를 조사하여 **AS06.27**에 명세된 대로 {감사 기록에 저장된 데이터에 대한 모든 운영자 읽기/쓰기, (역할들이 암호모듈에 의해 관리될 때) 암호 관리자 역할에서 임의의 사용자를 추가하거나 제거하는 행위, 인증 데이터 관리 메커니즘을 사용하기 위한 요청, 현재 보안수준에서 신뢰된 채널이 지원될 경우, 신뢰 채널이 보안수준을 제공할 때, 신뢰 채널 기능을 사용하기 위한 요청과 요청의 보장 여부, 현재 보안수준에서 신뢰된 채널이 지원될 경우, 신뢰된 채널을 수립하려는 측과 상대방 측의 신원}과 같은 사건들의 목록이 OS 감사 메커니즘에 이벤트 기록으로 제공되는지 확인해야 한다.

비고 운영체제에 의해 제공되고 벤더에 의해 식별되는 감사 메커니즘의 경우 시험자가시험할 필요는 없다.

AS06.28: (운영환경 – 보안수준 2)

운영체제는 보안정책에 인정되지 않은 운영자가 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터를 변경하지 못하게 설정되어야 한다.

[벤더 요구사항]

VE06.28.01
벤더는 운영체제가 보안정책에 인정된 권한을 가지는 운영자 외의 다른 운영자가 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터의 변경을 어떻게 방지하는지 명세한 운영체제 문서를 제공해야 한다.

[시험 절차]

TE06.28.01
시험자는 운영체제 설정 검사를 통해 운영체제가 보안정책에 인정된 권한을 가지는 운영자 외의 다른 운영자가 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터의 변경을 어떻게 방지하는지에 대해 개발 문서를 확인해야 한다.

TE06.28.02
시험자는 운영체제가 보안정책에 인정된 권한을 가지는 운영자 외의 다른 운영자가 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터의 변경을 방지하도록 운영체제를 설정해야 한다.

TE06.28.03
시험자는 보안정책에서 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터의 변경을 허용하는 승인된 권한을 가지고 변경이 되는지 확인해야 한다.

TE06.28.04
시험자는 보안정책에서 암호모듈의 운영환경 내에 저장된 암호모듈 소프트웨어와 감사 데이터의 변경을 허용하지 않는 권한을 가정하고 변경이 되지 않는지 확인해야 한다.

AS06.29: (운영환경 – 보안수준 2)

암호모듈이 검증대상 운영 모드로 작동하는지와 관계없이, 보안 요구사항 **{AS06.05 ~ AS06.28}**을 충족하도록 설정된 운영체제만 이 보안수준에 사용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS06.05 ~ AS06.28**의 일부분으로 시험된다.

6.7 물리적 보안

6.7.1 물리적 보안 형체

AS07.01: (물리적 보안 – 보안수준 1, 2, 3 및 4)

암호모듈은 모듈 내용물에 대한 비인가된 물리적 접근을 제한하고, 설치 시 모듈의 비인가된 사용이나 변경(모듈 전체 내용물 교체 포함)을 방지하기 위하여 물리적 보안 메커니즘을 사용해야 한다.

[벤더 요구사항]

VE07.01.01
벤더는 모듈에 적용된 물리적 보안 메커니즘을 명시한 개발 문서를 제출해야 한다. 모든 하드웨어,

펌웨어, 소프트웨어 및 데이터(평문 CSP 포함)를 포함한 모듈의 내용물이 보호되어야 한다.

[시험 절차]

TE07.01.01
시험자는 개발 문서에서 모듈에 적용된 물리적 보안 메커니즘을 확인하여야 한다.

TE07.01.02
시험자는 개발 문서에 명시된 물리적 보안 메커니즘이 구현되었음을 검증하여야 한다.

AS07.02: (물리적 보안 – 보안수준 1, 2, 3 및 4)

암호 경계 내의 모든 하드웨어 구성 요소, 소프트웨어 구성 요소, 펌웨어 구성 요소 및 데이터 구성 요소 및 SSP를 보호해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.03: (물리적 보안 – 보안수준 1, 2, 3 및 4)

해당 조항의 요구사항은 하드웨어 모듈, 펌웨어 모듈, 그리고 하이브리드 모듈의 하드웨어 구성 요소와 펌웨어 구성 요소에 적용되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.04: (물리적 보안 – 보안수준 1, 2, 3 및 4)

이 조항의 요구사항은 모듈의 정의된 물리적 경계에 적용할 수 있어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.05: (물리적 보안 – 보안수준 1, 2, 3 및 4)

암호모듈의 물리적 보안 메커니즘에 따라 다음에 대하여 물리적으로 접근하여 사용하거나 변경하고자 하는 인가되지 않은 시도가 높은 확률로 탐지되어야 한다.

- 시각적 흔적을 남기는 계속된 시도(즉, 변조-증거)
- 접근 시도 도중

{그리고 CSP를 보호하기 위해 암호모듈에 의해 적절하고 즉각적인 조치가 취해져야 한다.}

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.06: (물리적 보안 – 보안수준 1, 2, 3 및 4)

{**AS07.05**와 연계하여} 암호모듈은 CSP를 보호하기 위하여 적절하고 즉각적인 조치를 취해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.07: (물리적 보안 – 보안수준 1, 2, 3 및 4)

{KS X ISO/IEC 19790 **부속서**} **A.2.7**의 요구사항을 충족하는 개발 문서를 제출해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

6.7.2 물리적 보안 일반 요구사항

AS07.08: (물리적 보안－보안수준 1, 2, 3 및 4)

다음 요구사항은 모든 물리적 형체에 적용되어야 한다.

비고 **AS07.09**～**AS07.33**의 일부분으로 시험된다.

AS07.09: (물리적 보안－보안수준 1, 2, 3 및 4)

개발 문서는 암호모듈의 물리적 보안 메커니즘을 구현한 물리적 형체와 보안수준을 명세하여야 한다.

[벤더 요구사항]

VE07.09.01
벤더는 KS X ISO/IEC 19790의 **7.7.1**에서 정의된 바와 같이, 단일칩 암호모듈, 다중칩 내장형 암호모듈 또는 다중칩 독립형 암호모듈의 물리적 형체를 명세한 개발 문서를 제출해야 한다.

암호모듈의 물리적 형체는 물리적 형체에 대한 설계와 일관성이 있어야 한다. 개발 문서 역시 암호모듈이 만족하는 보안수준(1～4)과 일관성을 가지도록 서술되어야 한다.

[시험 절차]

TE07.09.01
시험자는 KS X ISO/IEC 19790의 **7.7.1**에 정의된 바와 같이 단일칩 모듈, 다중칩 내장형 모듈 또는 다중칩 독립형 모듈 중에서 벤더가 분류한 모듈이 적합한지 여부를 확인하여야 한다.

시험자는 물리적 형체가 아래에 제시된 세 가지 판정 기준 가운데 하나를 만족하고 있는지 독립된 판정을 수행해야 한다. 세 가지 물리적 형체에 대한 특성과 공통된 사례는 다음과 같이 요약된다.

a) **단일칩 암호모듈** 특성: 단일 집적회로(IC) 칩이 독립 장치로 사용되거나 또는 물리적으로 보호되지 않는 다른 모듈이나 봉함에 내장될 수 있다. 단일칩은 하나의 판에 플라스틱이나 세라믹과 같은 단일 형태의 외부 물질로 덮여 있고, 외부 입력·출력 커넥터가 연결된다. 예: 단일 IC칩, 단일 IC칩으로 구성된 스마트카드 또는 단일 IC칩으로 암호알고리즘을 구현한 기타 시스템
b) **다중칩 내장형 암호모듈** 특성: 둘 이상의 IC칩들이 상호 연결되고, 또한 물리적으로 보호되지 않은 다른 제품이나 봉함에 물리적으로 내장된다.
c) **다중칩 독립형 암호모듈** 특성: 둘 이상의 IC칩들이 상호 연결되고, 또한 전체적으로 물리적으로 보호된 봉함에 내장된다.

TE07.09.02
시험자는 개발 문서를 검토하여 모듈이 만족할 만한 보안수준을 명세하고 있는지 검증해야 한다. 시험자는 암호모듈이 실제로 보안수준을 만족하는지 독립적 판정 과정을 수행해야 한다.

AS07.10: (물리적 보안－보안수준 1, 2, 3 및 4)

물리적 보안 목적을 위해 중요 데이터를 짧은 시간 내에 제로화해야 한다. 탐지 후 제로화 과정에서 중요 데이터가 탈취되지 않도록 해야 한다.

[벤더 요구사항]

VE07.10.01
벤더는 암호모듈이 변조를 탐지한 후 제로화를 수행하는 시간을 명시한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.10.01
시험자는 암호모듈이 변조를 탐지한 후 제로화를 수행하는 시간이 개발 문서에 명시되어 있음을 확인하여야 한다.

TE07.10.02
시험자는 제로화 수행 메커니즘이 개발 문서에 명시된 것과 암호모듈에 동일하게 구현되어 있는지 확인하여야 한다.

AS07.11: (물리적 보안 – 보안수준 1, 2, 3 및 4)

{암호모듈이 모듈의 내용물에 물리적으로 접근이 필요한 유지보수 역할을 포함하거나 또는 그 모듈이 물리적 접근을 허용하도록 설계되어 있다면(예: 모듈 벤더나 기타 인가된 개인), 이때} 유지보수 접근 인터페이스가 정의되어야 한다.

[벤더 요구사항]

VE07.11.01
벤더는 모듈에 적용된 유지보수 접근 인터페이스를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.11.01
시험자는 유지보수 접근 인터페이스를 설명한 개발 문서를 확인하여야 한다.

TE07.11.02
시험자는 개발 문서와 구현물이 일관성을 갖는지 확인해야 한다.

AS07.12: (물리적 보안 – 보안수준 1, 2, 3 및 4)

{암호모듈이 모듈의 내용물에 물리적으로 접근이 필요한 유지보수 역할을 포함하거나 또는 그 모듈이 물리적 접근이 허용되도록 설계되어 있다면(예: 모듈 벤더나 기타 인가된 개인), 이때} 유지보수 접근 인터페이스는 제거 가능 덮개나 개구부까지도 포함해서 암호모듈 내용물에 대한 모든 물리적 접근 경로를 포함해야 한다.

[벤더 요구사항]

VE07.12.01
벤더는 제거 가능 덮개나 개구부를 포함한 유지보수 접근 인터페이스를 개발 문서에 명시하여 제출해야 한다.

[시험 절차]

TE07.12.01
시험자는 제거 가능 덮개나 개구부를 포함하여 유지보수 접근 인터페이스를 제공하는 개발 문서를 확인하여야 한다.

AS07.13: (물리적 보안－보안수준 1, 2, 3 및 4)

{암호모듈이 모듈의 내용물에 물리적으로 접근이 필요한 유지보수 역할을 포함하거나 또는 그 모듈이 물리적 접근을 허용하도록 설계되어 있다면(예: 모듈 벤더나 기타 인가된 개인), 이때} 유지보수 접근 인터페이스 내에 포함된 제거 가능 덮개나 개구부는 적절한 물리적 보안 메커니즘으로 보호되어야 한다.

[벤더 요구사항]

VE07.13.01
벤더는 유지보수 접근 인터페이스 내에 포함된 제거 가능 덮개나 개구부까지도 적절한 물리적 보안 메커니즘을 사용하여 보호되어야 한다는 등의 물리적 보호 기법을 명시한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.13.01
시험자는 유지보수 접근 인터페이스 내에 포함된 어떤 제거 가능 덮개나 개구부까지도 적절한 물리적 보안 메커니즘으로 보호되고 있음을 확인하여야 한다.

AS07.14: (물리적 보안－보안수준 1, 2, 3 및 4)

다음 요구사항은 보안수준 1에 대한 모든 암호모듈에 적용하여야 한다.

비고 AS07.15～AS07.16의 일부분으로 시험된다.

AS07.15: (물리적 보안－보안수준 1, 2, 3 및 4)

암호모듈은 표준 부식 방지 기술(예: 환경적 또는 기타 물리적 손상을 보호하기 위하여 모듈 회로에 적용된 절연 코팅 또는 봉인 코팅)을 포함한 생산 등급 구성 요소로 구성되어야 한다.

[벤더 요구사항]

VE07.15.01
모듈은 전력, 온도, 신뢰성 및 쇼크와 진동 등과 같은 상업용 등급 규격에 적합하게 설계되고, 표준화되고, 제품 품질을 갖춘 IC로 구성되어야 한다. 모듈은 칩 전체에 대하여 표준 부식 방지 기술이 적용되어야 한다. 벤더는 이러한 IC 품질을 명세한 개발 문서를 제출해야 한다. IC가 표준 부품이 아닌 규격을 사용하고 있다면 그 IC의 부식 방지 설계 기술이 반드시 명시되어 있어야 한다.

[시험 절차]

TE07.15.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여, 모듈이 균일 외부 물질이나 표준 커넥터와 연결할 수 있는 표준 집적 회로를 포함하는지 확인해야 한다. 시험자는 개발 문서를 검토하여 모듈에 사용된 칩들이 전력과 전압 범위, 온도, 신뢰성 및 쇼크와 진동에 관한 규격들이 상업용 등급에 적합

한지 확인해야 한다.

TE07.15.02
시험자는 개발 문서를 검토하여 모듈이 표준 부식 방지 기법이 적용되었는지 확인해야 한다. 부식 방지 기법은 환경적 또는 기타 물리적 손상을 방어하기 위하여 칩 회로에 적용된 봉인 코팅이어야 한다. 만일 표준 부식 방지 기법이 적용되지 않았다면 개발 문서는 그 기법이 표준 부식 방지 기법과 동등하다는 근거를 서술해야 한다.

AS07.16: (물리적 보안－보안수준 1, 2, 3 및 4)

물리적 유지보수를 수행할 때 운영자는 절차에 따라 제로화를 실행하거나 암호모듈이 자동으로 제로화를 실행해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS07.17: (물리적 보안－보안수준 2, 3 및 4)

비고 **AS07.18**～**AS07.20**의 일부분으로 시험된다.

AS07.18: (물리적 보안－보안수준 2, 3 및 4)

모듈에 물리적 접근을 시도할 때 암호모듈은 변조-증거(예: 덮개, 봉함 및 봉인)를 제공하여야 한다.

비고 해당 시험 항목은 단일칩 형체에 대해서는 **AS07.34**와 **AS07.35**의 일부분으로, 다중칩 내장형 형체에 대해서는 **AS07.44**와 **AS07.45**의 일부분으로, 다중칩 독립형 형체에 대해서는 **AS07.62**와 **AS07.63**의 일부분으로 시험된다.

AS07.19: (물리적 보안－보안수준 2, 3 및 4)

모듈의 핵심 영역에 대한 내부 동작 정보 수집을 방지하기 위하여 변조-증거 물질, 코팅 또는 봉함은 육안(가시광선 파장 범위 400 nm～750 nm의 빛)으로 볼 수 없게 불투명 또는 반투명이어야 한다.

[벤더 요구사항]

VE07.19.01
벤더는 가시광선 스펙트럼에서 불투명 또는 반투명한 변조-증거 물질, 코팅 또는 봉함을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.19.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 변조-증거 물질, 코팅 또는 봉함이 가시광선 범위에서 불투명하거나 반투명한지 확인해야 한다.

AS07.20: (물리적 보안－보안수준 2, 3 및 4)

만일 암호모듈에 환기구나 틈새가 있다면, 직접적인 육안 관찰을 통하여 모듈의 내부적 구조나 구성 요소 등의 정보를 수집하지 못하도록 모듈이 제작되어야 한다. 육안 관찰에는 모듈의 내부 구조나 구성 요소를 볼 수 있도록 인공 광원이 사용될 수 있다.

[벤더 요구사항]

VE07.20.01
만일 모듈이 환기구나 틈새가 있는 덮개나 봉함 안에 포함되어 있다면, 이 환기구나 틈새는 봉함 내부에 탐지되지 않는 물리적 탐침이 발생하지 않도록 구성되어야 한다. 벤더는 이들 환기성 물리적 기술을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.20.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈에 환기구나 틈새 또는 기타 개구부를 갖는 덮개나 봉함이 포함되는지 확인하고, 포함된다면 이들 환기구, 틈새 또는 기타 개구부를 통하여 덮개나 봉함 내부로 탐지되지 않는 탐침을 방지하도록 구성되었는지 확인해야 한다.

AS07.21: (물리적 보안－보안수준 3과 4)

다음 요구 조건들은 보안수준 3에 대한 모든 암호모듈에 적용되어야 한다.

비고 **AS07.22**～**AS07.28**의 일부분으로 시험된다.

AS07.22: (물리적 보안－보안수준 3과 4)

암호모듈에 개구부나 제거 가능 덮개가 포함되어 있거나 유지보수 접근 인터페이스가 정의되어 있다면 그 모듈은 변조 대응 및 제로화 기능을 포함해야 한다.

비고 해당 시험 항목은 일반 요구사항에 대해서는 **AS07.13**의 일부분으로, 단일칩 형체에 대해서는 **AS07.38**의 일부분으로, 다중칩 내장형 형체에 대해서는 **AS07.50**의 일부분으로, 다중칩 독립형 형체에 대해서는 **AS07.62**의 일부분으로 시험된다.

AS07.23: (물리적 보안－보안수준 3과 4)

개구부가 열리거나 덮개가 제거될 때 또는 유지보수 접근 인터페이스가 사용될 때, 암호모듈의 변조 대응 및 제로화 기능으로 모든 비보호된 SSP를 즉각 제로화시켜야 한다.

비고 해당 시험 항목은 일반 요구사항에 대해서는 **AS07.13**의 일부분으로, 단일칩 형체에 대해서는 **AS07.38**의 일부분으로, 다중칩 내장형 형체에 대해서는 **AS07.50**의 일부분으로, 다중칩 독립형 형체에 대해서는 **AS07.62**의 일부분으로 시험된다.

AS07.24: (물리적 보안－보안수준 3과 4)

보호되지 않은 SSP가 암호모듈 내부에 있을 때 변조 대응 및 제로화 기능이 작동 상태를 유지해야 한다.

비고 해당 시험 항목은 단일칩 형체에 대해서는 **AS07.38**의 일부분으로, 다중칩 내장형 형체에 대해서는 **AS07.50**의 일부분으로, 다중칩 독립형 형체에 대해서는 **AS07.62**의 일부분으로 시험된다.

AS07.25: (물리적 보안－보안수준 3과 4)

암호모듈에 환기구나 틈새가 있다면, 모듈은 봉함 내부로의 탐지되지 않는 탐침을 방지(예: 한 개의

연계 탐침기에 의한 탐침 방지)하는 방식으로 제작되어야 한다.

[벤더 요구사항]

VE07.25.01
만일 모듈이 환기구나 틈새가 있는 덮개나 봉함 안에 포함되어 있다면, 봉함 내부로의 탐지되지 않는 물리적 탐침을 방지하도록 환기구나 틈새가 구성되어야 한다. 벤더는 이들 환기성 물리적 기술을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.25.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈이 환기구, 틈새 또는 기타 개구부를 갖는 덮개나 봉함을 포함하는지 확인하고, 포함한다면 이들 환기구, 틈새 또는 기타 개구부를 통하여 덮개나 봉함 내부로 탐지되지 않는 탐침을 방지하도록 구성되었는지 확인해야 한다.

AS07.26: (물리적 보안－보안수준 3과 4)

강도 또는 경도가 높은 절연 또는 비절연의 봉함, 코팅 또는 매몰재는 모듈이 동작 중이거나 저장되거나 배포될 때의 온도 범위(설계 명세)에서 강도와 경도가 유지되어야 한다.

[벤더 요구사항]

VE07.26.01
벤더는 봉함의 강도를 명세하고, 이 강도가 암호모듈에 적절하다는 근거를 개발 문서에 명세하여 제출해야 한다.

[시험 절차]

TE07.26.01
시험자는 모듈을 검사하고 개발 문서를 검토하여 봉함이 개발 문서에 명세된 것과 같은지 확인하여야 한다.

AS07.27: (물리적 보안－보안수준 3과 4)

변조-증거 봉인이 있는 경우, 봉인은 고유 번호로 할당되거나 또는 독립적으로 식별 가능(예: 고유 번호가 있는 증거 테이프 또는 고유 식별 가능한 홀로그램 봉인)해야 한다.

[벤더 요구사항]

VE07.27.01
벤더는 변조-증거 봉인을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.27.01
시험자는 개발 문서에서 명세한 것과 같이 변조-증거 봉인이 고유 번호로 할당하였는지 또는 독립적으로 인식 가능한지 확인해야 한다.

AS07.28: (물리적 보안－보안수준 3과 4)

암호모듈은 EFP 특징을 포함하거나 EFT를 적용해야 한다.

비고 해당 시험 항목은 **AS07.68**의 일부분으로 시험된다.

AS07.29: (물리적 보안－보안수준 4)

다음 요구사항은 보안수준 4에 해당하는 모든 암호모듈에 적용되어야 한다.

비고 **AS07.30**～**AS07.33**의 일부분으로 시험된다.

AS07.30: (물리적 보안－보안수준 4)

암호모듈은 경도가 높은 불투명 제거-방지 코팅에 의해 보호되거나 변조 대응 및 제로화 기능을 갖는 변조 탐지 겉봉함에 의해 보호되어야 한다.

비고 해당 시험 항목은 단일칩 형체에 대해서는 **AS07.40**의 일부분으로, 다중칩 내장형 형체에 대해서는 **AS07.52**의 일부분으로, 다중칩 독립형 형체에 대해서는 **AS07.64**의 일부분으로 시험된다.

AS07.31: (물리적 보안－보안수준 4)

암호모듈은 EFP 특징을 포함하고 있어야 한다.

비고 해당 시험 항목은 **AS07.72**의 일부분으로 시험된다.

AS07.32: (물리적 보안－보안수준 4)

암호모듈은 오류 유도 공격에 대한 보호 기술을 제공하여야 한다.

[벤더 요구사항]

VE07.32.01
벤더는 오류 유도 공격에 대한 보호 메커니즘을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.32.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 오류 유도 공격에 대한 보호 메커니즘이 각각 명세된 바와 같이 동작하는지 확인해야 한다.

AS07.33: (물리적 보안－보안수준 4)

오류 유도 대응 기술과 대응 측정 지수들은 {KS X ISO/IEC 19790} **부속서** B에서 명시된 바와 같이 문서화되어야 한다.

[벤더 요구사항]

VE07.33.01
벤더는 모듈에 적용된 오류 유도 대응 기술과 대응 측정 지수를 명시한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.33.01
시험자는 모듈에 적용된 오류 유도 대응 기술과 대응 측정 지수가 개발 문서와 같은지 확인해야 한다.

6.7.3 물리적 보안 형체의 물리적 보안 요구사항

6.7.3.1 단일칩 암호모듈

비고 1 KS X ISO/IEC 19790의 **7.7.2**에서 명시된 일반 보안 요구사항과 이에 추가한 **AS07.34**~**AS07.42**의 요구사항은 단일칩 암호모듈에 적용된다.
비고 2 단일칩 암호모듈에 대한 보안수준 1 요구사항은 없다.

AS07.34: (단일칩 암호모듈 – 보안수준 2, 3 및 4)

다음 요구사항들은 보안수준 2의 단일칩 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS07.35**의 일부분으로 시험된다.

AS07.35: (단일칩 암호모듈 – 보안수준 2, 3 및 4)

암호모듈을 직접 관찰, 탐침 또는 조작 방지 목적과 모듈을 변조·제거하려는 시도에 대해 증거를 제공하기 위하여, 변조-증거 코팅(예: 변조-증거 부식 방지물 또는 부식 방지층 위에 도포한 변조-증거 물질) 또는 변조-증거 봉함이 암호모듈에 처리되어 있어야 한다.

비고 해당 요구사항은 **AS07.18**과 연관이 있다.

[벤더 요구사항]

VE07.35.01
벤더는 변조-증거 코팅과 그 특성을 식별할 수 있는 개발 문서를 제출해야 한다.

[시험 절차]

TE07.35.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈이 변조-증거 코팅으로 처리되었는지 확인해야 한다. 모듈 검사에 의해 변조-증거 코팅이 모듈을 완전하게 덮고 있는지 여부와 단일칩의 직접 관찰, 탐침, 조작이 방지하는지 여부를 확인해야 한다.

AS07.36: (단일칩 암호모듈 – 보안수준 3과 4)

다음 요구사항들은 보안수준 3의 단일칩 암호모듈에 적용되어야 한다.

비고 해당 요구사항은 **AS07.37**이나 **AS07.38**에서 시험된다.

[벤더 요구사항]

VE07.36.01
벤더는 **AS07.37**과 **AS07.38**에서 명세한 두 가지 방법이 해당 요구사항에 부합됨을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.36.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 **AS07.37**과 **AS07.38**에서 명세한 두 가지 방법이 해당 요구사항에 부합되는지 확인해야 한다.

TE07.36.02
암호모듈에 **AS07.37**에 명세된 방법이 존재한다면, 시험자는 TE07.38이 아닌 TE07.37의 시험 절차를 준수해야 한다. 모듈에 **AS07.38**에 명세된 방법이 존재한다면 시험자는 TE07.37이 아닌 TE07.38의 시험 절차를 준수해야 한다.

AS07.37: (단일칩 암호모듈 – 보안수준 3과 4)

{① 또는 ② 선택} ① 생산자가 규정한 온도 범위에서 경도가 높은 불투명 변조-증거 코팅(예: 부식 방지층을 덮고 있는 경도가 높은 불투명 에폭시)이 암호모듈에 처리되거나 {또는 ② **AS07.38**을 충족해야 한다.}

[벤더 요구사항]

VE07.37.01
벤더는 **AS07.37**에 명시된 방법이 해당 요구사항에 부합하도록 사용되는지 명세한 개발 문서를 제출해야 한다.

VE07.37.02
벤더는 적용된 코팅 유형 및 그 특성 등과 같은 상세 설계 정보를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.37.01
시험자는 모듈을 검사하고 개발 문서를 검토하여 암호모듈이 경도가 높은 불투명 변조-증거 코팅으로 처리되었는지 확인해야 한다.

TE07.37.02
시험자는 개발 문서가 적용된 코팅 유형 및 그 특성 등과 같은 상세 설계 정보를 명세하고 있는지 확인해야 한다.

TE07.37.03
시험자는 코팅 아래 회로가 있는 부분까지 코팅을 관통해 쉽게 침투할 수 없고 코팅이 변조-증거를 남기는 것을 확인해야 한다. 암호모듈을 검사하여 암호모듈이 코팅에 완전히 덮고 있고 시각적으로 불투명하며 직접 관찰, 탐침 또는 조작이 방지되어 있음을 확인해야 한다.

AS07.38: (단일칩 암호모듈 – 보안수준 3과 4)

{**AS07.37**이 충족되지 않을 때} {봉함을 제거하려는 시도 시 또는 침투하려는 시도 시, 암호모듈에 높은 확률로 심각한 손상(즉, 모듈 기능의 정지)을 주도록} 봉함이 구현되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS07.39**에서 시험된다.

AS07.39: (단일칩 암호모듈 – 보안수준 3과 4)

{**AS07.37**이 충족되지 않을 때} 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시, 암호모듈에 높은 확률로 심각한 손상(즉, 모듈 기능의 정지)을 주도록 {봉함이 구현되어야} 한다.

[벤더 요구사항]

VE07.39.01
벤더는 봉함이 개구부나 제거 가능 덮개를 포함하고 있는지 여부와 유지보수 접근 인터페이스가 명세되어 있는지 여부를 나타내는 세부 설계 정보를 명시한 개발 문서를 제출해야 한다. 봉함을 제거하려는 시도가 있을 때 봉함은 그 모듈 내부의 회로에 심각한 손상을 줄 확률이 높도록 설계되어야 한다.

VE07.39.02
봉함이 개구부나 제거 가능 덮개를 포함하거나 또는 유지보수 접근 인터페이스가 명세되어 있다면, 모듈은 변조 대응 및 제로화 회로를 포함해야 하며 벤더는 이를 명세한 개발 문서를 제출해야 한다. 이 회로는 덮개와 개구부를 지속적으로 감시해야 하고, 또한 덮개를 제거하거나 개구부를 개방한다면 모든 평문 CSP를 제로화해야 한다. 이 회로는 평문 CSP가 모듈 내부에 포함되어 있을 때 작동해야 한다.

[시험 절차]

TE07.39.01
시험자는 개발 문서를 통하여 봉함이 쉽게 제거될 수 없다는 사실을 확인해야 하고, 개구부나 제거 가능 덮개나 유지보수 접근 인터페이스의 포함 유무가 개발 문서에 명시되어 있는지 확인해야 한다. 봉함이 개구부 또는 제거 가능 덮개를 포함하거나 유지보수 접근 인터페이스를 가지고 있다는 점이 개발 문서에 명세되어 있다면, 시험자는 모듈이 변조 대응 및 제로화 회로를 포함하고 있음을 개발 문서에 명시하였는지 확인해야 한다.

TE07.39.02
봉함이 개구부 또는 제거 가능 덮개를 포함하거나 유지보수 접근 인터페이스를 가지고 있다는 점이 개발 문서에 명세되어 있다면 시험자는 개발 문서를 통하여 덮개나 개구부의 제거 또는 유지보수 접근 인터페이스에의 접근 발생 시 모듈이 모든 평문 CSP를 제로화하는지 확인해야 한다.

TE07.39.03
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 평문 CSP가 모듈 내부에 포함되어 있을 때 변조 응답 및 제로화 회로가 작동 상태로 유지되어 있는지 확인해야 한다.

TE07.39.04
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈에 높은 확률로 발생한 심각한 손상이 있지 않는 한 봉함이 제거되거나 침투되지 않음을 확인해야 한다.

TE07.39.05
봉함이 개구부 또는 제거 가능 덮개를 포함하거나 유지보수 접근 인터페이스를 가지고 있다는 점이 개발 문서에 명세되어 있다면 시험자는 덮개나 개구부가 제거될 때 또는 유지보수 접근 인터페이스에의 접근이 발생할 때 모듈이 모든 평문 CSP를 제로화한다는 것을 시험해야 한다.

TE07.39.06
시험자는 모듈에 높은 확률로 발생한 심각한 손상이 있지 않는 한 봉함이 제거되거나 침투되지 않음을 시험해야 한다.

AS07.40: (단일칩 암호모듈 – 보안수준 4)

다음 요구사항들은 보안수준 4에 따른 단일칩 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS07.41**과 **AS07.42**에서 시험된다.

AS07.41: (단일칩 암호모듈 – 보안수준 4)

모듈에서 코팅을 벗겨 내거나 들추어내려는 시도가 있을 때 모듈에 심각한 손상(즉, 모듈 기능의 정지)이 높은 확률로 일어나도록 경도가 높고 접착성이 있는 제거-방지용 불투명 코팅으로 모듈이 처리되어야 한다.

[벤더 요구사항]

VE07.41.01
벤더는 사용된 코팅의 종류를 명확하게 식별할 수 있도록 명세하고, 경도 특성 및 제거-방지 특성 등과 같은 코팅 특성을 상세하게 설명하는 개발 문서를 제출해야 한다.

VE07.41.02
벤더는 경도가 높고 불투명한 제거-방지 코팅으로 모듈 표면이 처리되어 있는 경우 이를 명세한 개발 문서를 제출해야 한다. 이 물질의 경도와 접착성은 이 물질을 모듈에서 벗겨 내거나 또는 들추어내려는 시도가 있을 때 모듈에 심각한 손상(즉, 모듈 기능의 정지)을 높은 확률로 줄 수 있어야 한다. 이 물질은 가시적 스펙트럼에서 불투명해야 한다.

[시험 절차]

TE07.41.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 모듈이 경도가 높고 불투명한 제거-방지 코팅으로 덮여 있는지 확인해야 한다.

TE07.41.02
시험자는 모듈 코팅이 제거-방지 특성을 가지고 있는지 확인해야 한다. 시험자가 모듈에서 물질을 벗겨 내거나 들추어내려고 시도할 때 모듈의 기능이 정지되며 또는 모듈 회로가 물리적으로 파괴됨을 확인해야 한다.

AS07.42: (단일칩 암호모듈 – 보안수준 4)

모듈의 코팅을 녹일 때 높은 확률로 모듈 자체를 녹이거나 모듈에 심각한 손상(즉, 모듈 기능의 정지)을 줄 수 있도록 제거-방지 코팅이 용해 특성을 가져야 한다.

[벤더 요구사항]

VE07.42.01
벤더는 제거-방지 코팅의 용해 특성을 명시한 개발 문서를 제출해야 한다. 코팅을 제거하기 위하여 그 물질을 녹이면 암호모듈 자체가 녹거나 모듈에 심각한 손상을 줄 수 있도록 코팅 물질이 용해 특성을 가져야 한다.

[시험 절차]

TE07.42.01

시험자는 개발 문서를 통하여 모듈의 제거-방지 코팅의 용해 특성을 확인해야 한다.

TE07.42.02
시험자는 모듈의 제거-방지 코팅의 용해 특성을 시험해야 한다. 시험자는 VE07.32.01에 따라 제출된 문서를 참조하여 어떤 유형의 용해가 제거-방지 코팅을 손상시키는 데 필요한지 확인해야 한다.

6.7.3.2 다중칩 내장형 암호모듈

비고 KS X ISO/IEC 19790의 **7.7.2**에 명시된 일반 보안 요구사항과 이에 추가한 다음 **AS07.43**~**AS07.58**의 요구사항이 다중칩 내장형 암호모듈에 적용되어야 한다.

AS07.43: (다중칩 내장형 암호모듈 – 보안수준 1, 2, 3 및 4)

암호모듈에 봉함이나 제거 가능 덮개가 처리되어 있다면, 생산 등급의 봉함 또는 제거 가능 덮개가 사용되어야 한다.

[벤더 요구사항]

VE07.43.01
모듈은 제품-등급의 봉함이나 제거 가능 덮개 내부에 전체적으로 처리되어야 하고, 벤더는 덮개 또는 봉함을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.43.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 모듈이 제품-등급인 봉함이나 제거 가능 덮개 내부에 포함되어 있는지 확인해야 한다.

AS07.44: (다중칩 내장형 암호모듈 – 보안수준 2, 3, 4)

다음 요구사항 {**AS07.45**~**AS07.46**}은 보안수준 2의 다중칩 내장형 암호모듈에 적용되어야 하고 {**AS07.45**~**AS07.46**은 다음 그룹, 즉 (**AS07.45**) 또는 (**AS07.46** 및 **AS07.47**) 또는 (**AS07.46** 및 **AS07.48**)을 충족해야 한다.}

[벤더 요구사항]

VE07.44.01
벤더는 보안수준 2의 다중칩 내장형 암호모듈이 (**AS07.45**) 또는 [**AS07.46** 및 (**AS07.47** 또는 **AS07.48**)]을 충족함을 명세하는 개발 문서를 제출해야 한다.

[시험 절차]

TE07.44.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 보안수준 2의 다중칩 내장형 암호모듈이 (**AS07.45**) 또는 [**AS07.46** 및 (**AS07.47** 또는 **AS07.48**)]을 충족하는지 확인해야 한다.

AS07.45: (다중칩 내장형 암호모듈 – 보안수준 2, 3, 4)

모듈 구성 요소는 직접 관찰을 방지하고 모듈 구성 요소를 변조하거나 제거하려는 시도를 할 때 증거를 제공할 수 있는 변조-증거 코팅 또는 매몰재(예: 에칭-방지 코팅 또는 비정상 표기 페인트)로

표면 처리되거나 {또는 (**AS07.46** 및 **AS07.47**) 또는 (**AS07.46** 및 **AS07.48**)이 충족되어야 한다.}

[벤더 요구사항]

VE07.45.01
벤더는 모듈이 에칭-방지 코팅 또는 비정상 표기(bleeding) 페인트와 같은 불투명한 변조-증거 코팅으로 캡슐화되어 있음을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.45.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 모듈이 불투명한 변조-증거 물질로 캡슐화되어 있는지 확인해야 한다.

TE07.45.02
시험자는 변조 시도 또는 모듈 구성 요소 제거 시도에 대해 모듈이 증거물을 남길 수 있는지 시험을 통하여 확인하여야 한다.

AS07.46: (다중칩 내장형 암호모듈 – 보안수준 2, 3, 4)

{만일 **AS07.45**가 충족되지 않으면, 이때} 모듈은 개구부나 제거 가능 덮개를 포함할 수 있는 금속으로 된 또는 경도가 높은 플라스틱으로 된 생산 등급 봉함 내부에 포함되어야 하고 {그리고 (**AS07.47** 및 **AS07.48**) 또는 (**AS07.47** 및 **AS07.49**)가 충족되어야 한다.}

[벤더 요구사항]

VE07.46.01
모듈은 제거 가능 덮개와 개구부를 포함할 수 있는 금속으로 된 또는 경도가 높은 플라스틱으로 된 생산 등급 봉함 내부에 포함되어야 한다. 벤더는 봉함과 봉함의 경도 특성을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.46.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈이 다음 요구사항을 충족하는 봉함에 내장되는지 확인해야 한다.

a) 봉함이 모듈 전체를 덮어 싸고 있어야 한다.
b) 봉함 물질은 개발 문서에 정의된 구성물이어야 한다.
c) 봉함은 생산 등급이어야 한다. 개발 문서는 봉함이 상업용으로 사용되고 있는 것과 동일한 물질을 명시하거나 상업용 제품과 동등함을 나타내는 자료를 제공해야 한다.

AS07.47: (다중칩 내장형 암호모듈 – 보안수준 2, 3, 4)

{만일 **AS07.45**가 만족되지 않는다면, 이때 만일} 봉함이 개구부나 제거 가능 덮개를 포함한다면, 개구부 또는 덮개는 물리적 또는 논리적 열쇠를 활용하여 따개-방지용 기계 잠금 장치로 잠그거나 {또는 **AS07.48**이 충족되어야 한다.}

[벤더 요구사항]

VE07.47.01
봉함에 포함된 개구부나 덮개는 물리적 또는 논리적 열쇠를 활용하여 따개-방지용 기계 잠금 장치로 잠가야 한다. 벤더는 잠금 장치와 활용된 물리적 또는 논리적 키를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.47.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 개구부나 덮개가 물리적 키 또는 논리적 키를 사용하여 따개-방지용 잠금 장치로 잠겨 있는지 확인해야 한다.

TE07.47.02
시험자는 잠금된 덮개나 개구부가 키 없이도 개방될 수 있는지 시도해 보고, 또한 손상 흔적도 없이 이들이 개방될 수 없음을 확인해야 한다.

AS07.48: (다중칩 내장형 암호모듈 – 보안수준 2, 3, 4)

{**AS07.45**가 충족되지 않고 봉함이 **AS07.47**을 적용하지 않은 개구부나 제거 가능 덮개를 포함한다면 이들(즉, 개구부나 제거 가능 덮개)은} 변조-증거 봉인(예: 증거 표시 테이프 또는 홀로그램 봉인)으로 보호되어야 하고 {그리고 (**AS07.47** 및 **AS07.49**)가 충족되어야 한다.}

[벤더 요구사항]

VE07.48.01
벤더는 변조-증거 봉인을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.48.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 덮개나 개구부가 증거 표시 테이프나 홀로그램 봉인과 같은 변조-증거 봉인으로 보호되고 있음을 확인해야 한다.

TE07.48.02
시험자는 덮개 또는 개구부가 봉인이 부서지거나 제거되지 않는 한 개봉될 수 없음을 확인해야 하고 봉인이 제거되거나 추후에 교체될 수 없음을 확인하여야 한다.

AS07.49: (다중칩 내장형 암호모듈 – 보안수준 3과 4)

다음 요구사항들은 보안수준 3의 다중칩 내장형 암호모듈에 적용되어야 한다.

비고 해당 시험 절차는 **AS07.50**이나 **AS07.51**에서 시험된다.

AS07.50: (다중칩 내장형 암호모듈 – 보안수준 3, 4)

{① 또는 ② 선택} ① 암호모듈 내부에 포함된 회로의 다중칩 형체는 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(즉, 모듈 기능의 정지)을 주는 경도 높은 코팅 또는 매몰재(예: 경도 높은 에폭시 물질)로 표면 처리되어야 하거나 {또는 ② **AS07.51**이 충족되어야 한다.}

[벤더 요구사항]

VE07.50.01
벤더는 경도 높은 코팅 또는 매몰재를 명세한 개발 문서를 제출해야 한다.

VE07.50.02
벤더는 코팅의 높은 경도나 매몰재의 불투명성을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.50.01
시험자는 개발 문서가 경도 높은 코팅 또는 매몰재를 명세하고 있는지 확인해야 한다.

TE07.50.02
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 경도 높은 코팅 또는 매몰재에 대하여 불투명한 특성을 확인해야 한다.

TE07.50.03
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 경도 높은 코팅 또는 매몰재는 높은 확률로 모듈에 심각한 손상을 주지 않는 한 제거되거나 침투되지 않음을 확인해야 한다.

AS07.51: (다중칩 내장형 암호모듈 – 보안수준 3, 4)

{만일 **AS07.50**이 적용되지 않는다면} 모듈은 봉함을 제거하려는 시도 시 또는 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(예: 모듈의 기능 정지)을 주는 강도 높은 봉함에 내장되어야 한다.

[벤더 요구사항]

VE07.51.01
벤더는 강도 높은 봉함을 명세한 개발 문서를 제출해야 한다. 모듈 전체가 강도 높은 봉함에 내장되어야 한다. 봉함은 이를 제거하려는 시도 시 높은 확률로 모듈 내부 회로에 심각한 손상(즉, 모듈의 기능 정지)을 주도록 설계되어야 한다.

VE07.51.02
봉함이 개구부나 제거 가능한 덮개를 포함한다면, 이때 모듈은 변조 대응 및 제로화 회로를 가져야 하며, 벤더는 변조 대응 및 제로화 회로를 명세한 개발 문서를 제출해야 한다. 이 회로는 덮개와 개구부를 지속적으로 감시해야 하며, 또한 덮개를 제거하거나 또는 개구부를 개봉할 때 모든 평문 CSP를 제로화해야 한다. 이 회로는 평문 CSP가 모듈 내부에 포함되어 있는 동안 작동 상태를 유지해야 한다.

[시험 절차]

TE07.51.01
시험자는 봉함이 개구부 또는 제거 가능 덮개를 포함하거나 유지보수 접근 인터페이스를 포함하면 모듈은 변조 대응 및 제로화 회로를 포함해야 하며 개발 문서에서 이를 명세하고 있는지 확인해야 한다.

TE07.51.02
봉함이 개구부나 제거 가능 덮개를 포함하거나 유지보수 접근 인터페이스가 규정되어 있으면, 시험자는 개구부나 덮개가 제거될 때 또는 유지보수 접근 인터페이스에 접속이 발생할 때 모든 평문 CSP를 제로화하는 모듈의 기능을 개발 문서에서 명세하고 있는지 확인해야 한다.

TE07.51.03
시험자는 VE07.51.01 및 VE07.51.02의 요구사항에 대한 구현과 관련 설계 내용이 개발 문서에 명시되어 있는지 확인해야 한다.

TE07.51.04
시험자는 암호모듈을 검사하고 개발 문서를 검토하여, 평문 CSP가 모듈에 포함되어 있을 때 변조 대응 및 제로화 회로가 항상 작동 상태로 유지되는지 확인해야 한다.

TE07.51.05
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 높은 확률로 모듈에 심각한 손상을 주지 않는 한 봉함이 제거되거나 침투되지 않음을 확인해야 한다.

TE07.51.06
시험자는 봉함 아래에 있는 회로에 접근을 시도하고 봉함이 쉽게 부서지지 않음을 검증하여 봉함의 경도 수준을 확인해야 한다. 시험자는 암호모듈을 검사하고 개발 문서를 검토하여 봉함이 제거될 수 없음을 확인해야 한다.

TE07.51.07
강도 높은 봉함이 개구부나 제거 가능 덮개를 포함한다면 또는 유지보수 접근 인터페이스가 규정되어 있다면, 시험자는 개발 문서를 통하여 덮개나 개구부가 제거될 때 모듈이 모든 평문 CSP를 제로화하는지 확인해야 한다.

TE07.51.08
봉함이 개구부나 제거 가능 덮개를 포함한다면 또는 유지보수 접근 인터페이스가 규정되어 있다면, 시험자는 시험을 통해 덮개나 개구부가 제거될 때 또는 유지보수 접근 인터페이스에 접속이 발생할 때 모듈이 모든 평문 CSP를 제로화하는지 확인해야 한다.

TE07.51.09
시험자는 모듈에 높은 확률로 심각한 손상을 주지 않는 한 봉함이 제거되거나 침투될 수 없음을 시험해야 한다.

AS07.52: (다중칩 내장형 암호모듈 – 보안수준 4)

다음 요구사항은 보안수준 4의 다중칩 내장형 암호모듈에 적용되어야 한다.

비고 해당 시험 항목 **AS07.53**～**AS07.59**에서 시험된다.

AS07.53: (다중칩 내장형 암호모듈 – 보안수준 4)

모듈 구성품은 강도 높고 경도가 높은 절연 또는 비절연 봉함에 내장되어야 한다.

[벤더 요구사항]

VE07.53.01
모듈은 매몰재나 봉함에 대한 변조 공격을 탐지하는 변조 탐지 겉봉함에 내장되어야 한다. 벤더는 변조 탐지 겉봉함을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.53.01

시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 모듈이 그 구성품을 모두 감싸고 있는 변조 탐지 겉봉함을 포함하는지 확인해야 한다. 모듈 내의 구성품을 감시하여 방어막이 모듈 구성품에 접근하기 위한 드릴하기, 밀링하기, 갈아내기 또는 분해하기 등의 변조 행위를 탐지할 수 있도록 설계되어야 한다.

AS07.54: (다중칩 내장형 암호모듈 – 보안수준 4)

{SSP에 충분한 범위까지 접근하기 위한 매몰재 혹은 봉함 자르기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기 등의 변조를 탐지하는} 겉봉함(예: 꼬불거리는 모양의 도체로, 휠 수 있는 절연막 인쇄 회로 또는 전선 묶음으로 둘러싼 패키지 또는 휘지 않으며 쉽게 부러지는 회로 또는 강도 높은 봉함)에 의해 봉함은 포장되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS07.55**에서 시험된다.

AS07.55: (다중칩 내장형 암호모듈 – 보안수준 4)

SSP에 충분한 범위까지 접근하기 위한 매몰재 혹은 봉함 자르기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기 등의 변조를 탐지하는 {겉봉함(예: 꼬불거리는 모양의 도체로, 휠 수 있는 절연막 인쇄 회로 또는 전선 묶음으로 둘러싼 패키지 또는 휘지 않으며 쉽게 부러지는 회로 또는 강도 높은 봉함)에 의해 봉함은 포장되어야 한다.}

[벤더 요구사항]

VE07.55.01
모듈은 매몰재나 봉함에 대한 변조 공격을 탐지하는 변조 탐지 겉봉함에 내장되어야 한다. 벤더는 변조 탐지 겉봉함을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.55.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈이 모듈 구성품을 둘러싸는 변조 탐지 겉봉함을 내장하는지 확인해야 한다. 이 방어막은 암호모듈 내부 구성품을 감시함에 의해 모듈 구성품에 접근하기 위한 자르기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기 등의 변조 행위를 탐지하도록 설계되어야 한다.

AS07.56: (다중칩 내장형 암호모듈 – 보안수준 4)

{변조 탐지 겉봉함을 지속적으로 감시해서 변조가 탐지되면 보호되지 않은 모든 SSP를 즉시 제로화해야 하는} 변조 대응 및 제로화 회로를 모듈은 포함해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS07.57**과 **AS07.58**에서 시험된다.

AS07.57: (다중칩 내장형 암호모듈 – 보안수준 4)

변조 탐지 겉봉함을 지속적으로 감시해서 {변조가 탐지되면 보호되지 않은 모든 SSP를 즉시 제로화해야 하는}{변조 대응 및 제로화 회로를 모듈은 포함해야 한다.}

[벤더 요구사항]

VE07.57.01
모듈은 변조 탐지 겉봉함을 지속적으로 감시해서 변조가 탐지되면 모든 평문 CSP를 제로화해야 하는 변조 대응 및 제로화 회로를 포함해야 한다. 평문 CSP가 모듈에 포함되어 있을 때 이 회로는 항상 작동 상태로 유지되어야 한다. 벤더는 변조 대응과 제로화를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.57.01
시험자는 개발 문서를 통하여 암호모듈이 변조 탐지 겉봉함을 지속적으로 감시하는, 즉 겉봉함 드릴하기, 밀링하기, 갈아내기 또는 분해하기와 같은 수단으로 변조가 일어나는지 탐지하고 그리고 탐지한 후 모든 평문 CSP를 제로화하는 변조 대응 및 제로화 회로를 포함하는지 확인해야 한다.

AS07.58: (다중칩 내장형 암호모듈 – 보안수준 4)

{모듈은 변조 탐지 겉봉함을 지속적으로 감사하는 변조 대응 및 제로화 회로를 포함해야 하며} 또한 변조가 탐지되었을 때 보호되지 않은 모든 SSP를 즉시 제로화해야 한다.

[벤더 요구사항]

VE07.58.01
모듈은 변조 탐지 겉봉함을 지속적으로 감사하는 변조 대응 및 제로화 회로를 포함해야 하며 또한 변조가 탐지되었을 때 모든 평문 SSP를 제로화해야 한다. 벤더는 변조 대응 및 제로화 회로를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.58.01
시험자는 변조 탐지 겉봉함 방어막을 파괴해 보고 모듈이 모든 평문 CSP를 제로화하는지 확인해야 한다.

AS07.59: (다중칩 내장형 암호모듈 – 보안수준 4)

암호모듈 내부에 보호되지 않은 SSP가 포함되어 있을 때 변조 대응 회로는 항상 작동 상태를 유지해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

6.7.4 다중칩 독립형 암호모듈

비고 KS X ISO/IEC 19790의 **7.7.2**에 명시된 일반 보안 요구사항과 이에 추가한 다음 **AS07.60**~**AS07.71**의 요구사항들이 다중칩 독립형 암호모듈에 적용되어야 한다.

AS07.60: (다중칩 독립형 암호모듈 – 보안수준 1, 2, 3, 4)

암호모듈은 개구부 또는 제거 가능 덮개를 포함할 수 있는 금속이거나 경도가 높은 플라스틱으로 된 생산 등급 봉함에 모듈 전체가 내장되어야 한다.

[벤더 요구사항]

VE07.60.01

암호모듈은 개구부 또는 제거 가능 덮개를 포함할 수 있는 금속이거나 경도가 높은 플라스틱으로 된 생산 등급 봉함에 모듈 전체가 내장되어야 한다. 벤더는 봉함과 이것의 경도 특성을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.60.01
시험자는 암호모듈을 육안으로 검사하고 개발 문서를 검토하여 모듈이 다음 요구사항을 충족하는 봉함에 내장되는지 확인해야 한다.

a) 봉함이 모듈 전체를 덮어 싸고 있어야 한다.
b) 봉함 물질은 개발 문서에 정의된 구성물이어야 한다.
c) 봉함은 생산 등급이어야 한다. 개발 문서는 봉함이 상업용으로 사용되고 있는 것과 동일한 물질을 명시하거나 상업용 제품과 동등함을 나타내는 자료를 제공해야 한다.

AS07.61: (다중칩 독립형 암호모듈 – 보안수준 2, 3, 4)

다음 요구사항은 보안수준 2의 다중칩 독립형 암호모듈에 적용되어야 한다.

비고 해당 시험 절차는 **AS07.62** 또는 **AS07.63**에서 시험된다.

AS07.62: (다중칩 독립형 암호모듈 – 보안수준 2, 3, 4)

암호모듈의 봉함이 개구부 또는 제거 가능 덮개를 포함한다면 개구부 또는 덮개는 물리적 또는 논리적 키를 적용한 따개-방지 기계 잠금 장치로 잠금이 되거나 {또는 **AS07.63**이 적용되어야 한다.}

[벤더 요구사항]

VE07.62.01
암호모듈의 봉함이 개구부 또는 제거 가능 덮개를 포함한다면 개구부 또는 덮개는 물리적 또는 논리적 키를 적용한 따개-방지 기계 잠금 장치로 잠금이 되어야 한다. 벤더는 물리적 키 또는 논리적 키를 적용한 따개-방지 기계 잠금 장치를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.62.01
시험자는 봉함이 제거 가능 덮개나 개구부를 포함하고 있는지 확인하여야 한다. 시험자는 각 덮개 또는 개구부가 물리적 키 또는 논리적 키를 필요로 하는 따개-방지 잠금 장치로 잠겨 있는지 확인해야 한다. 시험자는 키를 사용하지 않고 잠금된 덮개나 개구부를 개방을 시도해 보고 덮개나 개구부가 손상 흔적 없이 개방되지 않음을 확인해야 한다.

AS07.63: (다중칩 독립형 암호모듈 – 보안수준 2, 3, 4)

{**AS07.62**가 충족되지 않는다면, 이때 개구부나 덮개는} 변조-증거 봉인(예: 증거 테이프 또는 홀로그램 봉인)으로 보호되어야 한다.

[벤더 요구사항]

VE07.63.01

봉함이 증거 테이프 또는 홀로그램 봉인과 같은 변조-증거 봉인으로 보호된다면, 개발 문서는 변조-증거 봉인을 명시해야 한다.

[시험 절차]

TE07.63.01
덮개나 개구부는 증거 테이프나 홀로그램 봉인과 같은 봉인으로 보호되어야 한다. 시험자는 덮개 또는 개구부가 봉인이 부서지거나 제거되지 않는 한 개봉될 수 없음을 확인해야 하고, 봉인이 제거되거나 이후에 대체될 수 없음을 확인해야 한다.

AS07.64: (다중칩 독립형 암호모듈 – 보안수준 3, 4)

다음 요구사항은 보안수준 3의 다중칩 독립형 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS07.65**에서 시험된다.

AS07.65: (다중칩 독립형 암호모듈 – 수준 3과 4)

모듈은 봉함을 제거거나 침투하려는 시도 시 높은 확률로 모듈에 심각한 손상(예: 모듈의 작동 정지)을 주는 강도 높은 봉함에 내장되어 있어야 한다.

[벤더 요구사항]

VE07.65.01
벤더는 강도 높은 봉함을 명세한 개발 문서를 제출해야 한다. 강도 높은 봉함에 모듈 전체가 내장되어야 한다. 봉함은 이를 제거하려는 시도 시 높은 확률로 모듈 내부 회로에 심각한 손상(예: 모듈의 기능 정지)이 일어나도록 설계되어야 한다.

VE07.65.02
봉함이 개구부나 제거 가능한 덮개를 포함한다면 모듈은 변조 대응 및 제로화 회로를 포함해야 한다. 이 회로는 덮개와 개구부를 지속적으로 감시해야 하며, 덮개를 제거하거나 개구부를 개방하면 모든 평문 CSP를 제로화해야 한다. 이 회로는 평문 CSP가 모듈 내부에 있는 동안에는 항상 작동 상태를 유지해야 한다. 벤더는 변조 대응 및 제로화 회로를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.65.01
시험자는 개구부 또는 제거 가능 덮개를 포함하고 있거나 유지보수 접근 인터페이스가 봉함에 규정되어 있으면 모듈은 변조 응답 및 제로화 회로를 포함하고 있음을 개발 문서를 통하여 확인해야 한다.

TE07.65.02
봉함이 개구부나 제거 가능 덮개를 포함하거나 또는 유지보수 접근 인터페이스가 규정되어 있다면 시험자는 개구부나 덮개가 제거될 때 또는 유지보수 접근 인터페이스에 접속이 발생할 때 모듈이 모든 평문 CSP를 제로화하는 기능을 개발 문서에 명세하고 있는지 확인해야 한다.

TE07.65.03
시험자는 개발 문서가 VE07.51.01 및 VE07.51.02의 요구사양의 구현과 설계 내용을 명시하고 있는지 확인해야 한다.

TE07.65.04

시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈 내부에 평문 CSP가 포함되어 있을 때 대응 및 제로화 회로가 항상 작동 상태를 유지하는지 확인해야 한다.

TE07.65.05
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 높은 확률로 모듈에 심각한 손상을 주지 않는 한 봉함이 제거되거나 침투되지 않음을 확인해야 한다.

TE07.65.06
시험자는 봉함 아래에 있는 회로에 접근해 보고 봉함이 붕괴되지 않음을 검증하여 봉함의 강도를 확인해야 한다. 시험자는 암호모듈을 검사하고 개발 문서를 검토하여 봉함이 제거될 수 없음을 확인해야 한다.

TE07.65.07
강도 높은 봉함이 개구부나 제거 가능 덮개를 포함한다면 또는 유지보수 접속 인터페이스가 규정되어 있다면, 시험자는 개발 문서를 통하여 덮개나 개구부가 제거될 때 모듈이 모든 평문 CSP를 제로화시키고 있음을 확인해야 한다.

TE07.65.08
봉함이 개구부나 제거 가능 덮개를 포함한다면 또는 만일 유지보수 접속 인터페이스가 규정되어 있다면, 시험자는 시험을 통해 덮개나 개구부가 제거될 때 또는 유지 관리 접속 인터페이스에 접근될 때 모듈이 모든 평문 CSP들을 제로화시키고 있는지 확인해야 한다.

TE07.65.09
시험자는 시험을 통하여 높은 확률로 모듈에 심각한 손상을 주지 않는 한 봉함이 제거되거나 침투되지 않음을 확인해야 한다.

AS07.66: (다중칩 독립형 암호모듈 – 보안수준 4)

다음 요구사항은 보안수준 4의 다중칩 독립형 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS07.67**～**AS07.72**에서 시험된다.

AS07.67: (다중칩 독립형 암호모듈 – 보안수준 4)

암호모듈의 봉함은 덮개 스위치(예: 마이크로 스위치, 자기장 홀 효과 스위치, 영구자석 구동기 등), 움직임 검출기(예: 초음파, 적외선 또는 마이크로웨이브) 또는 {KS X ISO/IEC 19790} **7.7.3.2** 보안수준 4에 명시된 기타 변조 탐지 메커니즘과 같은 변조 탐지 메커니즘을 사용하는 변조 탐지 겉봉함을 포함해야 한다.

[벤더 요구사항]

VE07.67.01
봉함이나 매몰재는 겉봉함에 대한 변조 공격을 탐지할 수 있는 변조 탐지 메커니즘을 사용하여 포장되어야 한다. 벤더는 변조 탐지 겉봉함 설계를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.67.01
시험자는 암호모듈을 검사하고 개발 문서를 검토하여 모듈 봉함이나 매몰재가 모듈 구성품 보호용 변조 탐지 겉봉함으로 구성되는 변조 탐지 메커니즘을 포함하는지 확인해야 한다. 이 메커니즘은 모

듈 구성품에 접근하는 봉함 또는 매몰재에 대한 변조를 탐지할 수 있도록 설계되어야 한다.

AS07.68: (다중칩 독립형 암호모듈 – 보안수준 4)

변조 탐지 메커니즘은 SSP에 충분한 범위까지 접근하기 위해 시도되는 잘라내기, 드릴하기, 밀링하기, 갈아내기, 태우기, 용해하기 또는 분해하기와 같은 공격에 대응해야 한다.

비고 해당 시험 항목은 **AS07.71**의 일부분으로 시험된다.

AS07.69: (다중칩 독립형 암호모듈 – 보안수준 4)

암호모듈은 {변조 탐지 겉봉함을 지속적으로 감시하고 변조 탐지 시 보호되지 않은 모든 SSP를 즉시 제로화해야 하는} 변조 응답 및 제로화 기능을 포함해야 한다.

비고 해당 시험 항목은 **AS07.71**의 일부분으로 시험된다.

AS07.70: (다중칩 독립형 암호모듈 – 보안수준 4)

{암호모듈은} 변조 탐지 겉봉함을 지속적으로 감시하고 {변조 탐지 시 보호되지 않은 모든 SSP를 즉시 제로화해야 하는 변조 응답 및 제로화 기능을 포함해야 한다.}

비고 해당 시험 항목은 **AS07.71**의 일부분으로 시험된다.

AS07.71: (다중칩 독립형 암호모듈 – 수준 4)

{암호모듈은 변조 탐지 겉봉함을 지속적으로 감시하고} 변조가 탐지될 때 보호되지 않은 모든 SSP를 즉시 제로화해야 하는 {변조 응답 및 제로화 기능을 포함해야 한다.}

[벤더 요구사항]

VE07.71.01
모듈은 변조 탐지 겉봉함을 지속적으로 감시하는 변조 대응 및 제로화 회로를 포함해야 하며 변조가 탐지될 때 보호되지 않은 모든 SSP를 제로화해야 한다. 평문 SSP가 암호모듈 내부에 포함되어 있을 때 이 회로는 작동 상태를 유지해야 한다. 벤더는 이 변조 대응 및 제로화 설계를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.71.01
시험자는 개발 문서를 통하여 변조 탐지 겉봉함을 지속적으로 감시하고 또한 겉봉함에 드릴하기, 밀링하기, 갈아내기 또는 분해하기와 같은 수단으로 변조하는 것을 탐지하고 또한 탐지 후 모든 평문 SSP를 제로화하는 변조 대응 및 제로화 회로를 암호모듈이 포함하는지 확인해야 한다.

TE07.71.02
시험자는 변조 탐지 겉봉함 방어막을 파괴해 보고 모듈이 모든 평문 SSP를 제로화시키는지 확인해야 한다.

AS07.72: (다중칩 독립형 암호모듈 – 수준 4)

보호되지 않는 SSP가 암호모듈 내부에 포함되어 있을 때 변조 대응 및 제로화 회로 기능이 작동 상

태를 유지하고 있어야 한다.

비고 해당 시험 항목은 **AS07.71**의 일부분으로 시험된다.

6.7.5 환경장애보호 및 환경장애시험

6.7.5.1 환경장애보호와 환경장애시험에 대한 일반요구사항

비고 암호모듈은 보안수준 1과 2에서 환경장애보호 특성 또는 환경장애시험을 요구하지 않는다.

AS07.73: (환경장애보호/시험 – 보안수준 3, 4)

모듈은 환경장애보호(EFP) 특성 {**AS07.75**～**AS07.77**}을 충족하거나 환경장애시험(EFT) {**AS07.78**～**AS07.84**}를 충족해야 한다.

[벤더 요구사항]

VE07.73.01
벤더는 아래 둘 중 하나를 적용해야 한다.

a) EFP 특성
b) EFT

KS X ISO/IEC 19790의 **7.7.4**에 명시된 바와 같이, 모듈의 정상 동작 범위를 벗어난 다음 4가지 비정상 환경 조건이나 상황 변동(우발적 또는 고의적)으로 인해 모듈의 안전성을 손상하지 않음을 보증해야 한다.

a) 저온
b) 고온
c) 큰 음(－) 전압
d) 큰 양(＋) 전압

벤더는 각 조건에 따라 EFP 또는 EFT를 사용하는 것을 선택해야 한다. 조건에 따른 각 선택은 서로 독립적이다. 벤더는 각 조건에 따른 EFP 또는 EFT를 명세한 개발 문서와 선택된 방법이 어떻게 사용되는지 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.73.01
시험자는 개발 문서를 통하여 각 조건에 따른 EFP 또는 EFT 선택을 명시하고 있는지 그리고 명세된 방법이 어떻게 사용되고 있는지 확인해야 한다.

AS07.74: (환경장애보호/시험 – 보호 수준 4)

모듈은 환경시험보호(EFP) 특성을 적용하고 있어야 한다.

비고 시험 항목은 **AS07.75**～**AS07.77**에서 시험된다.

6.7.5.2 환경장애보호 특성

AS07.75: (환경장애보호 특성 – 보호 수준 3, 4)

환경장애보호(EFP) 특성은 모듈의 안전성을 손상시킬 수 있는 모듈의 정상 동작 범위 밖일 때의 비정상 환경 조건들(우발적 또는 고의적)로부터 암호모듈을 보호해야 한다.
비고 해당 시험 항목은 **AS07.77**의 일부분으로 시험된다.

AS07.76: (환경장애보호 특성 – 보안수준 3, 4)

동작 온도 및 동작 전압이 규정된 정상 동작 범위를 벗어날 때 암호모듈은 이를 감시하고 정확하게 대응해야 한다.

비고 해당 시험 항목은 **AS07.77**의 일부분으로 시험된다.

AS07.77: (환경장애보호 특성 – 보안수준 3, 4)

온도 또는 전압이 암호모듈의 정상 동작 범위를 벗어난다면, 보호 기능은 다음 둘 중 하나를 수행해야 한다.

- 동작 진행을 방지하기 위해 암호모듈을 정지함.
- 보호되지 않은 모든 SSP를 즉시 제로화함.

[벤더 요구사항]

VE07.77.01
EFP가 특정 조건에서 선택되었다면, 그 조건에서 모듈의 정상 동작 범위를 벗어날 때 모듈은 동작 온도나 동작 전압의 변동을 감시하고 적절히 대응해야 한다. EFP 특성은 이들 환경 조건을 지속적으로 측정해야 한다. 어떤 조건이 모듈의 정상 동작 범위를 벗어난다면, 보호 회로는 다음 둘 중 하나를 수행해야 한다.

a) 모듈을 정지함.
b) 모든 평문 SSP를 제로화함.

벤더는 모듈에 어떤 방법이 선택되었는지 명세한 개발 문서와 구현된 EFP 특성을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.77.01
시험자는 모듈에 규정된 정상 동작 범위에 근접하는 환경 조건(환경 온도 및 환경 전압)을 설정하고 모듈이 정상 동작 파라미터 내에서는 작동을 지속하는지 확인해야 한다.

TE07.77.02
시험자는 규정된 정상 범위를 벗어나도록 온도와 전압을 확장했을 때 모듈이 동작을 진행할 수 없게 정지하거나 모든 평문 SSP를 제로화하는지 확인해야 한다.

TE07.77.03
모듈이 모든 평문 SSP를 제로화시키도록 설계되었다면 또한 모듈이 정상 동작 범위로 복귀한 후에도 동작 상태에 있다면, 시험자는 키가 필요한 서비스를 수행하고 모듈이 이들 서비스들을 수행하지 못하는지 확인해야 한다.

6.7.5.3 환경장애시험 절차

AS07.78: (환경장애시험 절차 – 보안수준 3, 4)

환경장애시험(EFT)은 온도 및 전압이 모듈의 정상 동작 범위를 벗어났을 때 환경 조건(우발적 또는 고의적)에 의해 모듈의 안전성이 손상되지 않음을 보장하기 위해 암호모듈을 분석하고 시뮬레이션하고 시험하는 절차를 포함해야 한다.

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.79: (환경장애시험 절차 – 보안수준 4)

동작 온도 및 동작 전압이 모듈에 오류를 일으킬 만큼 정상 동작 범위를 벗어난다면, {어떠한 순간에서라도 암호모듈의 안전성이 손상되지 않음을} EFT는 입증해야 한다.

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.80: (환경장애시험 절차 – 보안수준 4)

{동작 온도 및 동작 전압이 모듈에 오류를 일으킬 만큼 정상 동작 범위를 벗어난다면,} 어떠한 순간에서라도 암호모듈의 안전성이 손상되지 않음을 {EFT는 입증해야 한다.}

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.81: (환경장애시험 절차 – 보안수준 4)

시험 온도 범위는 정상 동작 범위 안의 임의의 온도에서부터 ① 모듈을 동작하지 못하도록 정지시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 최저 온도(즉, 최저 추운 온도)까지 지정되어야 한다. 또한 시험 온도 범위는 정상 동작 범위 안의 임의의 온도에서부터 ① 모듈을 정지시키거나 오류 상태로 전환하거나 또는 ② 보호되지 않은 모든 SSP를 제로화시키는 최고 온도(즉, 최고 뜨거운 온도)까지 지정되어야 한다.

[벤더 요구사항]

VE07.81.01
EFT가 특정 조건에서 선택되었다면 모듈은 **AS07.82**에서 규정된 온도 및 전압 범위 내에서 시험되어야 한다. 모듈은 다음 동작 중에서 수행되어야 한다.

a) 계속 정상 작동
b) 작동 정지
c) 모든 평문 SSP 제로화

벤더는 모듈에 어떤 방법이 선택되었는지 명세한 개발 문서와 구현된 EFT를 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE07.81.01
시험자는 **AS07.82**에 명세되어 있는 것과 같이 환경 조건(환경 온도 및 환경 전압)을 설정한 후 모듈

이 정상 작동을 계속하는지, 또는 작동하지 않도록 정지하는지, 또는 모든 평문 SSP를 제로화하는지 확인해야 한다.

TE07.81.02
모듈이 모든 평문 SSP를 제로화시키도록 설계되었다면, 만일 모듈이 정상 환경 범위로 복귀한 후에도 동작하고 있다면, 시험자는 키가 필요한 서비스를 수행해 보고 모듈이 이들 서비스들을 수행하지 못하는지 확인해야 한다.

AS07.82: (환경장애시험 절차－보안수준 4)

시험 온도 범위는 섭씨 －100°부터 ＋200°까지(화씨 －150°부터 ＋400°까지) 지정되어야 한다. {그러나 ① 모듈이 작동되지 못하도록 중단하거나, ② 보호되지 않은 모든 SSP가 즉시 제로화되거나, 또는 ③ 모듈이 고장 상태에 진입하자마자 그 시험(EFT)은 중단되어야 한다.}

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.83: (환경장애시험 절차－보호 수준 4)

{시험 온도 범위는 섭씨 －100°부터 ＋200°까지(화씨 －150°부터 ＋400°까지) 지정되어야 한다.} 그러나 ① 모듈이 작동되지 못하도록 중단하거나, ② 보호되지 않은 모든 SSP가 즉시 제로화되거나, 또는 ③ 모듈이 고장 상태에 진입하자마자 그 시험(EFT)은 중단되어야 한다.

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.84: (환경장애시험 절차－보안수준 4)

모듈의 물리적 경계는 제외시키고, 중요한 구성 요소와 핵심 장치에서의 온도가 내부에서 감시되어야 한다.

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.85: (환경장애시험 절차－보안수준 4)

시험 전압 범위는 정상 동작 전압 범위 내 임의의 전압으로부터 ① 작동하지 못하도록 모듈을 중지시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 저전압까지 점진적으로 낮출 수 있어야 한다. {또한 시험 전압 범위는 정상 동작 전압 범위 내의 임의의 전압으로부터 ① 작동하지 못하도록 모듈을 중단시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 고전압까지 점차적으로 높일 수 있어야 한다.}

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

AS07.86: (환경장애시험 절차－보안수준 4)

{시험 전압 범위는 정상 동작 전압 범위 내 임의의 전압으로부터 ① 작동하지 못하도록 모듈을 중지시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 저전압까지 점진적으로 낮출 수 있어야 한다.} 또한 시험 전압 범위는 정상 동작 전압 범위 내의 임의의 전압으로부터 ① 작동하지 못하도록 모듈을 중단시키거나 또는 ② 보호되지 않은 모든 SSP를 즉시 제로화시키는 고전압까지 점차적으로 높일 수 있어야 한다.

비고 해당 시험 항목은 **AS07.81**의 일부분으로 시험된다.

6.8 비침투 보안

AS08.01: (비침투 보안－보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790} **부속서** F에 언급되지 않은 암호모듈 SSP의 보호를 위한 암호모듈에 구현되어 있는 비침투 공격에 대한 완화 방법은 {KS X ISO/IEC 19790} **7.12**의 요구사항을 충족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다. 해당 시험 항목은 **AS12.01**～**AS12.04**의 일부분으로 시험된다.

AS08.02: (비침투 보안－보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790} **부속서** F에 언급된 암호모듈 SSP의 보호를 위한 암호모듈에 구현되어 있는 비침투 공격에 대한 완화 방법은 다음의 요구사항을 충족해야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS08.03: (비침투 보안－보안수준 1, 2, 3, 4)

KS X ISO/IEC 19790의 **A.2.8**에 명세한 개발 문서를 제공해야 한다.

[벤더 요구사항]

VE08.03.01
벤더는 KS X ISO/IEC 19790의 **A.2.8**에 명세한 개발 문서를 제공해야 한다.

[시험 절차]

TE08.03.01
시험자는 벤더가 제공한 KS X ISO/IEC 19790의 **A.2.8**에 명세되어 있는 개발 문서를 확인한다.

AS08.04: (비침투 보안－보안수준 1, 2, 3, 4)

개발 문서는 {KS X ISO/IEC 19790} **부속서** F에 언급된 암호모듈 CSP의 보호를 위한 암호모듈에 적용된 모든 비침투 공격에 대한 완화 방법을 명세해야 한다.

[벤더 요구사항]

VE08.04.01
벤더는 개발 문서에서 {KS X ISO/IEC 19790} **부속서** F에 언급된 비침투 공격에 대해서 CSP가 보호됨을 확인할 수 있도록 모든 비침투 공격에 대한 약화 방법을 명세해야 한다.

[시험 절차]

TE08.04.01
시험자는 벤더에서 제공받은 개발 문서를 확인한다. 개발 문서에서는 {KS X ISO/IEC 19790} **부속서** F에 언급된 비침투 공격에 대해서 CSP가 보호됨을 확인할 수 있도록 모든 비침투 공격에 대한 약화 방법을 명세한다.

AS08.05: (비침투 보안－보안수준 1, 2, 3, 4)

개발 문서는 각각의 공격 약화 방법의 영향에 대해 입증할 수 있어야 한다.
[벤더 요구사항]

VE08.05.01
벤더는 약화 방법의 영향 분석에 대해 개발 문서에 명세해야 한다.

[시험 절차]

TE08.05.01
시험자는 벤더에게서 제공받은 약화 방법의 영향 분석을 확인한다.

AS08.06: (비침투 보안－보안수준 3)

보안수준 3의 암호모듈에 대해서 {KS X ISO/IEC 19790} **부속서** F에서 명세한 검증대상 비침투 공격 약화 방법에 대한 시험이 수행되어야 한다.

[벤더 요구사항]

VE08.06.01
보안수준 3을 위해서 벤더는 암호모듈이 검증대상 비침투 약화 방법을 제공함을 확인할 수 있는 문서를 제공해야 한다.

[시험 절차]

TE08.06.01
보안수준 3을 위해서 시험자는 벤더에게서 받은 검증대상 비침투 약화 방법을 제공한 문서를 확인한다.

AS08.07: (비침투 보안－보안수준 4)

보안수준 4의 암호모듈은 {KS X ISO/IEC 19790} **부속서** F에서 명세한 검증대상 비침투 공격 약화 방법에 대한 시험이 수행되어야 한다.

[벤더 요구사항]

VE08.07.01
보안수준 4를 위해서 시험자는 벤더에게서 받은 검증대상 비침투 약화 방법을 제공한 문서를 확인한다.

[시험 절차]

TE08.07.01
보안수준 4를 위해서 시험자는 벤더에게서 받은 검증대상 비침투 약화 방법을 제공한 문서를 확인한다.

6.9 중요 보안매개변수 관리

6.9.1 중요 보안매개변수 관리의 일반 요구사항

AS09.01: (중요 보안매개변수 관리 – 보안수준 1, 2, 3, 4)

CSP는 암호모듈 내에서 인가되지 않은 접근, 사용, 노출, 변경 및 대체로부터 보호되어야 한다.

[벤더 요구사항]

VE09.01.01
개발 문서에는 암호모듈 내부의 모든 CSP에 대한 보호 방법이 서술되어야 한다. 보호 방법에는 인가되지 않은 접근, 사용, 노출, 변경 및 대체를 막기 위한 메커니즘의 구현 방법이 포함되어야 한다.

[시험 절차]

TE09.01.01
시험자는 CSP에 대한 보호 방법이 개발 문서에 서술되어 있는지 확인해야 한다. 시험자는 인가되지 않은 접근, 사용, 노출, 변경 및 대체를 막기 위한 방법이 문서에 서술되어 있는지 확인해야 한다.

TE09.01.02
시험자는 접근이 허용되지 않은 CSP에 대하여 문서에서 보호한 메커니즘을 우회한 접근을 시도해야 한다. 모듈이 접근을 거부하면 해당 시험 항목이 충족된다.

TE09.01.03
시험자는 개발 문서에 명세되지 않은 방법을 사용하여 CSP에 대한 변경을 시도해야 한다.

비고 비검증대상 알고리즘 또는 독자적인 알고리즘이나 방법으로 암호화된 CSP는 평문으로 간주된다.

AS09.02: (중요 보안매개변수 관리 – 보안수준 1, 2, 3, 4)

PSP는 암호모듈 내에서 인가되지 않은 변경과 대체로부터 보호되어야 한다.

[벤더 요구사항]

VE09.02.01
개발 문서에는 인가되지 않은 변경과 대체로부터 모든 PSP를 보호하는 방법이 서술되어야 한다.

[시험 절차]

TE09.02.01
시험자는 개발 문서에 인가되지 않은 변경과 대체로부터 PSP를 보호하는 방법이 서술되어 있는지 확인해야 한다.

TE09.02.02
시험자는 개발 문서에 명세되지 않은 방법으로 모든 PSP에 대한 변경을 시도해야 하고, 모든 PSP를 명세되지 않은 방법을 사용하여 주입하려는 시도를 해야 한다.

AS09.03: (중요 보안매개변수 관리 – 보안수준 1, 2, 3, 4)

암호모듈은 생성, 주입되거나 출력되는 SSP를 지정된 개체(사람, 그룹, 역할 또는 프로세스)와 연계시켜야 한다.

[벤더 요구사항]

VE09.03.01
개발 문서에는 각각의 SSP가 올바른 개체와 연계되어 있는지 확인하는 메커니즘 또는 절차가 서술되어야 한다.

[시험 절차]

TE09.03.01
시험자는 문서화된 SSP 주입 또는 출력 절차가 주입 또는 출력된 SSP를 정확한 개체와 연결시키는 방법을 서술하고 있는지 확인해야 한다.

TE09.03.02
주입될 수 있는 각각의 SSP에 대하여 다음 시험을 수행한다. 시험자는 우선 올바른 개체와 연계된 SSP를 주입한다. 그 다음 올바르지 않은 개체와 연계된 SSP는 주입이 불가능함을 확인한다.

TE09.03.03
출력될 수 있는 각각의 SSP에 대하여 다음 시험을 수행한다. 시험자는 우선 올바른 개체와 연계된 SSP를 출력한다. 시험자는 그 다음 SSP와 올바르지 않은 개체와 연계된 SSP는 출력이 불가능함을 확인한다.

AS09.04: (중요 보안매개변수 관리 – 보안수준 1, 2, 3, 4)

패스워드의 해시값, 난수 발생기의 상태 정보 및 키 생성 중간값은 CSP로 간주되어야 한다.

[벤더 요구사항]

VE09.04.01
벤더는 패스워드의 해시값, 난수 발생기의 상태 정보 및 키 생성 중간값이 CSP로 정의된 개발 문서를 제공해야 한다.

[시험 절차]

TE09.04.01
시험자는 패스워드의 해시값, 난수 발생기의 상태 정보 및 키 생성 중간값을 CSP로 정의한 개발 문서를 확인해야 한다.

TE09.04.02
시험자는 패스워드의 해시값, 난수 발생기의 상태 정보 및 키 생성 중간값을 CSP로 정의한 보안정책 문서를 제공함을 확인해야 한다.

AS09.05: (중요 보안매개변수 관리 – 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790}의 **A.2.9**에 명세된 요구사항을 충족하는 개발 문서가 제공되어야 한다.

[벤더 요구사항]

VE09.05.01
벤더는 KS X ISO/IEC 19790의 **A.2.9**에 명세된 요구사항을 충족하는 개발 문서를 제공해야 한다.

[시험 절차]

TE09.05.01
시험자는 KS X ISO/IEC 19790의 **A.2.9**에 명세된 요구사항을 충족하는 개발 문서가 제공되었는지 확인해야 한다.

6.9.2 난수 발생기

비고 암호모듈은 다수의 난수 발생기, 난수 발생기의 체인 또는 단 하나의 난수 발생기를 포함할 수 있다.

AS09.06: (난수 발생기 – 보안수준 1, 2, 3, 4)

검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 난수가 필요하면, 이를 제공하기 위해 검증대상 난수 발생기가 사용되어야 한다.

비고 검증대상 난수 발생기는 KS X ISO/IEC 19790의 **부속서** C에 목록으로 제공되어 있다.

[벤더 요구사항]

VE09.06.01
벤더는 암호모듈 내에서 검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 사용된 모든 난수 발생기의 목록과 정확한 사용법을 제공해야 한다.

VE09.06.02
벤더는 검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 사용된 모든 난수가 검증대상 난수 발생기로부터 제공되었음을 문서화해야 한다.

[시험 절차]

TE09.06.01
시험자는 검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 사용된 모든 난수 발생기가 문서에 포함되어 있고 사용법이 정의되어 있는지 확인해야 한다.

TE09.06.02
시험자는 개발 문서로부터 검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 사용된 모든 난수 발생기가 KS X ISO/IEC 19790의 **부속서** C에 정의된 검증대상 난수 발생기 목록을 준수하는지 확인해야 한다.

TE09.06.03
시험자는 개발 문서로부터 검증대상 암호알고리즘, SSP 생성 또는 SSP 설정에 사용된 난수가 검증대상 난수 발생기로부터 제공된 것인지 확인해야 한다.

AS09.07: (난수 발생기 – 보안수준 1, 2, 3, 4)

엔트로피가 암호모듈의 암호 경계 외부에서 수집된다면, 엔트로피 입력으로 생성된 데이터는 CSP로 간주되어야 한다.

[벤더 요구사항]

VE09.07.01
암호모듈의 암호 경계 외부에서 수집된 엔트로피로부터 생성된 입력 데이터는 개발 문서에서 CSP로 정의되어야 한다.

[시험 절차]

TE09.07.01
시험자는 암호모듈의 암호 경계 외부에서 수집된 엔트로피로부터 생성된 입력 데이터는 개발 문서에 CSP로 정의되어 있는지 확인해야 한다.

6.9.3 중요 보안매개변수 생성

AS09.08: (중요 보안매개변수 생성 – 보안수준 1, 2, 3, 4)

검증대상 난수 발생기의 출력을 이용하는 SSP 생성을 손상하는 행위(예: 결정론적 난수 발생기를 초기화하는 시드값 추측)는 적어도 생성된 SSP의 값을 전수 조사로 찾는 만큼의 연산량을 필요로 해야 한다.

[벤더 요구사항]

VE09.08.01
벤더는 SSP 생성을 손상하는 행위(예를 들면, 결정론적 난수 발생기를 초기화하는 시드값 추측)는 적어도 생성된 SSP의 값을 전수 조사하여 찾는 만큼의 연산량이 필요하다는 근거를 설명한 개발 문서를 제공해야 한다.

[시험 절차]

TE09.08.01
시험자는 SSP 생성을 손상하는 행위(예를 들면, 결정론적 난수 발생기를 초기화하는 시드값 추측)는 적어도 생성된 SSP의 값을 전수 조사하여 찾는 만큼의 연산량을 필요로 한다는 근거가 개발 문서에 제시되었는지 확인해야 한다.

TE09.08.02
시험자는 벤더가 제공한 근거가 정확한지 확인해야 한다. 입증의 책임은 벤더에 있다. 부정확하거나 모호한 점이 있으면 시험자는 필요에 따라 벤더에게 추가적인 정보를 요구할 수 있다.

AS09.09: (중요 보안매개변수 생성 – 보안수준 1, 2, 3, 4)

① 검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로, 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP는 KS X ISO/IEC 19790의 **부속서** D의 목록에 제시된 검증대상 SSP 생성 방법을 사용해야 한다.

비고 검증대상 SSP 생성 방법은 KS X ISO/IEC 19790의 **부속서** D에 목록으로 제공한다.

[벤더 요구사항]

VE09.09.01
벤더는 ① 검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP 모두에 대한 목록과 상세한 사용법을 제공해야 한다.

VE09.09.02
벤더는 ① 검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP 모두가 검증대상 SSP 생성 방법에 따라 생성됨을 입증하는 개발 문서를 제공해야 한다.

[시험 절차]

TE09.09.01
시험자는 ① 검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP가 모두 문서화되어 있고 사용법이 정의되어 있는지 확인해야 한다.

TE09.09.02
시험자는 ①검증대상 난수 발생기를 이용하여 모듈에서 생성되거나 ② 모듈에 주입된 다른 SSP로부터 유도된 것으로 검증대상 암호알고리즘 또는 SSP 설정에 사용되는 SSP가 구현될 때 KS X ISO/IEC 19790의 **부속서** D에 정의된 검증대상 SSP 생성 방법을 준수하였는지 개발 문서에서 확인해야 한다.

6.9.4 중요 보안매개변수 설정

비고 중요 설정이란 ① 자동화된 SSP 전송이나 SSP 합의 방법, ② 수동 SSP 주입/출력이 직접 또는 전자적 방법을 통하여 이루어짐을 의미한다.

AS09.10: (중요 보안매개변수 생성 – 보안수준 1, 2, 3, 4)

자동화된 SSP 설정은 KS X ISO/IEC 19790의 **부속서** D에 검증대상으로 정의된 방법을 사용해야 한다.

비고 검증대상으로 정의된 중요 보안매개변수 설정 방법은 KS X ISO/IEC 19790의 **부속서** D에서 목록으로 제공된다.

[벤더 요구사항]

VE09.10.01
벤더는 암호모듈에 사용된 모든 자동화된 SSP 설정 방법을 목록으로 제시하고, 그 정확한 사용법을 제공해야 한다.

[시험 절차]

TE09.10.01
시험자는 모든 자동화된 SSP 설정 방법이 문서화되고 사용법이 정의되어 있는지 확인해야 한다.

TE09.10.02
시험자는 구현된 SSP 설정 방법이 KS X ISO/IEC 19790의 **부속서** D에 검증대상으로 정의된 중요 보안매개변수 설정 방법을 준수하는지 개발 문서에서 확인해야 한다.

AS09.11: (중요 보안매개변수 생성 – 보안수준 1, 2, 3, 4)

SSP의 수동 설정은 {KS X ISO/IEC 19790} **7.9.5**의 요구사항을 충족해야 한다.

비고 해당 시험 항목은 **AS09.12** ~ **AS09.24**의 일부분으로 시험된다.

6.9.5 중요 보안매개변수의 주입과 출력

비고 중요 보안매개변수는 수동으로 모듈에 주입되거나 외부로 출력되는 경우 ① 직접적으로(예: 키보드, 숫자 패드, 화면 출력) 또는 ② 전자식으로(예: 스마트카드, 토큰, PC카드, 전자식 키 저장 장치, 모듈의 운영체제) 수행된다.

AS09.12: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

SSP가 수동으로 모듈에 주입되거나 외부로 출력되는 경우 주입 또는 출력은 HMI, SFMI, HFMI 또는 HSMI(KS X ISO/IEC 19790의 **7.3.2**) 인터페이스를 사용해야 한다.

비고 해당 시험 항목은 **AS03.04**～**AS03.14**의 일부분으로 시험된다.

AS09.13: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

SSP가 모듈에 주입되거나 모듈 외부로 출력되는 경우 암호를 사용하여 보호되는 모든 SSP는 검증대상 암호알고리즘을 이용하여 암호화되어야 한다.

[벤더 요구사항]

VE09.13.01
벤더는 모듈에 주입되거나 외부로 출력되는 경우, 암호를 사용하여 보호되는 모든 SSP를 개발 문서에 명세해야 한다.

VE09.13.02
SSP가 모듈에 주입되거나 외부로 출력되는 경우, 암호를 사용하여 SSP를 보호한다면 사용된 암호화 방법을 개발 문서에 서술해야 한다.

[시험 절차]

TE09.13.01
시험자는 모듈에 주입되거나 외부로 출력되는 경우, 암호를 사용하여 보호되는 모든 SSP가 개발 문서에 명세되어 있는지 확인해야 한다.

TE09.13.02
시험자는 SSP가 모듈에 주입되거나 외부로 출력되는 경우, 암호를 사용하여 SSP를 보호하는 암호화 방법이 개발 문서에 명세되어 있는지 확인해야 한다.

TE09.13.03
시험자는 SSP가 모듈에 주입되거나 외부로 출력되는 경우, 암호를 사용하여 SSP를 보호한다면 검증대상 암호알고리즘이 사용되었는지 확인해야 한다.

비고 SSP를 직접 주입하는 경우, 육안 검사로 정확도를 높이기 위해 일시적으로 입력값을 화면에 나타나게 할 수 있다.

AS09.14: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

암호화된 SSP가 직접 모듈에 주입되는 경우, SSP가 평문으로 표시되지 않아야 한다.

[벤더 요구사항]

VE09.14.01
개발 문서에 서술된 암호화된 SSP에 대한 주입 메커니즘은 SSP를 평문으로 표시하지 않아야 한다.

[시험 절차]

TE09.14.01
시험자는 암호화된 SSP의 주입 메커니즘 문서를 검증하여 암호화된 SSP의 주입 과정에서 평문이 표시되지 않는지 확인해야 한다.

TE09.14.02
시험자는 모든 암호화된 SSP를 주입해 보고, 암호모듈의 출력 인터페이스를 통하여 평문에 대한 어떤 정보도 표시되지 않음을 확인해야 한다.

AS09.15: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

직접 주입되는 (평문이거나 암호화된) SSP는 암호모듈에 주입되는 동안 KS X ISO/IEC 19790의 **7.10.3.5**에 정의된 조건부 수동 주입 시험을 이용하여 정확한 주입 여부가 확인되어야 한다.

비고 해당 시험 항목은 **AS10.42**～**AS10.46**의 일부분으로 시험된다.

AS09.16: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

중요 정보를 의도치 않게 출력하는 것을 방지하기 위하여, CSP가 평문으로 출력되는 경우 두 개의 독립된 내부 조치가 있어야 한다.

[벤더 요구사항]

VE09.16.01
암호모듈이 CSP를 평문으로 출력한다면 출력 서비스를 개발 문서에 서술해야 한다.

VE09.16.02
CSP가 평문으로 출력되는 경우 두 개의 독립된 내부 조치를 유한 상태 모델 및 다른 개발 문서에 명시해야 한다.

[시험 절차]

TE09.16.01
시험자는 암호모듈이 CSP를 평문으로 출력할 수 있는지 개발 문서 또는 유한 상태 모델을 확인해야 한다.

TE09.16.02
시험자는 암호모듈이 CSP를 평문으로 출력하기 위해서는 두 개의 독립된 내부 조치가 필요함을 개발 문서 또는 유한 상태 모델에서 확인해야 한다.

TE09.16.03
시험자는 두 개의 독립된 내부 조치를 수행하지 않고 CSP를 평문으로 출력하려는 시도를 해야 한다. 이때 암호모듈이 CSP를 평문으로 출력한다면 해당 시험 항목은 실패한 것으로 판정된다.

AS09.17: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

위에서 정의된 두 개의 독립된 내부 조치는 CSP 출력 설정에만 전용으로 사용되어야 한다.

비고 해당 시험 항목은 독립적으로 시험되지 않으며 **AS09.16**의 일부분으로 시험된다.

AS09.18: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2, 3, 4)

무선 접속을 통한 전자식 주입 또는 출력의 경우, CSP, 키 구성 요소 및 인증 데이터는 암호화되어야 한다.

[벤더 요구사항]

VE09.18.01
암호모듈이 CSP, 키 구성 요소 및 인증 데이터를 무선 인터페이스를 통해 입출력한다면, 무선 서비스를 개발 문서에 서술해야 한다.

VE09.18.02
암호모듈이 CSP, 키 구성 요소 및 인증 데이터를 무선 인터페이스를 통해 입출력한다면, CSP, 키 구성 요소 및 인증 데이터를 암호화하는 데 사용한 방법을 개발 문서에 서술해야 한다.

[시험 절차]

TE09.18.01
시험자는 암호모듈이 CSP, 키 요소 및 인증 데이터를 무선 인터페이스를 통해 입출력하는지 확인해야 한다.

TE09.18.02
시험자는 CSP, 키 요소 및 인증 데이터를 암호화하는 방법이 검증대상 암호화 방식인지 확인해야 한다.

비고 보안수준 1, 2에서, 평문으로 된 ① CSP ② 키 구성 요소 및 ③ 인증 데이터는 다른 용도와 공동으로 사용되는 암호모듈의 물리적 포트 또는 논리적 인터페이스를 통해 입출력될 수 있다.

AS09.19: (중요 보안매개변수의 주입과 출력 – 보안수준 1, 2)

소프트웨어 암호모듈 또는 하이브리드 소프트웨어 모듈의 소프트웨어 구성 요소의 경우, CSP, 키 요소 및 인증 데이터가 운영환경 내에서 관리되고, KS X ISO/IEC 19790의 **7.6.3**의 요구사항을 충족한다면 평문이거나 암호화된 형식으로 입출력될 수 있다.

[벤더 요구사항]

VE09.19.01
벤더는 소프트웨어 암호모듈 또는 하이브리드 소프트웨어 모듈의 소프트웨어 구성 요소에 대하여, CSP, 키 요소, 인증 데이터가 운영환경 내에서 관리되고, KS X ISO/IEC 19790의 **7.6.3**의 요구사항(**AS06.05**～**AS06.29**의 해당 부분)을 충족한다면, 평문이거나 암호화된 형식으로 입출력됨을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE09.19.01
소프트웨어 암호모듈 또는 하이브리드 소프트웨어 모듈의 소프트웨어 구성 요소에 대하여, 시험자는

CSP, 키 요소 및 인증 데이터가 운영환경 내에서 관리되고, KS X ISO/IEC 19790의 **7.6.3**의 요구사항 (**AS06.05**～**AS06.29**의 해당 부분)을 충족한다면, 개발 문서를 통해 CSP, 키 요소 및 인증 데이터가 평문이거나 암호화된 형식으로 입출력되는 것을 확인해야 한다.

AS09.20: (중요 보안매개변수의 주입과 출력 – 보안수준 3, 4)

CSP, 키 요소 및 인증 데이터가 암호모듈에 주입되거나 외부로 출력될 때 암호화되거나 신뢰 채널을 통해야 한다.

비고 해당 시험 항목은 **AS09.13** 또는 **AS03.16**～**AS03.22**의 일부분으로 시험된다.

AS09.21: (중요 보안매개변수의 주입과 출력 – 보안수준 3, 4)

평문으로 된 비밀 정보 CSP와 개인키는 암호모듈에 주입되거나 외부로 출력될 때 지식 분산 기법 또는 신뢰 채널을 이용해야 한다.

[벤더 요구사항]

VE09.21.01
평문으로 된 비밀 정보와 개인키를 암호모듈에 입출력하기 위해 사용한 지식 분산 기법을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.21.01
시험자는 신뢰 채널을 통해 평문으로 된 비밀인 개인키를 입·출력하는 데 사용된 지식 분산 기법을 개발 문서에서 명세하고 있는지 확인해야 한다. 개발 문서에 명세된 지식 분산 기법이 구현 결과와 일치하는지 확인해야 한다.

TE09.21.02
시험자는 지식 분산 기법이 키를 여러 구성 요소로 분산하며, 각각의 키 구성 요소는 원본 키에 대한 어떤 정보도 갖고 있지 않음을 확인해야 한다.

TE09.21.03
시험자는 키를 입출력하기 위하여 분산된 정보의 일부분 또는 전체가 필요함을 확인해야 한다.

TE09.21.04
시험자는 신뢰 채널이 보안수준 3의 경우 **AS03.16**～**AS03.21**을, 보안수준 4의 경우 **AS03.22**를 만족함을 확인해야 한다.

AS09.22: (중요 보안매개변수의 주입과 출력 – 보안수준 3)

암호모듈이 지식 분산 기법을 사용한다면, 각 키 구성 요소의 입력과 출력을 위해 개별적인 신원 기반 운영자 인증을 채택해야 한다. {또한, 원본 암호키를 재구성하기 위해서는 적어도 두 개의 키 구성 요소가 요구되어야 한다.}

[벤더 요구사항]

VE09.22.01
분산된 각각의 키 구성 요소에 대하여 신원 기반 인증을 채택하고 있음을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.22.01
시험자는 각각의 개별 키 구성 요소에 대하여 신원 기반 인증을 채택하고 있음을 확인해야 한다.

AS09.23: (중요 보안매개변수의 주입과 출력 – 보안수준 3)

{암호모듈이 지식 분산 기법을 사용한다면, 키 구성 요소의 입력과 출력을 위해 개별적인 신원 기반 운영자 인증을 채택해야 하며,} 원본 암호키를 재구성하기 위해서는 적어도 두 개 이상의 키 구성 요소가 요구되어야 한다.

[벤더 요구사항]

VE09.23.01
원본 CSP를 구성하기 위해 필요한 구성 요소의 개수를 개발 문서에 명세해야 한다.

[시험 절차]

TE09.23.01
시험자는 원본 CSP를 구성하기 위해서는 지식 분산 기법이 적어도 두 개 이상의 구성 요소를 요구하는지 개발 문서에서 확인해야 한다.

TE09.23.02
시험자는 개발 문서를 통해 지식 분산 기법에 따라 CSP를 출력한 결과가 단일 구성 요소로 출력한 것과 동일하지 않음을 확인해야 한다. 여기서 단일 구성 요소는 원본 CSP를 구성할 수 있다.

AS09.24: (중요 보안매개변수의 주입과 출력 – 보안수준 4)

암호모듈은 키 구성 요소를 입출력할 때, 각 키 구성 요소에 대해 개별적으로 운영자에 대해 다중체계 신원 기반 인증을 해야 한다.

[벤더 요구사항]

VE09.24.01
분산된 키 구성 요소 각각에 대해 다중체계 신원 기반 인증을 채택하였다는 내용을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.24.01
시험자는 분산된 키 구성 요소 각각에 대하여 다중체계 신원 기반 인증을 채택하는지 확인해야 한다.

TE09.24.02
시험자는 다중체계 인증 방법이 **AS04.59**를 충족하는지 확인해야 한다.

6.9.6 중요 보안매개변수의 저장

AS09.25: (중요 보안매개변수의 저장 – 보안수준 1, 2, 3, 4)

암호모듈 내부에 저장되는 모든 SSP는 SSP를 지정한 개체(예: 운영자, 역할, 프로세스)와 연계되어

야 한다.

[벤더 요구사항]

VE09.25.01
모든 키가 올바른 개체와 연계됨을 확인할 수 있는 메커니즘과 절차가 개발 문서의 키 저장 부분에 서술되어야 한다.

[시험 절차]

TE09.25.01
시험자는 저장된 키를 올바른 개체와 연계시키는 방법을 개발 문서의 키 저장 부분에서 확인해야 한다.

TE09.25.02
시험자는 키와 개체의 연계를 변경한다. 시험자는 변경된 개체의 자격으로 암호 기능 수행을 시도하고 암호 기능 수행이 실패함을 확인한다.

AS09.26: (중요 보안매개변수의 저장 – 보안수준 1, 2, 3, 4)

인가되지 않은 운영자가 평문 CSP에 접근하는 것은 금지되어야 한다.

비고 해당 시험 항목은 **AS09.01**에서 시험된다.

AS09.27: (중요 보안매개변수의 저장 – 보안수준 1, 2, 3, 4)

인가되지 않은 운영자에 의한 PSP 변경은 금지되어야 한다.

[벤더 요구사항]

VE09.27.01
벤더는 인가되지 않은 운영자에 의한 PSP 변경 금지를 명세한 개발 문서로 제출해야 한다.

[시험 절차]

TE09.27.01
시험자는 벤더가 인가되지 않은 운영자에 의한 PSP 변경 금지를 명세한 개발 문서를 제출하는지 확인해야 한다.

TE09.27.02
시험자는 인가되지 않은 역할을 가정하고 암호모듈에 저장된 PSP를 변경을 시도해야 한다. 시도가 실패하면 해당 시험 절차는 충족된다.

6.9.7 중요 보안매개변수의 제로화

AS09.28: (중요 보안매개변수의 제로화 – 보안수준 1, 2, 3, 4)

암호모듈 내부에서 보호되지 않은 모든 SSP와 키 구성 요소를 제로화하는 방법을 제공해야 한다.

비고 1 해당 시험 항목은 **AS09.30**에서 시험된다.
비고 2 일시적으로 저장된 SSP와 암호모듈에 속하는 다른 저장값은 더 이상 필요하지 않은 경우

제로화되어야 한다.

AS09.29: (중요 보안매개변수의 제로화－보안수준 1, 2, 3, 4)

제로화된 SSP는 복구되거나 재사용될 수 없어야 한다.

[벤더 요구사항]

VE09.29.01
제로화된 SSP를 복구하거나 재사용할 수 없도록 하는 방법이 개발 문서에 명세되어야 한다.

[시험 절차]

TE09.29.01
시험자는 제로화된 SSP를 복구하거나 재사용할 수 없도록 하는 방법이 개발 문서에 명세되어 있는지 확인해야 한다.

TE09.29.02
시험자는 벤더가 제공한 근거가 정확한지 검증해야 한다. 입증의 책임은 벤더에 있다. 부정확하거나 모호한 점이 있으면 시험자는 필요에 따라 벤더에게 추가적인 정보를 요구할 수 있다.

비고 1 ① 보호된 PSP, ② 암호화된 CSP 또는 ③ 암호모듈에 별도로 탑재된 (해당 표준의 요구사항을 만족하는) 검증필 암호모듈 내부에서 물리적 또는 논리적으로 보호된 CSP의 제로화는 요구되지 않는다.

비고 2 SSP가 인증 프록시인 프로세스에 평문을 전달하기 위해서만 사용된다면(예: 암호모듈의 초기화 키인 CSP) 제로화 요구사항을 충족할 필요가 없다.

AS09.30: (중요 보안매개변수의 제로화－보안수준 2, 3, 4)

암호모듈은 보호되지 않는 SSP의 제로화를 수행해야 한다(예: 모두 0 또는 1로 덮어 쓰거나 난수로 채우기).

[벤더 요구사항]

VE09.30.01
개발 문서에 다음 SSP의 제로화에 대한 정보를 명세해야 한다.

a) 제로화 기법
b) 평문 SSP가 제로화될 수 있는 조건
c) 제로화되는 평문 SSP
d) 제로화되지 않는 평문 SSP와 근거
e) 제로화 기법이 평문 SSP가 노출되는 데 걸리는 시간 이내에 수행될 수 있음을 설명하는 근거

[시험 절차]

TE09.30.01
시험자는 개발 문서에 VE09.30.01에 명세된 정보가 포함되어 있는지 확인해야 한다. 시험자는 벤더가 제공한 근거가 정확한지 검증해야 한다. 입증 책임은 벤더에 있다. 부정확하거나 모호한 점이 있으면 시험자는 필요에 따라 벤더에게 추가적인 정보를 요구할 수 있다.

TE09.30.02
시험자는 현재 어떤 키가 모듈에 있는지 확인하고 제로화 명령을 시작한다. 초기화 명령 수행을 완료한 후 시험자는 모듈에 저장되어 있었던 평문 SSP를 이용한 암호 연산을 시도하고, 평문 SSP에 접근할 수 없음을 확인해야 한다.

TE09.30.03
시험자는 제로화를 시작한 후 평문 SSP가 손상(노출)되기 전에 키가 파기됨을 확인해야 한다.

TE09.30.04
시험자는 제로화 명령에 의해 제로화되지 않는 평문 SSP는 ① 검증대상 알고리즘으로 암호화되거나 ② 암호모듈에 별도로 탑재된 (해당 KS X ISO/IEC 19790을 준수하는) 검증필 암호모듈 내에서 물리적 또는 논리적으로 보호됨을 확인해야 한다.

AS09.31: (중요 보안매개변수의 제로화 – 보안수준 2, 3, 4)

제로화 수행 시 보호되지 않은 SSP를 보호되지 않은 다른 SSP로 덮어쓰는 것을 방지해야 한다.

[벤더 요구사항]

VE09.31.01
제로화 수행 시 보호되지 않은 SSP를 보호되지 않은 다른 SSP로 덮어쓰는 경우가 없음을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.31.01
시험자는 제로화 수행 시 보호되지 않은 SSP를 보호되지 않은 다른 SSP로 덮어쓰는 경우가 없음을 개발 문서로 제공하는지 확인해야 한다.

AS09.32: (중요 보안매개변수의 제로화 – 보안수준 2, 3, 4)

일시적으로 사용되는 SSP는 더 이상 필요하지 않게 되면 제로화되어야 한다.

[벤더 요구사항]

VE09.32.01
일시적으로 사용되는 SSP가 더 이상 필요하지 않게 되면 제로화됨을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.32.01
시험자는 일시적으로 사용되는 SSP가 더 이상 필요하지 않게 되면 제로화됨을 개발 문서에 명세했는지 확인해야 한다.

AS09.33: (중요 보안매개변수의 제로화 – 보안수준 2, 3, 4)

암호모듈은 제로화가 완료되었을 때 상태 표시를 출력해야 한다.

[벤더 요구사항]

VE09.33.01
암호모듈이 제로화가 완료될 때 **{AS03.11}**에 정의된 상태 표시를 출력함을 개발 문서에 명세해야 한다.

[시험 절차]

TE09.33.01
시험자는 개발 문서를 통해 암호모듈이 제로화가 완료될 때 상태 표시를 출력함을 확인해야 한다.

TE09.33.02
시험자는 제로화를 수행해 보고 상태 표시가 출력되는지 확인해야 한다.

AS09.34: (중요 보안매개변수의 제로화 – 보안수준 4)

다음 요구사항 {KS X ISO/IEC 19790, **AS09.35**～**AS09.37**}이 충족되어야 한다.

비고 해당 시험 항목은 **AS09.35**～**AS09.37**의 일부분으로 시험된다.

AS09.35: (중요 보안매개변수의 제로화 – 보안수준 4)

제로화는 즉각적으로, 중단됨 없이 수행되어야 한다. {또한 충분히 짧은 시간에 수행되어 중요 정보가 제로화의 시작과 종료 사이에 복구될 수 없도록 해야 하며 **{AS09.37**을 충족해야 한다.}}

비고 해당 시험 항목은 **AS09.36**의 일부분으로 시험된다.

AS09.36: (중요 보안매개변수의 제로화 – 보안수준 4)

{제로화는 즉각적으로, 중단됨 없이 수행되어야 하며} 짧은 시간에 수행되어 중요 정보가 제로화의 시작과 종료 사이에 복구될 수 없도록 해야 하며, **{AS09.37**을 충족해야 한다.}

[벤더 요구사항]

VE09.36.01
암호모듈의 제로화는 즉각적으로, 중단됨 없이 수행되고, 짧은 시간에 수행되어 중요 정보가 제로화의 시작과 종료 사이에 복구될 수 없음이 개발 문서에 기술되어 제공되어야 한다.

[시험 절차]

TE09.36.01
시험자는 암호모듈의 제로화는 즉각적으로 중단됨 없이 수행되고, 짧은 시간에 수행되어 중요 정보가 제로화의 시작과 종료 사이에 복구될 수 없음을 개발 문서로 제공했는지 확인해야 한다.

TE09.36.02
시험자는 암호모듈의 제로화를 수행해야 한다. 제로화의 일부분 또는 전체의 진행을 중단할 수 있는지 시도해야 한다. 진행을 중단할 수 있으면 해당 시험 항목은 실패한 것으로 판정된다.

AS09.37: (중요 보안매개변수의 제로화 – 보안수준 4)

평문이든 암호화되어 있든, 모든 SSP는 제로화되면 공장 출하 상태로 회귀되어야 한다.

[벤더 요구사항]

VE09.37.01
평문이든 암호화되어 있든, 보호되지 않는 모든 SSP는 제로화되면 공장 출하 상태로 회귀됨을 개발 문서에 기술해 제공해야 한다.

[시험 절차]

TE09.37.01
시험자는 평문이든 암호화되어 있든, 보호되지 않는 모든 SSP가 제로화되면 공장 출하 상태로 회귀됨을 개발 문서에 기술해 제공하는지 확인해야 한다.

TE09.37.02
시험자는 암호모듈의 제로화를 수행하여 모듈이 공장 출하 상태로 회귀됨을 확인해야 한다.

6.10 자가시험

6.10.1 자가시험 일반 요구사항

AS10.1 (자가시험 – 보안수준 1, 2, 3, 4)

자가시험이 수행되어야 한다. {또한 성공 또는 실패 판정이 암호모듈에 의해서만 결정되며, 외부의 제어, 외부로부터 제공되는 테스트 벡터, 예상 출력값, 운영자의 관여 또는 모듈이 검증대상 동작모드에 있는지 비검증대상 동작모드에 있는지 여부와 무관하게 수행되어야 한다.}

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.02: (자가시험 – 보안수준 1, 2, 3, 4)

{자가시험이 수행되어야 하며} 성공 또는 실패의 판정이 암호모듈에 의해서만 결정되며, 외부의 제어, 외부로부터 제공되는 테스트 벡터, 예상 출력값, 운영자의 관여 또는 모듈이 검증대상 동작모드에 있는지 비검증대상 동작모드에 있는지 여부와 무관하게 수행되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.03: (자가시험 – 보안수준 1, 2, 3, 4)

암호모듈이 출력 인터페이스를 통해 데이터를 출력되기 이전에, 암호모듈이 동작 전 자가시험을 수행해야 하며 수행 결과가 성공해야 한다.

비고 해당 시험 항목은 **AS10.15**에서 시험된다.

AS10.04: (자가시험 – 보안수준 1, 2, 3, 4)

적용되는 암호알고리즘이나 프로세스가 호출될 때, 조건부 자가시험이 수행되어야 한다(즉, 사용되는 암호알고리즘에 대해 자가시험이 요구된다).

비고 1 해당 시험 항목은 **AS10.25**에서 시험된다.
비고 2 암호모듈은 KS X ISO/IEC 19790에 정의된 시험 외에 추가적으로 다른 전원 인가 또는 조건부 자가시험을 수행할 수 있다.

AS10.05: (자가시험 – 보안수준 1, 2, 3, 4)

알고리즘 표준(KS X ISO/IEC 19790의 **부속서** C～E)에 대해 적용되는 모든 자가시험은 암호모듈 자체 내에서 구현될 수 있어야 한다.

비고 해당 시험 항목은 **AS10.26**에서 시험된다.

AS10.06: (자가시험 – 보안수준 1, 2, 3, 4)

검증대상 암호알고리즘, SSP 설정 방법, 인증 메커니즘에 대하여 알고리즘 표준(KS X ISO/IEC 19790의 **부속서** C～E)에 대한 자가시험은 표준(KS X ISO/IEC 19790의 **부속서** C～E)에 명세된 방법에 따라 구현되어야 한다.

비고 해당 시험 항목은 **AS10.26**에서 시험된다.

AS10.07: (자가시험 – 보안수준 1, 2, 3, 4)

암호모듈이 자가시험에 실패한다면 오류 상태로 전환되어야 한다. {그리고 KS X ISO/IEC 19790의 **7.3.3**에 명세된 방식으로 오류 표시를 출력해야 한다.}

[벤더 요구사항]

VE10.07.01
오류 발생 조건 각각에 대하여, 오류 조건의 명칭, 설명, 오류 조건을 발생시킬 수 있는 이벤트 및 오류 조건을 해제시키고 정상 동작을 다시 가동하기 위해 필요한 행위를 개발 문서에 서술해야 한다.

[시험 절차]

TE10.07.01
시험자는 다음 항목들을 포함한 자가시험 목록을 확인해야 한다.

a) 동작 전 자가시험
   1) 동작 전 소프트웨어/펌웨어 무결성 시험
   2) 동작 전 우회 기능 시험
   3) 동작 전 핵심 기능 시험

b) 조건부 자가시험
   1) 조건부 암호알고리즘 시험
   2) 조건부 암호키 쌍 일치 시험
   3) 조건부 소프트웨어/펌웨어 로드 시험
   4) 조건부 수동 주입 시험
   5) 조건부 우회 기능 시험
   6) 조건부 핵심 기능 시험

TE10.07.02
시험자는 각각의 오류 조건에 대하여 위의 정보가 명세되어 있는지 조사한다.

TE10.07.03
시험자는 각각의 오류를 유발하여 오류 조건이 해제되도록 시도해야 한다. 시험자는 오류 상태를 해

제하는 데 필요한 행위가 개발 문서와 부합하는지 확인해야 한다. 시험자가 각 오류 조건을 만들 수 없다면, 소스 코드와 설계 문서를 검토하는 방법으로 오류 상태를 해제하는 데 필요한 행위가 개발 문서와 부합하는지 확인해야 한다.

TE10.07.04
시험자는 암호모듈이 검증대상 동작모드로 운영되는지 비검증대상 동작모드로 운영되는지에 무관하게 모든 자가시험이 수행됨을 확인해야 한다.

TE10.07.05
시험자는 검사와 개발 문서 점검을 통하여 각각의 자가시험에 대한 성공 또는 실패의 판정이 암호모듈에 의해서만 결정되며, 외부의 제어, 외부로부터 제공되는 테스트 벡터, 예상 출력값, 운영자의 관여 또는 모듈이 검증대상 동작모드에 있는지 비검증대상 동작모드에 있는지 여부와 무관하게 수행되는지 확인해야 한다.

AS10.08: (자가시험 – 보안수준 1, 2, 3, 4)

{암호모듈이 자가시험에 실패한다면 오류 상태로 진입하며} KS X ISO/IEC 19790의 **7.3.3**에 명세된 방식으로 오류 표시를 출력해야 한다.

[벤더 요구사항]

VE10.08.01
벤더는 개발 문서에 각 자가시험에 따른 모든 오류 상태를 명세하고 각 오류 상태에 대한 오류 표시를 명세해야 한다.

[시험 절차]

TE10.08.01
시험자는 개발 문서를 검토하여 자가시험이 실패하는 경우 진입하는 모든 오류 상태의 목록과 각각의 오류 상태와 관련된 오류 표시가 제공됨을 확인해야 한다. 시험자는 오류 상태 목록이 유한 상태 모델(**AS11.10** 참조)에 정의된 것과 일치하는지 비교해야 한다.

TE10.08.02
시험자는 개발 문서에서 자가시험이 오류를 처리하는 방법을 검토하여 다음을 확인해야 한다.

a) 자가시험이 실패하는 경우 암호모듈이 오류 상태에 진입하는가?
b) 오류 상태가 개발 문서 및 유한 상태 모델과 일치하는가?
c) 암호모듈이 오류 표시를 출력하는가?
d) 오류 표시가 개발 문서에 서술된 것과 일치하는가?

TE10.08.03
시험자는 각각의 자가시험을 실행하여 암호모듈이 오류 상태에 진입하도록 한다. 관찰되는 오류 표시를 개발 문서의 명세와 비교하여 일치하지 않으면 해당 시험 항목은 실패로 판정된다.

AS10.09: (자가시험 – 보안수준 1, 2, 3, 4)

암호모듈이 오류 상태에서 암호 연산을 수행하지 않아야 하고 제어 출력 인터페이스와 데이터 출력 인터페이스를 통한 제어 출력 및 데이터 출력을 수행하지 않아야 한다.

[벤더 요구사항]

VE10.09.01
개발 문서는 VE03.07.01, VE03.07.02, VE03.10.01, VE03.10.02에 따라 명세되어야 한다. 벤더의 설계 문서는 암호모듈의 오류 상태에서 어떠한 암호 연산도 수행할 수 없음을 보증해야 한다.

[시험 절차]

TE10.09.01
시험자는 TE03.07.01, TE03.07.02, TE03.10.01, TE03.10.02에 따라 제어 출력과 데이터 출력이 금지됨을 확인해야 한다. 다음과 같은 결과를 확인해야 한다.

a) 암호모듈의 오류 상태에서 제어 출력 인터페이스와 데이터 출력 인터페이스를 통해 모든 제어 출력 및 데이터 출력이 금지됨을 개발 문서가 보여야 한다.
b) 암호모듈의 오류 상태에서 모든 제어 출력과 데이터 출력이 금지된다.

TE10.09.02
시험자는 암호모듈이 오류 상태에 있을 때 암호 기능이 금지됨을 개발 문서에 명세하고 있는지 확인해야 한다.

TE10.09.03
시험자는 암호모듈을 오류 상태에 진입시키고, 시도하는 어떤 암호 기능도 수행되지 않음을 확인해야 한다.

AS10.10: (자가시험 – 보안수준 1, 2, 3, 4)

암호모듈은 함수 또는 알고리즘과 관련된 자가시험이 반복 수행되어 성공적으로 통과될 때까지 자가시험이 실패한 함수와 알고리즘에 관련된 어떠한 기능도 사용하지 않아야 한다.

[벤더 요구사항]

VE10.10.1
벤더는 함수 또는 알고리즘과 관련된 자가시험이 반복 수행되어 성공적으로 통과될 때까지 암호모듈은 자가시험이 실패한 함수와 알고리즘에 관련된 어떠한 기능도 사용하고 있지 않음을 서술하는 개발 문서를 제출해야 한다.

[시험 절차]

TE10.10.01
시험자는 함수 및 알고리즘에 대한 자가시험을 실패시키는 오류를 유발하고 이 함수 또는 알고리즘을 사용하는 기능을 시작한 후 암호모듈이 이 기능을 사용할 수 없음을 확인해야 한다.

TE10.10.02
시험자는 각각의 자가시험을 수행하여 암호모듈이 각 오류 상태 또는 안전한 복구 동작 상태로 진입하도록 해야 한다. 시험자는 암호모듈을 운영하여 함수 또는 알고리즘과 관련된 자가시험이 반복 수행되어 성공적으로 통과될 때까지는 해당 함수와 알고리즘에 관련된 기능이 활용될 수 없음을 확인해야 한다.

AS10.11: (자가시험 – 보안수준 1, 2, 3, 4)

암호모듈이 자가시험 실패에 대하여 오류 상태를 출력하지 않는다면, 모듈이 오류 상태에 진입했는지를 암시적으로 보안정책 문서(KS X ISO/IEC 19790의 **부속서** B)에 서술된 명백한 절차를 통해 결정할 수 있어야 한다.

[벤더 요구사항]

VE10.11.01
벤더는 암호모듈이 자가시험 실패에 대하여 오류 상태를 출력하지 않는다면, 암호모듈이 오류 상태에 진입했는지를 결정할 수 있는 명백한 절차를 명세한 보안정책 문서를 제출해야 한다.

[시험 절차]

TE10.11.01
시험자는 각각의 자가시험을 실행하여 암호모듈이 모든 오류 상태에 진입하게 해야 한다. 시험자는 암호모듈이 보안정책 문서에 서술된 절차를 통해 암시적으로 오류 상태에 진입했음을 확인해야 한다.

AS10.12: (자가시험 – 보안수준 3, 4)

암호모듈은 인가된 운영자만 접근할 수 있는 오류 로그를 관리해야 한다.

[벤더 요구사항]

VE10.12.01
오류 로그에 기록되는 정보의 유형(예: 실패한 자가시험의 종류, 오류가 발생한 시점)을 포함한 오류 로그 기능을 개발 문서에 명세해야 한다.

VE10.12.02
오류 로그의 무결성을 유지하는 메커니즘에 대하여 개발 문서에 서술해야 한다.

[시험 절차]

TE10.12.01
시험자는 개발 문서를 검토하여 인가되지 않은 운영자는 오류 로그에 접근할 수 없음을 확인해야 한다.

TE10.12.02
시험자는 개발 문서를 검토하여 오류 로그 기능이 최소한 가장 최근에 발생한 오류 이벤트에 대한 정보를 제공하는지 확인해야 한다.

비고 해당 시험 항목은 **AS10.13**을 충족한다.

TE10.12.03
시험자는 암호모듈이 오류 상태에 진입하도록 하여 모듈이 적어도 가장 최근에 발생한 오류 이벤트에 대한 오류 로그를 생성하는지 확인해야 한다.

TE10.12.04
시험자는 암호모듈이 지원하는 인가된 역할을 부여받지 않고 오류 로그에 접근을 시도한다. 만일 오류 로그에 접근할 수 있으면 해당 시험 항목은 실패로 판정된다.

TE10.12.05
시험자는 암호모듈을 동작시켜 오류 로그가 인가되지 않은 변경이나 인가되지 않은 대체로부터 보호되는지 확인해야 한다.

AS10.13: (자가시험 – 보안수준 3, 4)

오류 로그는 적어도 가장 최근에 발생한 오류 이벤트에 대한 정보(예: 실패한 자가시험의 종류)를 제공해야 한다.

비고 해당 시험 항목은 **AS10.12**의 일부분으로 시험된다.

AS10.14: (자가시험 – 보안수준 1, 2, 3, 4)

KS X ISO/IEC 19790의 **A.2.10** 요구사항을 충족한 개발 문서가 제출되어야 한다.

비고 해당 시험 항목은 **ASA.01**의 일부분으로 시험된다.

6.10.2 동작 전 자가시험

6.10.2.1 동작 전 자가시험의 일반 요구사항

AS10.15: (동작 전 자가시험 – 보안수준 1, 2, 3, 4)

암호모듈에 전원이 인가되는 시점 또는 (전원 꺼짐, 리셋, 리부팅, 콜드-스타트, 전원 인터럽트 등이 발생한 후) 인스턴스화되는 시점과 암호모듈이 동작 상태로 천이되기 직전 시점 사이에 암호모듈에 의해 동작 전 시험이 수행되고 성공적으로 시험을 통과해야 한다.

[벤더 요구사항]

VE10.15.01
벤더는 각각의 동작 전 자가시험에 대한 정보를 명세한 개발 문서를 제출해야 한다.

VE10.15.02
암호모듈의 전원이 인가되는 시점 또는 인스턴스화되는 시점과 동작 상태로 천이되기 직전 시점 사이에서 수행되는 동작 전 자가시험의 절차를 제공해야 한다.

[시험 절차]

TE10.15.01
시험자는 각각의 동작 전 자가시험이 개발 문서에 명세되었는지 확인해야 한다. 시험자는 동작 전 자가시험이 개발 문서에 명세된 대로 수행되는지 확인해야 한다.

TE10.15.02
시험자는 소스 코드와 설계 문서를 확인하여 각각의 동작 전 자가시험이 암호모듈의 전원이 인가되는 시점 또는 인스턴스화되는 시점과 동작 상태로 전이되는 시점 사이에 수행되어 성공적으로 통과되는지 확인해야 한다.

AS10.16: (동작 전 자가시험 – 보안수준 1, 2, 3, 4)

암호모듈은 해당하는 경우 다음과 같은 동작 전 자가시험을 수행해야 한다.

- 동작 전 소프트웨어/펌웨어 무결성 시험
- 동작 전 우회 기능 시험
- 동작 전 핵심 기능 시험

비고 해당 시험 항목은 **AS10.17**～**AS10.24**의 일부분으로 시험된다.

6.10.2.2 동작 전 소프트웨어/펌웨어 무결성 시험

AS10.17: (동작 전 소프트웨어/펌웨어 무결성 시험－보안수준 1, 2, 3, 4)

암호 경계 내부의 모든 소프트웨어와 펌웨어 구성 요소는 KS X ISO/IEC 19790의 **7.5**에 정의된 요구사항을 만족하는 검증대상 무결성 검증 기술을 이용하여 검증되어야 한다.

[벤더 요구사항]

VE10.17.01
암호 경계 내부의 모든 소프트웨어와 펌웨어 구성 요소에 대한 무결성을 확인하기 위하여 암호모듈은 검증대상 무결성 검증 기술을 사용하고 있음을 개발 문서에 명세해야 한다.

VE10.17.02
검증대상 무결성 검증 기술이 암호모듈 자체적으로 구현되는지 아니면 검증대상 동작모드에서 동작되는 다른 검증필 암호모듈에 의하여 구현되는지 개발 문서에 명세해야 한다.

VE10.17.03
구현된 무결성 검증 메커니즘이 개발 문서에 서술되어야 한다.

VE10.17.04
벤더는 VE02.20.01에 명세된 바와 같이 구현 적합성 검증을 사전 검토 단계에서 수행할 수 있도록 검증대상 무결성 기술을 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE10.17.01
시험자는 VE02.20.01 및 TE02.20.01에 명세된 바와 같이 사전 검토 단계에서 수행한 검증대상 무결성 검증 기술의 구현 적합성 검증이 성공했는지 확인해야 한다.

TE10.17.02
암호모듈에 소프트웨어/펌웨어 무결성 시험를 위해 해시나 MAC가 구현되어 있다면, 시험자는 개발 문서를 검토하여 해시나 MAC가 계산되고 확인되는 과정을 빠짐없이 서술하고 있는지 확인해야 한다.

TE10.17.03
암호모듈에 소프트웨어/펌웨어 무결성 시험을 위해 검증대상 전자서명이 구현되어 있을 때, 시험자는 개발 문서에 다음 사항이 포함되었는지 확인해야 한다.

a) 구현된 검증대상 전자서명 알고리즘의 명세
b) 검증대상 전자서명에 의해 보호되는 소프트웨어 또는 펌웨어의 식별
c) 소프트웨어 또는 펌웨어에 포함되는 검증대상 전자서명의 사전 계산값 검증 방법
d) 검증대상 전자서명의 검증 방법
e) 검증대상 전자서명 검증 실패에 따른 자가시험 실패

TE10.17.04
암호모듈에 검증대상 무결성 검증 기술이 구현되었을 때, 시험자는 소스 코드와 설계 문서를 검토하여 구현 결과가 TE10.17.01～TE10.17.03과 일치하는지 확인해야 한다.

TE10.17.05
검증대상 무결성 검증 기술이 다른 검증필 암호모듈에 의해 지원되는 경우에도, 시험자는 소프트웨어/펌웨어 무결성 시험의 성공 또는 실패 판정이 **AS10.01**의 명세를 따르는지 확인해야 한다.

TE10.17.06
시험자는 암호모듈의 소프트웨어 구성 요소와 펌웨어 구성 요소를 변경해 본다. 무결성 검증 메커니즘이 소프트웨어 구성 요소와 펌웨어 구성 요소가 변경되었음을 탐지하지 못하면 해당 시험 항목은 실패로 판정된다.

AS10.18: (동작 전 소프트웨어/펌웨어 무결성 시험 – 보안수준 1, 2, 3, 4)

검증이 실패하면 동작 전 소프트웨어/펌웨어 무결성 시험이 실패한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.19: (동작 전 소프트웨어/펌웨어 무결성 시험 – 보안수준 1, 2, 3, 4)

하드웨어 암호모듈이 소프트웨어 또는 펌웨어를 포함하지 않는 경우, 모듈에는 동작 전 자가시험으로 KS X ISO/IEC 19790의 **7.10.3.2**에 따라 적어도 하나의 암호알고리즘 자가시험이 구현되어야 한다.

비고 해당 시험 항목은 독립적으로 시험되지 않는다.

AS10.20: (동작 전 소프트웨어/펌웨어 무결성 시험 – 보안수준 1, 2, 3, 4)

동작 전 소프트웨어/펌웨어 무결성 시험을 위해 사용되는 검증대상 무결성 검증 기술에 사용되는 암호알고리즘은 우선 KS X ISO/IEC 19790의 **7.10.3.2**에 따른 암호알고리즘 자가시험을 통과해야 한다.

[벤더 요구사항]

VE10.20.01
관련된 개발 문서에 대한 요구사항은 VE10.15.02에 명세되어 있다.

[시험 절차]

TE10.20.01
시험자는 소스 코드와 설계 문서를 검토하여, 동작 전 소프트웨어/펌웨어 무결성 시험이 시작되기 전 검증대상 무결성 검증 기술에 사용되는 암호알고리즘 시험이 통과되는지 확인해야 한다.

6.10.2.3 동작 전 우회 기능 시험

AS10.21: (동작 전 우회 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈에 우회 기능이 구현되는 경우, 우회 기능을 활성화하기 위해 필요한 통제 로직이 정확히 동작하는지 보증해야 한다.

[벤더 요구사항]

VE10.21.01
암호모듈이 우회 기능을 활성화하기 위해 필요한 통제 로직의 올바른 동작을 확인하는 방법을 개발 문서에 명세해야 한다.

[시험 절차]

TE10.21.01
시험자는 개발 문서의 검토와 모듈의 검사를 통해 우회 기능을 활성화하기 위해 필요한 통제 로직이 명세된 대로 구현되었는지 확인해야 한다.

TE10.21.02
시험자는 암호모듈 검사와 개발 문서 검토를 통해 우회 기능을 활성화하기 위해 필요한 통제 로직을 수행하는 동작 전 우회 기능 시험이 구현되어 있는지 확인해야 한다.

TE10.21.03
시험자는 동작 전 우회 기능 시험에서 발생할 수 있는 각각의 오류 조건을 유발시킨 후, TE03.07.01～TE03.07.05와 TE03.10.01～TE03.10.05에 따라 출력이 금지되는지 확인해야 한다.

TE10.21.04
시험자는 동작 전 우회 기능 시험을 실행하여, 우회 기능을 활성화하기 위해 필요한 통제 로직과 관련된 어떠한 기능도 TE10.10.01～TE10.10.02에 따라 사용될 수 없음을 확인해야 한다.

AS10.22: (동작 전 우회 기능 시험－보안수준 1, 2, 3, 4)

암호모듈은 다음과 같은 방법에 의해 데이터 경로를 검증해야 한다.

- 우회 기능 스위치가 암호 프로세스를 지원하도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되는지 검증을 수행함.
- 우회 기능 스위치가 암호 프로세스를 지원하지 않도록 설정되는 경우, 암호모듈이 우회 기능을 통하여 전달되는 데이터가 암호에 의해 처리되지 않는지 검증을 수행함.

[벤더 요구사항]

VE10.22.01
암호 처리를 지원하도록 우회 기능 스위치를 설정하는 방법이 개발 문서에 명세되어야 한다.

VE10.22.02
암호 처리를 지원하도록 우회 기능 스위치를 설정하면 데이터 경로를 통해 암호에 의해 처리된 데이터가 강제로 전송되도록 설계된 우회 기능 메커니즘을 개발 문서에 서술해야 한다.

VE10.22.03
암호 처리를 지원하지 않도록 우회 기능 스위치를 설정하는 방법이 개발 문서에 명세되어야 한다.

VE10.22.04
암호 처리를 지원하지 않도록 우회 기능 스위치를 설정하면 데이터 경로를 통해 암호에 의해 처리되지 않은 데이터가 강제로 전송되도록 설계된 우회 기능 메커니즘을 개발 문서에 서술해야 한다.

[시험 절차]

TE10.22.01
시험자는 암호모듈 검사를 통해, 암호 처리를 지원하도록 우회 기능 스위치를 설정하여 우회 기능이 동작하지 않음을 확인해야 한다.

TE10.22.02
시험자는 소스 코드와 개발 문서의 검토를 통해 구현된 우회 기능 메커니즘이 개발 문서와 일치하는지 확인해야 한다.

TE10.22.03
시험자는 소스 코드와 개발 문서의 검토를 통해, 암호 처리를 지원하도록 우회 기능 스위치를 설정하면 데이터 경로를 통해 전송되는 데이터가 암호를 사용하여 처리되는지 검증하는 동작 전 우회 기능 시험을 암호모듈이 수행하는지 확인해야 한다.

TE10.22.04
시험자는 암호모듈 검사를 통해, 암호 처리를 지원하지 않도록 우회 기능 스위치를 설정하여 우회 기능이 동작함을 확인해야 한다.

TE10.22.05
시험자는 소스 코드와 개발 문서의 검토를 통해, 암호 처리를 지원하지 않도록 우회 기능 스위치를 설정하면 데이터 경로를 통해 전송되는 데이터는 암호를 사용하여 처리되지 않음을 검증하는 동작 전 우회 기능 시험을 암호모듈이 수행하는지 확인해야 한다.

6.10.2.4 동작 전 핵심 기능 시험

AS10.23: (동작 전 핵심 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈의 안전한 운영을 위해 동작 전 시험에서 시험해야 하는 핵심적인 보안 기능이 있을 수 있다.

비고 해당 시험 항목은 **AS10.24**의 일부분으로 시험된다.

AS10.24: (동작 전 핵심 기능 시험 – 보안수준 1, 2, 3, 4)

동작 전 시험에 포함되는 핵심 기능에 대하여 개발 문서에 명세해야 한다.

비고 핵심 기능(critical function)은 오류 발생 시 CSP의 노출을 초래할 수 있는 기능으로 정의한다. 핵심 기능의 예로는 난수 발생기, 암호알고리즘의 동작, 암호 우회 기능 등이 있다.

[벤더 요구사항]

VE10.24.01
벤더는 모든 핵심 기능에 대하여 개발 문서를 제출해야 한다. 각각의 핵심 기능에 대하여 다음을 명시해야 한다.

a) 핵심 기능의 목적
b) 동작 전 자가시험에서 시험할 핵심 기능의 종류
c) 조건부 자가시험에서 시험할 핵심 기능의 종류

[시험 절차]

TE10.24.01
시험자는 핵심 기능 및 이를 검증할 수 있도록 설계된 자가시험이 개발 문서에 명세되었는지 확인해야 한다. 문서는 다음을 포함해야 한다.

a) 모든 핵심 기능의 식별 및 설명
b) 각 핵심 기능에 대한 하나 이상의 자가시험 식별

TE10.24.02
시험자는 소스 코드와 설계 문서를 검토하여 암호모듈이 각 핵심 기능에 대하여 자가시험을 수행하는지 확인해야 한다.

6.10.3 조건부 자가시험

6.10.3.1 조건부 자가시험 일반 요구사항

AS10.25: (조건부 자가시험 – 보안수준 1, 2, 3, 4)

다음 시험에 대하여 개발 문서에 명세된 조건이 발생하면, 암호모듈에 의해 조건부 자가시험이 수행되어야 한다.

암호알고리즘 자가시험, 암호키 쌍 일치 시험, 소프트웨어/펌웨어 로드 시험, 수동 주입 시험, 조건부 우회 기능 시험 및 조건부 핵심 기능 시험

[벤더 요구사항]

VE10.25.01
조건부 자가시험에 대한 정보가 개발 문서에 명세되어야 한다.

[시험 절차]

TE10.25.01
시험자는 조건부 자가시험이 개발 문서에 명세되어 있는지 확인해야 한다.

TE10.25.02
시험자는 조건부 자가시험이 명세된 대로 수행되는지 확인해야 한다.

6.10.3.2 조건부 암호알고리즘 자가시험

AS10.26: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

암호알고리즘 시험은 KS X ISO/IEC 19790의 **부속서** C～E에 명세된 목록 중 모듈에 구현된 검증대상 암호알고리즘에 대하여 모든 암호 기능(예: 암호알고리즘, SSP 설정 방법, 인증)이 수행되어야 한다.

비고 해당 시험 항목은 **AS10.27**의 일부분으로 시험된다.

AS10.27: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

암호알고리즘이 최초로 사용되기 이전에 조건부 자가시험이 수행되어야 한다.

[벤더 요구사항]

VE10.27.01
암호알고리즘에 대한 조건부 자가시험이 개발 문서에 명세되어야 한다.

VE10.27.02
각각의 암호알고리즘이 최초로 사용되기 이전에 조건부 자가시험을 수행하는 방법에 대한 근거를 개발 문서에 명세해야 한다.

VE10.27.03
모듈의 암호알고리즘을 시험하기 위하여 기지 답안 시험, 비교 시험 또는 오류 탐지 시험 등이 사용된 시험방법을 명세해야 한다. 비교 시험 또는 오류 탐지 시험 등이 사용된다면 벤더는 이 시험방법에 대한 설명을 제출해야 한다.

[시험 절차]

TE10.27.01
시험자는 모듈의 검사와 개발 문서의 검토를 통하여, 암호모듈은 암호알고리즘이 최초로 사용되기 이전에 조건부 자가시험을 수행하는지 확인해야 한다.

AS10.28: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

시험의 수행으로 계산된 출력값이 이미 알고 있는 정답과 일치하지 않으면 암호알고리즘의 기지 답안 자가시험은 실패로 판정된다.

[벤더 요구사항]

VE10.28.01
시험의 수행으로 계산된 출력값과 이미 알고 있는 정답을 비교하는 데 사용하는 방법을 개발 문서에 명세해야 한다.

VE10.28.02
두 출력값이 일치하지 않는 경우, 오류 상태로 천이되고 오류 표시를 출력하도록 개발 문서에 명세해야 한다.

[시험 절차]

TE10.28.01
시험자는 개발 문서를 검토하여 구현된 결과와 일치하는지 확인해야 한다.

TE10.28.02
해당 시험 항목은 TE10.07.02, TE10.08.01, TE10.08.02, TE10.08.03에 의하여 수행된다.

AS10.29: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

알고리즘의 자가시험은 암호모듈에서 지원하는 검증대상 키 길이, 모듈의 크기, DSA용 소수 또는 타원 곡선의 각각에 대하여 최소한 가장 작은 것을 사용해야 한다.

[벤더 요구사항]

VE10.29.01
암호모듈에 구현된 각각의 암호알고리즘에 대한 조건부 자가시험이 개발 문서에 명세되어야 한다.

[시험 절차]

TE10.29.01
시험자는 모듈의 검사와 개발 문서의 검토를 통하여 알고리즘의 자가시험이 암호모듈에서 지원하는 검증대상 키 길이, 모듈의 크기, DSA용 소수 또는 타원 곡선의 각각에 대하여 최소한 가장 작은 것으로 구현하고 있는지 확인해야 한다.

AS10.30: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

알고리즘이 다중 운영 모드(예: ECB, CBC)를 지원하는 경우, 자가시험에서 암호모듈이 지원하거나 검증기관이 지정하는 최소한의 한 개 이상의 운영 모드가 선택되어야 한다.

비고 해당 시험 항목은 **AS10.29**의 일부분으로 시험된다.

AS10.31: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

기지 답안 시험의 예로 일방향 함수가 있으며, 입력 테스트 벡터가 예상되는 값과 일치하는 출력을 생성해야 한다(예: 해시, 키를 사용한 해시, 메시지 인증, 엔트로피 벡터가 고정된 난수 발생기, SSP 합의).

비고 해당 시험 항목은 **AS10.28**의 일부분으로 시험된다.

AS10.32: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

기지 답안 시험의 예로 가역 함수가 있으며, 전방향 또는 역방향 기능이 모두 자가시험을 통과해야 한다(예: 대칭키 암호화 및 복호화, SSP 전송용 암호화 및 복호화, 전자서명의 생성과 검증).

비고 해당 시험 항목은 **AS10.28**의 일부분으로 시험된다.

AS10.33: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

비교 시험은 암호알고리즘을 두 번 이상 독립적으로 구현한 후 두 개 이상 구현물의 출력값을 비교한다. 출력값이 일치하지 않으면 암호알고리즘의 비교 자가시험은 실패로 판정된다.

[벤더 요구사항]

VE10.33.01
벤더는 구현된 암호알고리즘의 비교 자가시험을 서술해야 한다.

VE10.33.02
관련된 개발 문서에 대한 요구사항은 VE10.27.03에 명세되어 있다.

[시험 절차]

TE10.33.01
시험자는 비교 시험에 대하여 개발 문서가 다음을 포함하고 있는지 확인해야 한다.

a) 암호알고리즘을 두 번 이상 독립적으로 구현하여 사용함.
b) 알고리즘 구현물의 출력값을 연속적으로 비교함.
c) 두 출력값이 일치하지 않을 때 오류 상태로 전환되고 오류 표시를 출력함.

TE10.33.02
시험자는 소스 코드와 설계 문서를 검토하여 문서화된 비교 시험 수행 단계가 암호모듈에 구현되어 있는지 확인해야 한다.

AS10.34: (조건부 암호알고리즘 자가시험 – 보안수준 1, 2, 3, 4)

오류 탐지 시험은 암호알고리즘 구현 범위 내에서 오류 탐지 메커니즘들의 통합된 구현을 포함한다. 만약 오류가 탐지되면 암호알고리즘에 대한 오류 탐지 자가시험은 실패로 판정된다.

보기 난수 발생기에 대한 오류 탐지 시험은 난수 발생기의 구현물 내에서 엔트로피 소스가 정확하게 처리되고 있는가에 대한 오류도 시험한다.

[벤더 요구사항]

VE10.34.01
암호모듈에서 암호알고리즘에 대한 기지 답안 시험이나 비교 시험을 보완하기 위하여 오류 탐지 시험을 구현했는지 여부를 개발 문서에 명세해야 한다.

[시험 절차]

TE10.34.01
시험자는 오류 탐지 시험에 대하여 개발 문서가 다음을 포함하고 있는지 확인해야 한다.

a) 암호알고리즘의 명세/구현에 대한 오류 조건의 설명
b) 각 오류 조건에 대응되는 (내부적인) 오류 표시의 명세
c) 오류 탐지 시험에서 각각의 오류 조건이 시험된다는 것을 설명한 근거

TE10.34.02
시험자는 개발 문서를 검토하여 명세된 오류 탐지 시험과 구현된 오류 탐지 시험이 일치하는지 확인해야 한다.

TE10.34.03
해당 시험 항목은 TE10.07.02, TE10.07.03, TE10.09.02, TE10.09.03, TE10.10.01, TE10.10.02에 의하여 수행된다.

6.10.3.3 조건부 암호키 쌍 일치 시험

AS10.35: (조건부 암호키 쌍 일치 시험 – 보안수준 1, 2, 3, 4)

암호모듈이 공개키, 개인키 쌍을 생성한다면, KS X ISO/IEC 19790의 **부속서** C~E의 암호알고리즘 명세에 따라 생성된 공개키, 개인키 쌍에 대하여 암호키 쌍 일치 시험을 수행해야 한다.

비고 키 용도를 모르는 상태에서 키를 생성할 때, 암호키 쌍 일치 시험은 TE10.35.01 또는 TE10.35.02 중 한 개로 수행되어야 한다.

[벤더 요구사항]

VE10.35.01
검증대상 키 전송 방법, 비대칭 암호 기술을 수행하기 위하여 공개키, 개인키 쌍이 사용된다면 암호키 쌍 일치 시험에 대하여 개발 문서에 서술해야 한다. 이 시험에서는 평문 형태이거나 부호화된 메시지에 대하여 공개키를 이용하여 암호문을 생성한다. 암호화 적용 전과 후를 비교하여 동일한지 확인한다.

- 두 값이 일치하면, 암호모듈은 오류 상태에 진입하고 상태 인터페이스를 통해 오류 표시를 출력한다.
- 두 값이 다르면 개인키를 이용하여 복호화한다. 복호화된 결과가 원문과 일치하지 않으면 암호키 쌍 일치 시험은 실패로 판정된다.

VE10.35.02
공개키, 개인키 쌍이 전자서명의 생성과 검증에만 사용된다면, 서명 생성과 검증에 대한 암호키 쌍 일치 시험을 개발 문서에 제공해야 한다. 만일 서명이 검증되지 않으면 암호키 쌍 일치 시험은 실패한 것으로 판정된다.

VE10.35.03
공개키, 개인키 쌍이 SSP 합의를 수행하기 위하여 사용된다면, 암호키 쌍 일치 시험을 개발 문서에 제공해야 한다. 개발 문서에서 SSP 합의 시험에 요구되는 알고리즘을 식별해야 한다. 이 시험은 요구되는 알고리즘들을 구현하고 암호키 쌍 일치 시험이 통과되는지 확인하기 위하여 암호키 쌍을 적용하는 것으로 구성된다.

보기 Diffie-Hellman 키 합의는 전자서명 알고리즘과 동일한 유한체를 사용한다.

[시험 절차]

TE10.35.01
검증대상 키 전송 방법, 비대칭 암호 기술을 수행하기 위하여 공개키, 개인키 쌍이 사용된다면, 시험자는 소스 코드와 설계 문서를 확인하여 VE10.35.01에 정의된 대로 암호키 쌍 일치 시험의 구현이 개발 문서와 일치하는지 확인해야 한다.

TE10.35.02
공개키, 개인키 쌍이 전자서명의 생성과 검증에 사용된다면, 시험자는 소스 코드와 설계 문서를 확인하여 암호키 쌍 일치 시험의 구현이 VE10.35.02에 정의된 대로 개발 문서와 일치하는지 확인해야 한다.

TE10.35.03
공개키, 개인키 쌍이 SSP 합의를 수행하기 위하여 사용된다면, 시험자는 소스 코드와 설계 문서를 확인하여 암호키 쌍 일치 시험의 구현이 VE10.35.03에 정의된 대로 개발 문서와 일치하는지 확인해야 한다.

6.10.3.4 조건부 소프트웨어/펌웨어 로드 시험

AS10.36: (조건부 소프트웨어/펌웨어 로드 시험 – 보안수준 1, 2, 3, 4)

암호모듈이 외부에서 소프트웨어 또는 펌웨어를 로드하는 기능이 있을 때, KS X ISO/IEC 19790의 **7.4.3.4**에 추가하여 다음 요구사항이 충족되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.37: (조건부 소프트웨어/펌웨어 로드 시험 – 보안수준 1, 2, 3, 4)

암호모듈은 로드되는 소프트웨어 또는 펌웨어의 유효성 확인을 위해 검증대상 인증 기술을 구현해야 한다.

[벤더 요구사항]

VE10.37.01
외부에서 로드되는 소프트웨어 또는 펌웨어 구성 요소의 무결성을 보호하기 위해 검증대상 인증 기술이 사용됨을 개발 문서에 서술해야 한다.

VE10.37.02
암호모듈이 검증대상 인증 기술을 사용한다면, VE02.20.01에 명세된 바와 같이 구현 적합성 검증을 사전 검토 단계에서 받을 수 있도록 검증대상 인증 기술을 명세한 개발 문서를 제공해야 한다.

VE10.37.03
소프트웨어 또는 펌웨어가 로드되기 전에 참조될 인증키가 독립적으로 로드되는 방법을 개발 문서에 명세해야 한다.

VE10.37.04
소프트웨어/펌웨어 로드 시험이 통과되지 못하면, 로드된 소프트웨어/펌웨어가 사용되지 못하도록 하는 메커니즘을 개발 문서에 서술해야 한다.

[시험 절차]

TE10.37.01
시험자는 소프트웨어/펌웨어 로드 시험에 검증대상 인증 기술이 사용됨을 개발 문서로 제공하는지 확인해야 한다.

TE10.37.02
시험자는 암호모듈에 검증대상 인증 기술이 구현되었다면, VE02.20.01 및 TE02.20.02에 명세된 바와 같이 사전 검토 단계에서 시험한 구현 적합성 검증이 성공했는지 확인해야 한다.

TE10.37.03
암호모듈에 소프트웨어/펌웨어 로드 시험을 위해 검증대상 인증 기술이 구현되었다면, 시험자는 개발 문서에 소프트웨어/펌웨어 로드 시험에 대하여 다음 사항이 포함되어 있는지 확인해야 한다.

a) 구현된 검증대상 인증 기술의 명세
b) 검증대상 인증 기술로 보호하는 소프트웨어와 펌웨어 식별
c) 소프트웨어와 펌웨어가 로드될 때 검증대상 인증 기술을 적용하는 방법
d) 로드 시험이 시작될 때 검증대상 인증 기술을 이용하여 검증하는 방법
e) 검증대상 인증 기술에 의한 검증 실패가 자가시험의 실패로 판정

TE10.37.04
시험자는 소스 코드와 설계 문서를 검토하여 소프트웨어/펌웨어 로드 시험의 구현 결과가 TE10.37.01～ TE10.37.03과 일치하는지 확인해야 한다.

TE10.37.05
시험자는 로드되는 소프트웨어 또는 펌웨어를 변경하거나, 구현된 인증 메커니즘을 변경한 후 자가시험을 시작하고 상태 출력 인터페이스의 출력을 관찰한다. 만일 소프트웨어/펌웨어 로드 시험이 실

패했음을 출력하지 않으면 해당 시험 항목은 실패로 판정된다. 만일 시험자가 로드되는 소프트웨어 또는 펌웨어를 변경하거나 구현된 인증 메커니즘을 변경하는 것이 불가능하다면, 벤더는 시험이 수행될 수 없는 타당한 근거를 시험자에게 제공해야 한다.

TE10.37.06
시험자는 로드되는 소프트웨어 또는 펌웨어를 변경하거나, 참조될 서명값을 변경하거나, 구현된 서명 메커니즘을 변경한 후 암호모듈을 실행시키고 소프트웨어/펌웨어 로드 시험을 시작한다. 시험자는 자가시험 실패 시 로드된 소프트웨어 또는 펌웨어가 사용될 수 없게 되고 모듈의 버전 정보가 변하지 않음을 확인해야 한다.

TE10.37.07
시험자는 소스 코드와 설계 문서를 검토하여 참조될 서명값이 로드되는 소프트웨어 또는 펌웨어와는 독립적으로 로드됨을 확인해야 한다.

TE10.37.08
시험자는 소스 코드와 설계 문서를 검토하여 참조될 서명값이 소프트웨어 또는 펌웨어보다 먼저 로드되지 않으면 소프트웨어/펌웨어 로드 시험이 실패함을 확인해야 한다.

TE10.37.09
시험자는 참조될 서명값을 먼저 로드하지 않고 암호모듈을 실행하여 소프트웨어/펌웨어 로드 시험을 시작시킨다. 소프트웨어/펌웨어 로드 시험이 통과되면 해당 시험 항목은 실패로 판정된다.

AS10.38: (조건부 소프트웨어/펌웨어 로드 시험 – 보안수준 1, 2, 3, 4)

참조될 인증키는 소프트웨어 또는 펌웨어가 로드되기 이전에 독립적으로 암호모듈에 로드되어야 한다.

비고 해당 시험 항목은 **AS10.37**의 일부분으로 시험된다.

AS10.39: (**조건부 소프트웨어/펌웨어 로드 시험 – 보안수준** 1, 2, 3, 4)

적용된 검증대상 인증 기술이 성공적으로 검증되어야 한다. {그렇지 않으면 소프트웨어/펌웨어 로드 시험은 실패로 판정된다.}

비고 해당 시험 항목은 **AS10.37**의 일부분으로 시험된다.

AS10.40: (조건부 소프트웨어/펌웨어 로드 시험 – 보안수준 1, 2, 3, 4)

{적용된 검증대상 인증 기술이 성공적으로 검증되어야 한다.} 그렇지 않으면 소프트웨어/펌웨어 로드 시험은 실패로 판정된다.

비고 해당 시험 항목은 **AS10.37**의 일부분으로 시험된다.

AS10.41: (조건부 소프트웨어/펌웨어 로드 시험 – 보안수준 1, 2, 3, 4)

소프트웨어/펌웨어 로드 시험의 실패 시 로드된 소프트웨어 또는 펌웨어는 사용될 수 없어야 한다.

비고 해당 시험 항목은 **AS10.37**의 일부분으로 시험된다.

6.10.3.5 조건부 수동 주입 시험

AS10.42: (조건부 수동 주입 시험 – 보안수준 1, 2, 3, 4)

SSP 또는 키 구성 요소가 수동으로 암호모듈에 직접 주입되거나, 인간 운영자가 입력값을 잘못 주입하여 오류가 유발될 수 있는 경우, 다음과 같은 수동 주입 시험이 수행되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.43: (조건부 수동 주입 시험 – 보안수준 1, 2, 3, 4)

SSP 또는 키 구성 요소에 오류 탐지 코드(EDC)가 적용되어야 한다. {또는 중복 입력으로 주입되어야 한다.}

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.44: (조건부 수동 주입 시험 – 보안수준 1, 2, 3, 4)

{SSP 또는 키 구성 요소에 오류 탐지 코드(EDC)가 적용되어야 한다.} 또는 중복 입력으로 주입되어야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.45: (조건부 수동 주입 시험 – 보안수준 1, 2, 3, 4)

EDC가 사용된다면 EDC는 적어도 16비트의 길이를 가져야 한다.

비고 해당 시험 항목은 별도로 시험되지 않는다.

AS10.46: (조건부 수동 주입 시험 – 보안수준 1, 2, 3, 4)

EDC 검증이 실패하거나 반복 입력된 값이 일치하지 않으면 해당 시험 항목은 실패로 판정된다.

[벤더 요구사항]

VE10.46.01
벤더는 수동 주입 시험을 문서화해야 한다. SSP 또는 키 구성 요소에 대하여 오류 탐지 코드를 사용하는지 반복 입력을 사용하는지에 따라 수동 주입 시험은 다음을 포함한다.

a) 오류 탐지 코드(EDC)
   1) EDC 계산 알고리즘의 설명
   2) 검증 과정에 대한 설명
   3) 시험의 성공 또는 실패 시 예상되는 출력값

b) 반복 키 입력
   1) 검증 과정에 대한 설명
   2) 시험의 성공 또는 실패 시 예상되는 출력값

VE10.46.02
EDC가 SSP 또는 키 구성 요소와 연계된다면, SSP 또는 키 구성 요소의 형식(**AS09.03**)에 EDC용 필드를 포함해 이를 개발 문서에 명세해야 한다.

[시험 절차]

TE10.46.01
시험자는 개발 문서를 검토하여 수동 주입 시험에 어떤 방법(오류 탐지 코드 또는 중복 키 입력)이 사용되었는지 확인해야 한다. 사용된 방법에 따라 시험자는 소스 코드와 수동 주입 시험의 구현을 명세한 설계 문서를 검토하여 다음 정보가 포함되어 있는지 확인해야 한다.

a) 오류 탐지 코드(EDC)
   1) 수동 주입되는 모든 SSP 또는 키 구성 요소에 대하여 EDC용 필드가 포함된 형식(**AS09.03** 참조)
   2) EDC 알고리즘의 설명
   3) EDC 검증 과정에 대한 설명
   4) 시험의 성공 또는 실패 시 예상되는 모든 출력값

b) SSP와 키 구성 요소에 대한 반복 주입
   1) 수동 입력되는 모든 SSP와 키 구성 요소에 대한 반복 주입
   2) 반복 주입의 검증 과정에 대한 설명
   3) 시험의 성공 또는 실패 시 예상되는 모든 출력값

TE10.46.02
EDC를 이용한 수동 주입 시험에 대하여, 시험자는 암호모듈 검사와 개발 문서의 검토를 통해, SSP 또는 키 구성 요소의 형식에 EDC용 필드가 포함되어 있고 EDC의 길이가 적어도 16비트임을 확인해야 한다.

TE10.46.03
EDC를 이용한 수동 주입 시험에 대하여 시험자는 다음 시험을 수행해야 한다.

a) 시험자는 수동으로 입력되는 모든 SSP를 주입하고, 각 SSP의 입력에 사용되는 과정이 문서화된 절차와 일치하는지 확인해야 한다. 여기서 입력될 때 SSP의 형식도 개발 문서와 일치하는지 확인해야 한다.
b) 시험자는 수동으로 입력되는 각종 SSP를 오류 없이 주입한 후 상태 출력 인터페이스를 확인한다. 출력 표시가 없거나 수동 주입 시험의 성공에 대한 출력 표시와 개발 문서에 명세된 출력 표시가 일치하지 않으면 해당 시험 항목은 실패로 판정된다.
c) 시험자는 SSP가 정확하게 입력되었는지 확인하기 위하여, 주입된 SSP를 이용한 암호 연산의 수행을 시도해야 한다.
d) 시험자는 수동 주입 SSP와 연계된 EDC 또는 SSP 자체를 변경한 후 암호모듈에 이들을 주입한다. 시험자는 상태 출력 인터페이스를 통해 출력을 확인한다. 출력 표시가 없거나 수동 주입 시험의 실패에 대한 출력 표시와 개발 문서에 명세된 출력 표시가 일치하지 않으면 해당 시험 항목은 실패로 판정된다.
e) 시험자는 주입에 성공하지 못한 SSP를 사용하여 암호 연산을 시도해야 한다. SSP가 주입되지 않았음이 확인되도록 SSP를 사용한 각 연산은 실패해야 한다.

TE10.46.04
SSP 또는 키 구성 요소의 반복 주입을 이용한 수동 주입 시험에 대하여 시험자는 다음 시험을 수행해야 한다.

a) 시험자는 수동으로 입력되는 각종 SSP를 오류 없이 주입한 후 상태 출력 인터페이스를 확인한다. 출력 표시가 없거나 수동 주입 시험의 성공에 대한 출력 표시와 개발 문서에 명세된 출력 표시가 일치하지 않으면 해당 시험 항목은 실패로 판정된다.

b) 시험자는 SSP가 정확하게 입력되었는지 확인하기 위하여, 주입된 SSP를 이용한 암호 연산의 수행을 시도해야 한다.
c) 시험자는 반복 입력되는 첫 번째 또는 두 번째 SSP값 중 하나를 변경한 후 이들을 암호모듈에 입력해야 한다. 시험자는 상태 출력 인터페이스를 통해 출력 표시를 확인한다. 출력 표시가 없거나 수동 주입 시험의 실패에 대한 출력 표시와 개발 문서에 명세된 출력 표시가 일치하지 않으면 해당 시험 항목은 실패로 판정된다.
d) 시험자는 주입에 성공하지 못한 SSP를 사용하여 암호 연산을 시도해야 한다. SSP가 주입되지 않았음이 확인되도록 SSP를 사용한 각 연산은 실패해야 한다.

6.10.3.6 조건부 우회 기능 시험

AS10.47: (조건부 우회 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈에 암호 처리 없이 서비스를 제공하는 우회 기능이 구현되어 있다면(예: 모듈을 통해 평문이 전송되는 경우), 다음과 같은 우회 기능 시험이 수행되어 암호모듈의 구성 요소 가운데 단 하나라도 실패하는 경우 의도하지 않은 평문의 출력이 방지됨을 확인해야 한다.

비고 해당 시험 항목은 **AS10.48**～**AS10.51**의 일부분으로 시험된다.

AS10.48: (조건부 우회 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈이 서로 배타적인 우회 서비스나 암호 서비스 중 하나만을 선택할 때, 암호 기능을 제공하는 서비스가 올바르게 동작하는지 시험해야 한다.

[벤더 요구사항]

VE10.48.01
암호모듈에 우회 서비스가 구현되어 있다면, 암호모듈이 서로 배타적인 우회 서비스나 암호 서비스 중 하나를 선택할 때 암호 기능을 제공하는 서비스가 올바른 동작을 하는지 시험하는 우회 기능 시험을 구현해야 한다.

VE10.48.02
벤더는 우회 기능 시험을 명세한 개발 문서를 제출해야 한다. 우회 기능 시험에서는 배타적인 암호 서비스를 선택할 때 암호모듈이 평문 정보를 출력하지 않음을 입증해야 한다.

[시험 절차]

TE10.48.01
시험자는 암호모듈이 서로 배타적인 우회 서비스나 암호 서비스 중 하나를 선택할 때, 암호 기능을 제공하는 서비스가 올바른 동작을 하는지 시험하는 우회 기능 시험을 구현했는지 확인해야 한다.

TE10.48.02
시험자는 소스 코드와 설계 문서를 검토하여 우회 기능 시험의 구현이 개발 문서와 일치하는지 확인해야 한다.

TE10.48.03
시험자는 암호모듈을 배타적인 우회 서비스에서 배타적인 암호 서비스로 기능 전환을 수행한 후 평문 정보가 출력되지 않음을 확인해야 한다.

AS10.49: (조건부 우회 기능 시험 – 보안수준 1, 2, 3, 4)

암호 처리를 지원하는 서비스와 암호 처리를 지원하지 않는 서비스를 제공하는 경우, 암호모듈이 우회 서비스와 암호 서비스를 자동적으로 선택할 수 있다면, 암호모듈은 전환 과정 통제 메커니즘이 변경될 때(예: IP 송신/수신 주소 테이블) 암호 처리를 지원하는 서비스의 정확한 동작을 시험해야 한다.

[벤더 요구사항]

VE10.49.01
암호모듈이 우회 서비스와 암호 서비스를 자동적으로 선택할 수 있는 경우, 벤더는 전환 과정 통제 메커니즘이 변경될 때 암호 서비스의 정확한 동작을 검증하기 위한 우회 기능 시험을 구현해야 한다.

VE10.49.02
벤더는 우회 기능 시험을 명세한 개발 문서를 제출해야 한다. 우회 기능 시험은 전환 과정 통제 메커니즘이 변경될 때 다음을 보증해야 한다.

a) 전환 과정 통제 메커니즘이 직전 변경 이후부터 현재까지 변경되지 않았음을 확인해야 한다. 전환 과정 통제 메커니즘이 변경된 경우, 암호모듈은 오류 상태에 진입하고 상태 인터페이스를 통해 오류 표시를 출력해야 한다.
b) 암호모듈이 평문 정보를 출력하지 않는지 입증하는 방법으로 암호 서비스의 정확한 동작을 확인해야 한다. 암호모듈이 평문 정보를 출력하면 우회 기능 시험은 실패로 판정되어야 한다.

[시험 절차]

TE10.49.01
시험자는 전환 과정 통제 메커니즘이 변경될 때 서비스의 정확한 동작을 확인할 수 있는 우회 기능 시험을 암호모듈에 구현했는지 확인해야 한다.

TE10.49.02
시험자는 소스 코드와 설계 문서를 검토하여 우회 기능 시험에 대한 개발 문서가 구현된 결과와 일치하는지 확인해야 한다.

TE10.49.03
시험자는 다음으로부터 우회 기능 시험의 정확한 동작을 확인해야 한다.

a) 전환 과정 메커니즘이 직전 변경 이후부터 현재까지 변경되지 않았음을 보증하는지 확인해야 한다. 시험자는 사용된 방법을 문서화해야 한다. 암호모듈의 설계상 가능하다면, 시험자는 사용된 방법을 시험하기 위하여 전환 과정 메커니즘을 변경해 봐야 한다.
b) 평문 정보가 출력되지 않음을 확인함에 의해 전환 과정 메커니즘의 정상 동작을 확인하고 암호 서비스의 정확한 동작을 확인한다. 이를 위하여 전환 과정 메커니즘을 변경해야 한다.

AS10.50: (조건부 우회 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈이 우회 기능을 통제하는 내부 정보를 유지한다면, 암호모듈은 통제 정보의 변경이 진행되는 즉시 검증대상 인증 기술로 통제 정보의 무결성을 검증해야 한다. {그리고 통제 정보의 변경 직후 검증대상 인증 기술을 이용하여 새로운 무결성 검증값을 생성해야 한다.}

비고 해당 시험 항목은 별도로 시험되지 않는다. **AS10.51**의 일부분으로 시험된다.

AS10.51: (조건부 우회 기능 시험 – 보안수준 1, 2, 3, 4)

{암호모듈이 우회 기능을 통제하는 내부 정보를 유지한다면, 암호모듈은 통제 정보의 변경이 진행되는 즉시 검증대상 인증 기술로 통제 정보의 무결성을 검증해야 한다.} 그리고 통제 정보의 변경 직후 검증대상 인증 기술을 이용하여 새로운 무결성 검증값을 생성해야 한다.

[벤더 요구사항]

VE10.51.01
벤더는 우회 기능을 통제하는 내부 정보를 변경하는 방법을 개발 문서에 명세해야 한다.

VE10.51.02
벤더는 ① 우회 기능을 통제하는 내부 정보, ② 통제 정보를 갱신하는 내부 절차 및 ③ 검증대상 무결성 기술을 이용한 통제 정보의 무결성을 유지하는 메커니즘을 상세하게 명세한 개발 문서를 제출해야 한다.

[시험 절차]

TE10.51.01
시험자는 소스 코드와 설계 문서를 검토하여 암호모듈에서 유지되는 통제 정보가 개발 문서와 일치하는지 확인해야 한다.

TE10.51.02
시험자는 소스 코드와 설계 문서를 검토하여 통제 정보를 갱신하는 내부적인 절차가 개발 문서와 일치하는지 확인해야 한다.

TE10.51.03
시험자는 소스 코드와 설계 문서를 검토하여 통제 정보의 무결성을 유지하는 메커니즘이 개발 문서와 일치하는지 확인해야 한다.

6.10.3.7 조건부 핵심 기능 시험

AS10.52: (조건부 핵심 기능 시험 – 보안수준 1, 2, 3, 4)

암호모듈의 안전한 운영에 핵심적인 보안 기능이 있으면 조건부 자가시험에 반영되어야 한다.

비고 해당 시험 항목은 **AS10.24**의 일부분으로 시험된다.

6.10.3.8 주기적 자가시험

AS10.53: (주기적 자가시험 – 보안수준 1, 2, 3, 4)

암호모듈에 대한 주기적 시험의 요청이 있으면 암호모듈은 동작 전 또는 조건부 자가시험을 실행해야 한다. 주기적 자가시험을 시작하기 위해 요청할 수 있는 수단은 제공되는 서비스 요청, 리셋, 리부팅 또는 반복적인 전원 인가 등이다.

[벤더 요구사항]

VE10.53.01
운영자가 암호모듈의 주기적 시험을 요청하여 암호모듈이 동작 전 자가시험을 시작할 수 있게 하는

절차를 개발 문서에 명세해야 한다. 해당 절차는 모든 동작 전 자가시험을 포함해야 한다.

VE10.53.02
운영자가 암호모듈의 주기적 시험을 요청하여 암호모듈이 조건부 자가시험을 시작할 수 있게 하는 절차를 개발 문서에 명세해야 한다. 해당 절차는 적어도 조건부 암호알고리즘 시험을 포함해야 한다.

[시험 절차]

TE10.53.01
시험자는 개발 문서를 검토하여 요청에 의한 동작 전 자가시험의 시작에 모든 동작 전 자가시험이 포함되는지 확인해야 한다.

TE10.53.02
시험자는 요청에 의한 동작 전 자가시험을 시작하여 요청에 의한 동작 전 자가시험이 개발 문서와 일치하는지 확인해야 한다.

TE10.53.03
시험자는 요청에 의한 조건부 자가시험을 시작하여 요청에 의한 조건부 자가시험이 개발 문서와 일치하는지 확인해야 한다.

AS10.54: (주기적 자가시험 – 보안수준 3, 4)

암호모듈은 정해진 간격마다 자동적으로, 외부 입력 또는 외부 제어에 무관하게 동작 전 자가시험 또는 조건부 자가시험을 수행해야 한다.

[벤더 요구사항]

VE10.54.01
정해진 시간마다 자동적으로, 외부 입력 또는 외부 제어에 무관하게 동작 전 자가시험과 조건부 자가시험이 수행되는 방법을 개발 문서에 명세해야 한다.

VE10.54.02
동적 전 자가시험 또는 조건부 자가시험에 의해 암호모듈의 동작이 중단됨(interrupt)을 표시하는 상태 표시를 개발 문서에 명세해야 한다.

VE10.54.03
벤더는 동작 전 자가시험 또는 조건부 자가시험을 반복하는 동안 암호모듈의 동작을 중단하게 만드는 정해진 시간 간격과 조건에 대한 정보를 명세한 보안정책 문서를 제출해야 한다.

[시험 절차]

TE10.54.01
시험자는 암호모듈의 검사를 통하여 동작 전 자가시험과 조건부 자가시험이 VE10.54.01과 VE10.54.02에 명세된 대로 반복 수행되는지 확인해야 한다.

AS10.55: (주기적 자가시험 – 보안수준 3, 4)

동작 전 자가시험 또는 조건부 자가시험을 반복하는 동안 암호모듈의 작동을 중단시키는 시간 간격과 조건에 대한 정보를 보안정책 문서(KS X ISO/IEC 19790의 **부속서** B)에 명세해야 한다(예: 모듈이 중단할 수 없는 핵심적인 서비스를 수행하고 있을 때 동작 전 자가시험을 실시할 시간이 도래한 경

우, 자가시험은 다음 번으로 연기된다).

비고 해당 시험 항목은 **AS10.54**의 일부분으로 시험된다.

6.11 생명주기 보증

6.11.1 생명주기 보증 일반 요구사항

AS11.01: (생명주기 보증 – 수준 1, 2, 3, 4)

{ISO/IEC KS X 19790 **부속서**} **A.2.11**에 명세된 개발 문서는 제공되어야 한다.

[벤더 요구사항]

VE11.01.01
벤더는 KS X ISO/IEC19790의 **A.2.11**에서 명세된 대로 개발 문서를 제공해야 한다.

[시험 절차]

TE11.01.01
시험자는 벤더가 KS X ISO/IEC 19790의 **A.2.11**에 명세된 문서를 제공하는지 확인해야 한다.

6.11.2 형상 관리

AS11.02: (형상 관리 – 보안수준 1, 2, 3, 4)

보안 요구사항 {KS X ISO/IEC 19790, **AS11.03**～**AS11.05**}은 보안수준 1과 2 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS11.03**～**AS11.05**의 일부분으로 시험된다.

AS11.03: (형상 관리 – 보안수준 1, 2, 3, 4)

형상 관리 시스템은 암호모듈 및 암호 경계 내의 모듈 구성 요소를 개발하기 위해 사용되어야 하고, 또한 암호모듈과 관련된 개발 문서를 개발하기 위해 사용되어야 한다.

[벤더 요구사항]

VE11.03.01
개발 문서는 암호모듈, 모듈 구성 요소 및 모듈 관련 개발 문서를 관리하는 형상 관리 시스템을 서술해야 한다.

[시험 절차]

TE11.03.01
시험자는 형상 관리 시스템에 관한 개발 문서를 검증해야 한다.

AS11.04: (형상 관리 – 보안수준 1, 2, 3, 4)

암호모듈과 관련된 문서를 구성하고 있는 각 형상 항목(예: 암호모듈, 모듈 하드웨어 부품, 모듈 소프

트웨어 구성 요소, 모듈 HDL, 사용자 안내서, 보안정책 문서, 기타)에 대한 개별 버전은 유일한 식별자가 할당되어 표시되어야 한다.

[벤더 요구사항]

VE11.04.01
개발 문서는 모든 형상 항목의 목록을 포함해야 한다. 개발 문서는 형상 항목을 식별하는 방법을 반드시 서술해야 한다.

VE11.04.02
개발 문서는 검증대상 형상 항목의 버전을 식별하는 방법을 서술해야 한다.

[시험 절차]

TE11.04.01
시험자는 벤더가 형상 항목을 포함한 형상 목록을 제공하는지 확인해야 한다.

TE11.04.02
시험자는 개발 문서를 통해 모든 형상 항목을 식별하는 방법을 확인해야 한다.

TE11.04.03
시험자는 개발 문서를 통해 검증대상 형상 항목의 버전을 식별하는 방법을 확인해야 한다.

TE11.04.04
시험자는 개발 문서를 통해 검증대상 형상 항목의 버전이 유일하다는 것을 확인해야 한다.

AS11.05: (형상 관리 – 보안수준 1, 2, 3, 4)

형상 관리 시스템은 검증필 암호모듈(validated module) 생명주기 전체 동안 발생하는 개별 형상 항목을 ① 식별, ② 버전 또는 개정에 대한 변경을 추적하고 유지하여야 한다.

[벤더 요구사항]

VE11.05.01
개발 문서는 승인된 형상 변경이 형상 항목에 반영되는 방법을 명세해야 한다.

[시험 절차]

TE11.05.01
시험자는 개발 문서를 통해 승인된 형상 변경이 형상 항목에 반영되는 방법을 확인해야 한다.

AS11.06: (형상 관리 – 보안수준 3, 4)

자동화된 형상 관리 시스템을 사용하여 형상 항목이 관리되어야 한다.

[벤더 요구사항]

VE11.06.01
개발 문서는 암호모듈의 개발 및 생산을 지원하는 형상 관리 시스템의 자동화된 방법을 명세해야 한다.

[시험 절차]

TE11.06.01
시험자는 개발 문서를 통해 암호모듈의 개발을 지원하는 형상 관리 시스템의 자동화된 방법을 확인해야 한다.

6.11.3 설계

AS11.07: (설계 – 보안수준 1, 2, 3, 4)

암호모듈이 제공하는 보안 관련 서비스를 시험할 수 있도록 암호모듈이 설계되어야 한다.

비고 해당 시험 항목은 **6.4.3**에 따라 시험을 수행한다.

6.11.4 유한 상태 모델

AS11.08: (유한 상태 모델 – 보안수준 1, 2, 3, 4)

암호모듈 동작은 유한 상태 모델을 사용하여 명세되어야 한다. 유한 상태 모델은 ① 상태 천이도, ② 상태 천이표와 상태 설명으로 구성된다.

[벤더 요구사항]

VE11.08.01
벤더는 유한 상태 모델에 대한 개발 문서를 제공해야 한다. 유한 상태 모델은 모듈의 모든 상태를 식별해야 하고, 모든 상태 천이를 표시해야 한다. 상태 천이에 관한 개발 문서는 ① 내부 모듈 조건, ② 다른 상태로 천이를 시키는 입력 데이터 및 제어 입력, ③ 다른 상태 천이 후 얻어지는 데이터 출력 및 상태 출력을 서술해야 한다.

VE11.08.02
개발 문서는 다음 항목을 서술해야 한다.

a) 정상 동작
b) 기능 제한 동작
c) 데이터 입력 인터페이스
d) 데이터 출력 인터페이스
e) 제어 입력 인터페이스
f) 제어 출력 인터페이스
g) 상태 출력 인터페이스
h) 신뢰 채널
i) 암호 관리자 역할
j) 사용자 역할
k) 기타 역할(해당될 경우)
l) 보안 서비스
m) SSP 주입 서비스
n) 상태 출력 서비스
o) 운영자 인증
p) 자가시험
q) 타 인가된 서비스, 동작 및 기능(해당될 경우)

r) 오류 상태
s) 우회 서비스(해당될 경우)
t) 유지보수 접근 인터페이스(해당될 경우)
u) 유지보수 역할(암호모듈에 유지보수 접근 인터페이스가 제공되는 경우)
v) SSP 생성과 설정 서비스(해당될 경우)
w) SSP 출력 서비스(해당될 경우)
x) 휴면 상태(해당될 경우)
y) 초기화 이전 상태(해당될 경우)

[시험 절차]

TE11.08.01
시험자는 벤더가 제공한 개발 문서를 통해 유한 상태 모델을 검증해야 한다. 유한 상태 모델은 모듈의 모든 상태를 식별해야 하고, 모든 상태 천이를 표시해야 한다. 시험자는 개발 문서를 통해 ① 내부 모듈 조건, ② 다른 상태로 천이하는 입력 데이터 및 제어 입력, ③ 다른 상태 천이 후 얻어지는 데이터 출력 및 상태 출력을 확인해야 한다.

TE11.08.02
시험자는 유한 상태 천이도가 다음 항목과 일관성이 있음을 확인해야 한다.

a) 정상 동작
b) 기능 제한 동작
c) 데이터 입력 인터페이스
d) 데이터 출력 인터페이스
e) 제어 입력 인터페이스
f) 제어 출력 인터페이스
g) 상태 출력 인터페이스
h) 신뢰 채널
i) 암호 관리자 역할
j) 사용자 역할
k) 기타 역할(해당될 경우)
l) 보안 서비스
m) SSP 주입 서비스
n) 상태 출력 서비스
o) 운영자 인증
p) 자가시험
q) 타 인가된 서비스, 동작 및 기능(해당될 경우)
r) 오류 상태
s) 우회 서비스(해당될 경우)
t) 유지보수 접근 인터페이스(해당될 경우)
u) 유지보수 역할(암호모듈에 유지보수 접근 인터페이스가 제공되는 경우)
v) SSP 생성과 설정 서비스(해당될 경우)
w) SSP 출력 서비스(해당될 경우)
x) 휴면 상태(해당될 경우)
y) 초기화 이전 상태(해당될 경우)

TE11.08.03
시험자는 유한 상태 모델이 암호모듈 서비스, 보안 기능 사용, 오류 상태, 자가시험 또는 운영자 인

증 등의 상태가 구별되어 정의되어 있는지 확인해야 한다.

TE11.08.04
시험자는 개발 문서를 통해 유한 상태 천이도의 모든 상태가 상태 천이표와 상태 설명에 명세화되어 있는지 확인해야 한다.

TE11.08.05
시험자는 개발 문서를 통해 상태 천이표와 상태 설명에 포함된 모든 상태가 상태 천이도에 명세화되어 있는지 확인해야 한다.

TE11.08.06
시험자는 모듈의 동작이 유한 상태 천이도와 상태 천이표 및 상태 설명과 일관성이 있는지 확인해야 한다.

TE11.08.07
만약 모듈이 유지보수 접근 인터페이스를 포함하고 있다면, 시험자는 유한 상태 모델이 적어도 한 개 이상의 유지보수 상태가 정의되어 있음을 확인해야 한다. 시험자는 모든 유지보수 상태가 유한 상태 모델에 포함되어 있음을 확인해야 한다.

TE11.08.08
만약 유한 상태 모델이 분기를 명확하게 정의한다면, 시험자는 모듈의 유한 상태 모델을 확인해야 한다. 시험자는 데이터 입력과 제어 입력을 결합한 모든 가능한 조합을 분기 집합으로 나눌 수 있음을 확인해야 한다.

TE11.08.09
시험자는 모듈의 주요 상태로 진입하도록 암호모듈을 동작시켜야 한다. 시험자는 암호모듈이 특정 상태에 있는 동안을 나타내는 상태 표시를 확인해야 한다. 예측된 상태 표시가 관찰되지 않거나 같은 시간에 두 개 이상의 상태 표시가 관찰된다면(이것은 모듈이 같은 시간에 한 개 이상의 상태를 갖고 있음을 나타내고 있다.) 해당 시험 항목은 실패로 판정된다.

TE11.08.10
시험자는 초기 전원 인가 상태에서 초기 전원 인가 상태가 아닌 암호모듈의 다른 모든 상태로 천이하는 체인이 존재하는 것을 확인해야 한다.

TE11.08.11
시험자는 전원 꺼짐이 아닌 여러 상태에서 유한 상태 모델의 전원 꺼진 상태로 천이하는 체인이 존재함을 확인해야 한다.

TE11.08.12
시험자는 모든 가능한 데이터 입력 및 제어 입력에 의해 수행되는 유한 상태 모델의 작동이 정의되어 있는지 확인해야 한다. 작동에 대한 서술의 예는 다음과 같다.

“데이터 입력과 제어 입력의 모든 조합에 의해 수행되는 작동이 유한 상태 모델을 ERROR－3 상태로 진입하게 한다.”

AS11.09: (유한 상태 모델－보안수준 1, 2, 3, 4)

암호모듈이 해당 표준의 모든 요구사항을 충족할 수 있도록 FSM을 상세하게 서술하여야 한다.

비고 해당 시험 항목은 **AS11.10**～**AS11.13**의 일부분으로 시험된다.

AS11.10: (유한 상태 모델 – 보안수준 1, 2, 3, 4)

암호모듈의 FSM은 최소한 다음 동작 상태 및 오류 상태를 포함해야 한다.

- **전원 켜진 상태/전원 꺼진 상태**: 전원 꺼진 상태는 전원이 모듈에 공급되지 않아 대기 상태(휘발성 메모리 유지)가 되거나 비휘발성 메모리에 동작 상태가 유지되어 있는 상태(예: 동면 상태)이다. 전원 켜진 상태는 주전원, 보조 전원 또는 백업 전원이 모듈에 공급되는 상태이다. 해당 상태는 암호모듈에 공급되는 전력원과 별개의 상태이다. 소프트웨어 모듈에서 전원 켜진 상태는 암호모듈의 실행 가능한 이미지를 프로그램 실행 메모리에 로드하는 상태이다.
- **초기화 상태**: 암호모듈이 검증대상 동작 상태로 천이하기 전 암호모듈을 초기화하는 상태
- **암호 관리자 상태**: 암호 관리자 서비스가 실행되는 상태(예: 암호 초기화, 안전한 관리 및 키 관리)
- CSP **주입 상태**: CSP를 암호모듈에 주입하는 상태
- **사용자 상태**: (사용자 역할이 구현된 경우): 인가된 사용자가 보안 서비스, 암호 동작 또는 다른 검증대상 기능을 암호모듈이 수행하게 하는 상태
- **검증대상 동작 상태**: 검증대상 암호알고리즘이 수행되는 상태
- **자가시험 상태**: 암호모듈이 자가시험을 수행하고 있는 상태
- **오류 상태**: 암호모듈에서 오류가 발생한 상태(예: 자가시험 실패). 하나의 암호모듈 오류 상태는 한 가지 이상의 오류 조건으로부터 발생할 수 있다. 오류 상태는 암호모듈의 유지보수, 서비스나 수리를 요구하는 “심각한 오류”(예: 장비의 오작동으로 발생하는 오류)와 모듈의 초기화나 재설정을 요구하는 “단순한 오류”로 구분된다.

비고 해당 시험 항목은 **AS11.08**의 부분으로 시험된다.

AS11.11: (유한 상태 모델 – 보안수준 1, 2, 3, 4)

암호모듈의 유지보수, 서비스나 수리가 필요한 심각한 오류 상태가 아니라면, 모든 오류 상태는 그로부터 복구 가능해야 한다.

[벤더 요구사항]

VE11.11.01
개발 문서는 암호모듈의 유지보수, 서비스나 수리가 필요하지 않은 개별 오류 상태에 적용할 수 있는 복구 방법을 서술해야 한다.

[시험 절차]

TE11.11.01
유지보수, 서비스나 수리를 요구하지 않는 각각의 오류 상태에서, 시험자는 암호모듈이 허용 가능한 운영 상태나 초기화 상태로 천이될 수 있음을 확인해야 한다. 오류 상태에서 운영 상태 또는 초기화 상태로의 천이는 두 부분으로 구성된다. 첫째, 시험자는 암호모듈이 오류 상태를 표시함을 확인한다. 둘째, 시험자는 암호모듈이 목표 상태에서 정확하게 운영 중임을 확인한다. 시험자는 오류 상태에서 복구하는 요구사항을 (즉, 소스 코드 검사나 모듈의 실행에 의한) 확인하는 방법을 보고해야 한다.

AS11.12: (유한 상태 모델 – 보안수준 1, 2, 3, 4)

암호모듈 서비스, 암호알고리즘 사용, 오류 상태, 자가시험 또는 운영자 인증은 별개의 상태로 정의되어야 한다.

비고 해당 시험 항목은 **AS11.08**의 일부분으로 시험된다.

AS11.13: (유한 상태 모델 – 보안수준 1, 2, 3, 4)

암호 관리자를 제외한 역할은 다른 암호모듈 상태에서 암호 관리자 상태로 변경할 수 없다.

[벤더 요구사항]

VE11.13.01
개발 문서는 암호 관리자가 아닌 역할 상태에서 암호 관리자 상태로 천이할 수 없음을 명시해야 한다.

[시험 절차]

TE11.13.01
시험자는 개발 문서를 검토하여 암호 관리자가 아닌 역할 상태에서 암호 관리자 상태로의 천이가 금지됨을 확인해야 한다.

6.11.5 개발

AS11.14: (개발 – 보안수준 1, 2, 3, 4)

다음 요구사항은 보안수준 1에 해당하는 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS11.15**~**AS11.21**의 일부분으로 시험된다.

AS11.15: (개발 – 보안수준 1, 2, 3, 4)

암호모듈이 소프트웨어나 펌웨어를 포함한다면, 컴파일하여 실행 형태로 변환하는 데 사용된 소스 코드, 언어 참고 자료, 컴파일러, 컴파일러 버전과 컴파일러 옵션, 링커와 링커 옵션, 런타임 라이브러리와 런타임 라이브러리 설정, 구성 설정, 빌드 프로세스와 방법, 빌드 옵션, 환경 변수, 모든 다른 리소스 등은 형상 관리 시스템을 사용하여 추적되어야 한다.

[벤더 요구사항]

VE11.15.01
소프트웨어나 펌웨어를 포함하고 있는 암호모듈의 경우, 벤더는 컴파일하여 실행 형태로 변환하는 데 사용된 소스 코드, 언어 참고 자료, 컴파일러, 컴파일러 버전과 컴파일러 옵션, 링커와 링커 옵션, 런타임 라이브러리와 런타임 라이브러리 설정, 구성 설정, 빌드 프로세스와 방법, 빌드 옵션, 환경 변수, 모든 다른 리소스 등을 서술한 개발 문서를 제공해야 한다.

VE11.15.02
VE11.15.01에서 개발 문서에 서술된 개별 항목에 대하여, 벤더는 형상 관리 시스템을 사용하여 동 항목을 추적하고 있다는 개발 문서를 제공해야 한다.

[시험 절차]

TE11.15.01
소프트웨어나 펌웨어를 포함하고 있는 암호모듈의 경우, 시험자는 컴파일하여 실행 형태로 변환하는 데 사용된 소스 코드, 언어 참고 자료, 컴파일러, 컴파일러 버전과 컴파일러 옵션, 링커와 링커 옵션, 런타임 라이브러리와 런타임 라이브러리 설정, 구성 설정, 빌드 프로세스와 방법, 빌드 옵션, 환경 변수, 모든 다른 리소스 등을 서술한 개발 문서를 확인해야 한다.

TE11.15.02
TE11.15.01에서 개발 문서의 서술된 개별 항목에 대하여, 시험자는 형상 관리 시스템을 사용하여 동 항목들을 추적하고 있다는 개발 문서를 확인해야 한다.

AS11.16: (개발 – 보안수준 1, 2, 3, 4)

암호모듈이 소프트웨어나 펌웨어를 포함한다면 소프트웨어나 펌웨어가 암호모듈의 설계와 일치함을 나타내는 주석을 소스 코드에 달아야 한다.

[벤더 요구사항]

VE11.16.01
벤더는 암호모듈이 포함하고 있는 모든 소프트웨어 구성 요소와 펌웨어 구소 요소에 대한 명칭과 목록을 제공해야 한다.

VE11.16.02
벤더는 암호모듈이 포함하고 있는 소프트웨어 구성 요소와 펌웨어 구성 요소의 주석이 있는 소스 목록을 제공해야 한다.

[시험 절차]

TE11.16.01
시험자는 벤더가 제공한 목록을 사용하여 각 소프트웨어 구성 요소와 펌웨어 구성 요소에 대한 소스 목록이 암호모듈에 포함되어 있음을 검증해야 한다.

AS11.17: (개발 – 보안수준 1, 2, 3, 4)

암호모듈이 하드웨어를 포함한다면 개발 문서는 해당 사항이 있는 경우, 회로도(schematics) 혹은 하드웨어 서술 언어(HDL)를 명세해야 한다.

[벤더 요구사항]

VE11.17.01
벤더는 암호모듈에 포함된 하드웨어 구성 요소 목록을 제공해야 한다.

[시험 절차]

TE11.17.01
시험자는 벤더가 제공한 목록을 사용해서 개발 문서가 하드웨어 구성 요소를 서술한 회로도 또는 하드웨어 서술 언어(HDL) 목록를 포함하는지 검증해야 한다.

AS11.18: (개발 – 보안수준 1, 2, 3, 4)

암호모듈이 하드웨어를 내장한다면, HDL은 하드웨어와 암호모듈의 설계가 일치함을 나타내도록 주석 처리해야 한다.

[벤더 요구사항]

VE11.18.01
벤더는 암호모듈에 포함된 각 하드웨어 구성 요소를 주석으로 표시한 HDL 목록을 제공해야 한다.

[시험 절차]

TE11.18.01
시험자는 벤더가 제공한 목록을 사용하여 각 하드웨어 구성 요소의 HDL 목록이 암호모듈에 포함되어 있는지 검증해야 한다.

AS11.19: (개발 – 보안수준 1, 2, 3, 4)

{소프트에어 암호모듈, 펌웨어 암호모듈, 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여} 벤더가 개발 단계에서 무결성 및 인증 기법 메커니즘의 결과 코드를 계산하여 이 결과 코드를 소프트웨어 모듈 혹은 펌웨어 모듈에 결합해야 한다. 여기서 무결성 및 인증 메커니즘은 {KS X ISO/IEC 19790} **7.5**와 **7.10**에 명세되어 있다.

[벤더 요구사항]

VE11.19.01
소프트에어 암호모듈, 펌웨어 암호모듈, 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여, 벤더는 개발 단계에서 무결성 및 인증 기법 메커니즘의 결과 코드를 계산하여 이 결과 코드가 소프트웨어 모듈 혹은 펌웨어 모듈에 결합되었음을 서술하는 개발 문서를 제출해야 한다. 여기서 무결성 및 인증 기법 메커니즘은 {KS X ISO/IEC 19790} **7.5**와 **7.10**에 명세되어 있다.

[시험 절차]

TE11.19.01
소프트에어 암호모듈, 펌웨어 암호모듈, 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여, 시험자는 개발 단계에서 무결성 및 인증 기법 메커니즘의 결과 코드를 계산하여 이 결과 코드가 소프트웨어 모듈 혹은 펌웨어 모듈에 결합되었음을 서술한 개발 문서를 확인해야 한다. 여기서 무결성 및 인증 기법 메커니즘은 {KS X ISO/IEC 19790} **7.5**와 **7.10**에 명세되어 있다.

AS11.20: (개발 – 보안수준 1, 2, 3, 4)

{소프트웨어 암호모듈, 펌웨어 암호모듈, 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여} 개발 문서는 소스 코드를 실행 파일 형태로 컴파일하는 컴파일러, 구성 설정 및 방법을 명세해야 한다.

비고 해당 시험 항목은 **AS11.15**의 일부분으로 시험된다.

AS11.21: (개발 – 보안수준 1, 2, 3, 4)

{소프트웨어 암호모듈, 펌웨어 암호모듈, 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여} 제품을 생산할 수 있는 개발 도구(예: 컴파일러)를 사용하여 암호모듈을 개발해야 한다.

[벤더 요구사항]

VE11.21.01
벤더는 제품을 생산할 수 있는 개발 도구(예: 컴파일러)를 사용하여 암호모듈을 개발하였음을 서술하는 개발 문서를 제공해야 한다.

[시험 절차]

TE11.21.01
시험자는 제품을 생산할 수 있는 개발 도구(예: 컴파일러)를 사용하여 암호모듈을 개발하였음을 서술하는 개발 문서를 확인해야 한다.

AS11.22: (개발 – 보안수준 2, 3, 4)

보안 요구사항 {KS X ISO/IEC 19790, **AS11.23**～**AS11.26**}은 보안수준 2와 3의 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS11.23**～**AS11.26**의 일부분으로 시험된다.

AS11.23: (개발 – 보안수준 2, 3, 4)

모든 소프트웨어 또는 펌웨어는 상위 수준의 언어로 구현되어야 한다. {또는 암호모듈의 성능이 중요하거나 상위 수준 언어를 사용할 수 없어 하위 수준 언어(예: 어셈블리 언어 또는 마이크로코드)를 사용하는 경우 근거가 제공되어야 한다.}

[벤더 요구사항]

VE11.23.01
벤더는 암호모듈의 모든 소프트웨어 또는 펌웨어는 상위 수준의 언어로 구현되었음을 서술하는 개발 문서를 제공해야 한다.

[시험 절차]

TE11.23.01
시험자는 암호모듈의 모든 소프트웨어 또는 펌웨어는 상위 수준의 언어로 구현되었음을 서술하는 개발 문서를 확인해야 한다.

AS11.24: (개발 – 보안수준 2, 3, 4)

{모든 소프트웨어 또는 펌웨어는 상위 수준이며 언어로 구현되어야 한다.} 또는 암호모듈의 성능이 중요하거나 상위 수준 언어를 사용할 수 없어 하위 수준 언어(예: 어셈플리 언어 또는 마이크로코드)를 사용하는 경우 근거가 제공되어야 한다.

[벤더 요구사항]

VE11.24.01
벤더는 상위 수준 언어를 사용하지 않고 구현된 모든 소프트웨어 또는 펌웨어를 식별하거나 하위 수준 언어를 사용하여 구현한 경우 근거를 제공해야 한다. 근거는 상위 수준 언어의 비가용성이나 소프트웨어나 펌웨어의 강화된 성능의 필요성을 언급해야 한다.

[시험 절차]

TE11.24.01
시험자는 소프트웨어 구성 요소 또는 펌웨어 구성 요소의 소스 코드를 검사해서 소프트웨어 구성 요소와 펌웨어 구성 요소가 하위 수준 언어로 개발되었는지 확인해야 한다. 시험자는 VE11.24.01에서 벤더가 식별하지 못한 하위 수준으로 개발된 소프트웨어 구성 요소 또는 펌웨어 구성 요소가 없음을 확인해야 한다.

AS11.25: (개발 – 보안수준 2, 3, 4)

암호모듈에 내장된 맞춤형 집적회로는 고급 하드웨어 기술 언어(HDL)(예: VHDL 또는 Verilog)를 사용하여 구현되어야 한다.

[벤더 요구사항]

VE11.25.01
벤더는 상위 수준의 정형화 언어를 사용하여 구현된 하드웨어 구성 요소를 서술한 문서를 제공해야 한다.

[시험 절차]

TE11.25.01
시험자는 VE11.25.01에 명시된 정보를 서술한 개발 문서를 확인해야 한다.

AS11.26: (개발 – 보안수준 2, 3, 4)

암호모듈의 기능과 실행과 관련이 없는 코드, 매개변수, 기호를 사용하지 않는 방식으로 소프트웨어 암호모듈 또는 펌웨어 암호모듈 및 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소를 설계하고 구현해야 한다.

[벤더 요구사항]

VE11.26.01
소프트웨어 암호모듈 또는 펌웨어 암호모듈 및 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여, 벤더는 암호모듈의 기능과 실행과 관련이 없는 코드, 매개변수, 기호를 사용하지 않는 방식으로 소프트웨어 또는 펌웨어를 설계하고 구현했음을 서술한 문서를 제공해야 한다.

[시험 절차]

TE11.26.01
소프트웨어 암호모듈 또는 펌웨어 암호모듈 및 하이브리드 모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여, 시험자는 암호모듈의 기능과 실행과 관련이 없는 코드, 매개변수, 기호를 사용하지 않는 방식으로 소프트웨어 또는 펌웨어를 설계하고 구현했음을 서술한 문서를 확인해야 한다.

AS11.27: (개발 – 보안수준 4)

보안 요구사항(**AS11.28**)은 보안수준 4 암호모듈에 적용해야 한다.

비고 해당 시험 항목은 **AS11.28**의 일부분으로 시험된다.

AS11.28: (개발 – 보안수준 4)

각 암호모듈 하드웨어 구성 요소 및 암호모듈 소프트웨어 구성 요소에 대하여, 개발 문서는 ① 암호모듈 구성 요소, 기능 또는 절차를 정확하게 실행시키기 위해 시작 단계에서 요구되는 사전 조건과 ② 암호모듈 구성 요소, 기능 또는 절차의 실행이 정확히 완료된 경우 예측되는 사후 조건을 명세하는 주석을 서술해야 한다.

비고 사전 조건과 사후 조건은 암호모듈 구성 요소, 기능 또는 절차를 실행하는 동작을 완전하고,

명확하게 설명할 수 있도록 상세화된 표기법을 사용하여 명세할 수 있다.

[벤더 요구사항]

VE11.28.01
하드웨어, 소프트웨어, 펌웨어 구성 요소에 대한 소스 코드는 **AS11.28**이 요구하는 주석, 사전 조건과 사후 조건을 포함해야 한다.

[시험 절차]

TE11.28.01
시험자는 VE11.28.01에서 명세된 정보를 포함하고 있는 소스 코드를 검증해야 한다.

6.11.6 벤더 시험

AS11.29: (벤더 시험 – 수준 1, 2, 3, 4)

개발 문서는 암호모듈에 대하여 수행된 기능 시험을 명시해야 한다.

[벤더 요구사항]

VE11.29.01
벤더는 암호모듈에 대하여 수행된 기능 시험을 명시한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.29.01
시험자는 암호모듈에 대하여 수행된 기능 시험을 명시한 개발 문서를 검증해야 한다.

AS11.30: (벤더 시험 – 보안수준 1, 2, 3, 4)

소프트웨어 암호모듈, 펌웨어 암호모듈 또는 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여 벤더는 현재 자동화 보안 진단 도구(예: 버퍼 오버플로 탐지)를 사용해야 한다.

[벤더 요구사항]

VE11.30.01
소프트웨어 암호모듈, 펌웨어 암호모듈 또는 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여 벤더는 현재 자동화 보안 진단 도구(예: 버퍼 오버플로 탐지)를 사용했음을 서술한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.30.01
소프트웨어 암호모듈, 펌웨어 암호모듈 또는 하이브리드 암호모듈의 소프트웨어 구성 요소 또는 펌웨어 구성 요소에 대하여 시험자는 현재 버전의 자동화 보안 진단 도구(예: 버퍼 오버플로 탐지)를 사용했음을 서술한 개발 문서를 확인해야 한다.

AS11.31: (벤더 시험 – 보안수준 3, 4)

개발 문서는 암호모듈에 대하여 수행된 상세 수준의 시험 절차와 결과를 명세화해야 한다.

[벤더 요구사항]

VE11.31.01
벤더는 암호모듈에 대하여 수행된 상세 수준의 시험 절차와 결과를 명세화한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.31.01
시험자는 암호모듈에 대하여 수행된 상세 수준의 시험 절차와 결과를 명세화한 개발 문서를 확인해야 한다.

6.11.7 배포 및 운영

AS11.32: (배포 및 운영 – 보안수준 1, 2, 3, 4)

개발 문서는 암호모듈의 안전한 설치, 초기화 및 시동을 위한 절차를 명세화해야 한다.

[벤더 요구사항]

VE11.32.01
개발 문서는 암호모듈의 안전한 설치, 초기화 및 시동을 위한 절차를 서술해야 한다.

[시험 절차]

TE11.32.01
시험자는 문서가 암호모듈의 안전한 설치, 초기화 및 시동을 위한 절차 등을 포함하고 있는지 확인해야 한다.

TE11.32.02
시험자는 암호모듈의 안전한 설치, 초기화, 시작 등의 절차를 수행하고, 정확성을 확인해야 한다.

AS11.33: (배포 및 운영 – 보안수준 2, 3, 4)

개발 문서는 암호모듈 버전들이 인가된 운영자에게 배포, 설치, 초기화되는 동안 안전성 유지에 필요한 절차를 명세해야 한다.

[벤더 요구사항]

VE11.33.01
배포 문서는 암호모듈이 인가된 운영자에게 배포, 설치, 초기화되는 동안 안전성 유지에 필요한 절차를 서술해야 한다.

[시험 절차]

TE11.33.01
시험자는 암호모듈이 인가된 운영자에게 배포, 설치, 초기화되는 동안 안전성 유지에 필요한 절차를 서술한 개발 문서를 확인해야 한다.

AS11.34: (배포 및 운영 – 보안수준 2, 3, 4)

해당 절차는 암호모듈이 인가받은 운영자에게 운송, 설치, 초기화되는 동안 변조 탐지 방법을 명세해야 한다.

[벤더 요구사항]

VE11.34.01
벤더는 암호모듈이 인가받은 운영자에게 운송, 설치, 초기화되는 동안 변조 탐지 방법 절차를 서술한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.34.01
시험자는 암호모듈이 인가받은 운영자에게 운송, 설치, 초기화되는 동안 변조 탐지 방법 절차를 서술한 개발 문서를 확인해야 한다.

AS11.35: (배포 및 운영 – 보안수준 4)

해당 절차는 인가받은 운영자가 벤더가 제공한 인증 데이터를 사용하여 암호모듈을 인증할 것을 요구해야 한다.

[벤더 요구사항]

VE11.35.01
벤더는 인가받은 운영자가 벤더가 제공한 인증 데이터를 사용하여 암호모듈을 인증할 것을 요구하는 절차를 서술한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.35.01
시험자는 인가받은 운영자가 벤더에 의해 제공된 인증 데이터를 사용하여 암호모듈을 인증할 것을 요구하는 절차를 서술한 개발 문서를 확인해야 한다.

6.11.8 수명의 종료

AS11.36: (수명의 종료 – 수준 1, 2, 3, 4)

개발 문서는 암호모듈의 안전한 소거 절차를 명세해야 한다.

[벤더 요구사항]

VE11.36.01
벤더는 암호모듈의 안전한 소거 절차를 명세화한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.36.01
시험자는 암호모듈의 안전한 소거 절차를 명세화한 개발 문서를 확인해야 한다.

AS11.37: (수명의 종료 – 보안수준 3, 4)

개발 문서는 암호모듈을 안전하게 파기하는 데 필요한 절차를 명세해야 한다.

[벤더 요구사항]

VE11.37.01
벤더는 암호모듈을 안전하게 파기하는 데 필요한 절차를 명세한 개발 문서를 제공해야 한다.

[시험 절차]

TE11.37.01
시험자는 암호모듈을 안전하게 파기하는 데 필요한 절차를 명세한 개발 문서를 확인해야 한다.

6.11.9 안내서

AS11.38: (안내서 – 보안수준 1, 2, 3, 4)

관리자 안내서는 다음을 명세해야 한다.

- 암호 관리자와 다른 관리자 역할에 사용할 수 있는 암호모듈의 관리 기능, 보안 이벤트, 보안매개변수(해당되면 매개변수값), 물리적 포트와 논리적 인터페이스
- 독립된 운영자 인증 메커니즘이 기능적으로 독립을 유지하기 위해 요구되는 절차
- 검증대상 동작모드에서 암호모듈을 관리하는 방법에 대한 절차
- 암호모듈의 안전한 운영과 관련된 사용자 동작에 대한 가정 사항

[벤더 요구사항]

VE11.38.01
벤더는 **AS.38**에 있는 정보 목록을 포함하는 개발 문서를 제공해야 한다.

VE11.38.02
안내서는 모듈의 필요한 관리자가 사용할 수 있어야 한다.

[시험 절차]

TE11.38.01
시험자는 **AS11.38**에 있는 정보 목록을 포함하는 개발 문서를 확인해야 한다.

AS11.39: (안내서 – 보안수준 1, 2, 3, 4)

비관리자 안내서는 다음을 명세해야 한다.

- 암호모듈 사용자가 사용할 수 있는 검증대상 및 비검증대상 암호알고리즘, 물리적 포트, 논리적 인터페이스
- 암호모듈의 검증대상 동작모드에 대한 모든 사용자의 책임

[벤더 요구사항]

VE11.39.01

벤더는 **AS11.39**에 포함된 정보 목록을 포함하는 문서를 제공해야 한다.

VE11.39.02
안내서는 모듈의 적절한 비관리자가 사용할 수 있어야 한다.

[시험 절차]

TE11.39.01
시험자는 **AS11.39**에 포함된 정보 목록을 포함하는 벤더 제공 문서를 확인해야 한다.

6.12 기타 공격에 대한 대응

비고 1 보안 요구사항 및 관련 시험을 통해 보안 메커니즘의 존재와 적합한 기능 동작 여부가 검증될 수 있다.
비고 2 보안정책서는 {KS X ISO/IEC 19790 **부속서**} **B.2.12**에 명세된 보안 요구사항들을 포함해야 한다.

AS12.01: (기타 공격에 대한 대응 – 보안수준 1, 2, 3, 4)

{KS X ISO/IEC 19790 **부속서**} **A.2.12**에 명세된 보안 요구사항을 충족하는 개발 문서가 제출되어야 한다.

[벤더 요구사항]

VE12.01.01
벤더는 KS X ISO/IEC 19790의 **A.2.12**에서 명세된 문서 요구사항을 제출해야 한다.

[시험 절차]

TE12.01.01
시험자는 벤더가 KS X ISO/IEC 19790의 **A.2.12**에서 명세된 문서를 제출했는지 확인해야 한다.

AS12.02: (기타 공격에 대한 대응 – 보안수준 1, 2, 3, 4)

암호모듈이 {KS X ISO/IEC 19790} 내 어디서도 명세되지 않은 하나 이상의 특정 공격에 대응하도록 설계되었다면 개발 문서는 모듈이 대응하도록 설계된 공격을 열거해야 한다.

[벤더 요구사항]

VE12.02.01
벤더는 모듈이 대응하도록 설계된 공격들을 열거한 문서를 제출해야 한다.

[시험 절차]

TE12.02.01
시험자는 벤더가 모듈이 대응하도록 설계된 공격들을 열거한 문서를 확인해야 한다.

AS12.03: (기타 공격에 대한 대응 – 보안수준 4)

다음 보안 요구사항은 보안수준 4 암호모듈에 적용되어야 한다.

비고 해당 시험 항목은 **AS12.04**의 일부분으로 시험된다.

AS12.04: (기타 공격에 대한 대응－보안수준 4)

{KS X ISO/IEC 19790} 내 어디서도 명세되지 않은 특정 공격들에 대한 대응 기법이 요구되면, 개발 문서는 공격에 대응하기 위한 방법과 대응 기술의 효과를 시험하는 방법을 명세해야 한다.

[벤더 요구사항]

VE12.04.01
벤더는 공격에 대응을 위한 방법을 문서에 명세해야 한다.

VE12.04.02
벤더는 대응 기술의 유효성 시험방법을 문서에 명세해야 한다.

VE12.04.03
벤더는 대응 기술의 유효성을 문서에 명세해야 한다.

[시험 절차]

TE12.04.01
시험자는 벤더가 공격에 대응하기 위한 방법을 명세하였는지 확인해야 한다.

TE12.04.02
시험자는 벤더가 대응 기술의 유효성 시험방법을 명세한 문서를 제출했는지 확인해야 한다.

TE12.04.03
시험자는 벤더가 대응 기술의 유효성을 명세한 문서를 제출했는지 확인해야 한다.

6.13 A 문서 요구사항

비고 KS X ISO/IEC 19790의 **부속서** A는 암호모듈의 최소 문서 요구사항을 명세한 것이다.

ASA.01: (문서－보안수준 1, 2, 3, 4)

이 부속서 {KS X ISO/IEC 19790 **부속서** A}는 독립적으로 검증을 수행하기 위한 암호모듈에 요구되는 최소한 문서 내용을 명시한다. {문서는 이들 요구사항을 충족해야 한다.}

[벤더 요구사항]

VEA.01.01
벤더는 KS X ISO/IEC 19790의 **A.2.1**～**A.2.12**에 명시된 최소 문서 요구사항을 만족하는 문서를 제공해야 한다.

[시험 절차]

TEA.01.01
시험자는 벤더에서 제공받은 문서가 KS X ISO/IEC 19790의 **A.2.1**～**A.2.12**에 명시된 최소 문서 요구사항을 만족하는 문서인지 확인해야 한다.

6.14 B 암호모듈 보안정책서

비고 KS X ISO/IEC 19790의 **부속서** B는 암호모듈 보안정책서의 최소 요구사항을 명세한 것이다.

ASB.01: (보안정책서 – 보안수준 1, 2, 3, 4)

다음 목록은 보안정책서에서 제공되어야 할 요구사항을 요약한 것이다.

[벤더 요구사항]

VEB.01.01
벤더는 KS X ISO/IEC 19790의 **B.2.1**～**B.2.12**에 명시된 최소 보안정책서 요구사항을 만족하는 암호모듈 보안정책서를 제공해야 한다.

[시험 절차]

TEB.01.01
시험자는 벤더에서 제공받은 보안정책서가 KS X ISO/IEC 19790의 **B.2.1**～**B.2.12**에 명시된 최소 보안정책서 요구사항을 만족하는 문서인지 확인해야 한다.

ASB.02: (보안정책서 – 보안수준 1, 2, 3, 4)

보안정책서의 형식은 KS X ISO/IEC 19790의 **부속서** B나 검증기관에서 명시한 양식을 참조하여 작성한다.

[벤더 요구사항]

VEB.02.01
벤더는 KS X ISO/IEC 19790의 **B.2.1**～**B.2.12**에 명시되거나 검증기관에서 명시한 보안정책서를 제공해야 한다.

[시험 절차]

TEB.02.01
시험자는 벤더에게 제공받은 보안정책서가 KS X ISO/IEC 19790의 **B.2.1**～**B.2.12**에 명시되거나 검증기관에서 명시한 보안정책서를 충족하는 문서인지 확인해야 한다.

ASB.03: (보안정책서 – 보안수준 1, 2, 3, 4)

보안정책서는 복사나 배포에 대한 저작권을 가지지 않아야 한다.

[벤더 요구사항]

VEB.03.01
벤더는 저작권이 없는 보안정책서를 제공해야 한다.

VEB03.02
벤더가 보안정책서에 저작권에 대한 내용을 포함할 경우 복사나 배포의 대상을 명시해야 한다.

[시험 절차]

TEB.03.01
시험자는 벤더에게 제공받은 보안정책서가 저작권이 없는 문서인지 확인해야 한다.

TEB.03.02
시험자는 벤더에게 제공받은 저작권이 있는 보안정책서가 복사나 배포의 대상이 포함되었는지 확인해야 한다.

6.15 C 검증대상 암호알고리즘

비고 1 KS X ISO/IEC 19790의 **부속서** C는 암호모듈의 검증대상 암호알고리즘을 명세한 것이다.
비고 2 이 절의 요구사항은 없다.

6.16 D 검증대상 중요 보안매개변수 생성 및 설정 방법

비고 1 KS X ISO/IEC 19790의 **부속서** D는 암호모듈의 검증대상 중요 보안매개변수 생성 및 설정 방법을 명세한 것이다.
비고 2 이 절의 요구사항은 없다.

6.17 E 검증대상 인증 메커니즘

비고 1 KS X ISO/IEC 19790의 **부속서** E는 암호모듈의 검증대상 인증 메커니즘을 명세한 것이다.
비고 2 이 절의 요구사항은 없다.

6.18 F 검증대상 비침투 공격 완화 방법

비고 1 KS X ISO/IEC 19790의 **부속서** F는 암호모듈의 검증대상 비침투 공격 완화 방법을 명세한 것이다.
비고 2 이 절의 요구사항은 없다.

한국산업표준	정보기술 — 보안기술 — 암호모듈 시험 요구사항
발간 • 보급	한 국 표 준 협 회 153-787 서울특별시 금천구 가산디지털1로 145 에이스하이엔드타워 3차(16층) ☎ (02)2624-0114 ☎ (02)2624-0148 http://www.kssn.net

KS X ISO/IEC 24759:2015

KSKSKS
SKSKS
KSKS
SKS
KS
SKS
KSKS
SKSKS
KSKSKS

Information technology — Security techniques — Test requirements for cryptographic modules

ICS 35.040

Korean Agency for Technology and Standards
http://www.kats.go.kr